Turvallisuuden johtamisen kehittäminen Terveyden ja hyvinvoinnin laitoksella

Mikael Inkinen

Julkaisuvuosi 2020

Laurea-ammattikorkeakoulu

Turvallisuuden johtamisen kehittäminen
Terveyden ja hyvinvoinnin laitoksella

Kiitokset työn ohjaajille professori Jukka Ojasalolle (Laurea) ja palvelujohtaja Mikko Nissiselle (THL) sekä haastatelluille turvallisuusalan asiantuntijoille ja kiitos ennen kaikkea aviopuolisolleni Tommi Inkiselle ja ”pojallemme”, borderterrieri Danielille. Ilman teitä en olisi mitään.

Mikael Inkinen
Turvallisuusjohtamisen YAMK
Opinnäytetyö
Syyskuu, 2020

Lyhenteet

Lyhenne	**Selite**
THL	Terveyden ja hyvinvoinnin laitos Finnish institute for health and welfare
STM	Sosiaali- ja terveysministeriö
Fimea	Lääkealan turvallisuus- ja kehittämiskeskus
PMO	Project Management Office, projektihallintatoimisto
ISO	International Organization for Standardization
SFS	Suomen Standardisoimisliitto
BS	British Standard
COSO	The Committee of Sponsoring Organizations of the Treadway Comission
ERM	Enterprise Risk Management
BIA	Business Impact Analysis
VAP	Vapautettu aseellisesta palveluksesta sodan aikana
OTO	Oman toimen ohella

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusjohtaminen
Tradenomi Ylempi AMK

Mikael Inkinen

Turvallisuuden johtamisen kehittäminen Terveyden ja hyvinvoinnin laitoksella

Vuosi 2020 Sivumäärä 133

Tässä opinnäytetyössä tarkastellaan turvallisuutta, riskienhallintaa ja jatkuvuuden hallintaa turvallisuuden johtamisen kokonaisuudessa. Kehittämistyön tarkoitus on tarkastella, millaisista elementeistä turvallisuuden johtaminen muodostuu ja miten sitä voidaan kehittää kohdeorganisaatiossa. Terveyden ja hyvinvoinnin laitos on toimintaympäristönä monimuotoinen ja perinteikäs sekä jatkuvasti muuttuva tutkimus- ja asiantuntijalaitos, jolla on valtiohallinnon toimijana myös merkittävä vastuu yhteiskunnallisesta kokonaisturvallisuudesta.

Käytetty tutkimusmenetelmä on laadullinen tapaustutkimus, jossa tiedonkeruumenetelmänä ovat teemahaastattelut ja dokumenttianalyysi. Tutkimuksen tuloksena on kehitetty kaksi turvallisuuden kokonaisvaltaisen johtamisen mallia.

Turvallisuusjohtaminen on kokonaisvaltaista lakien, asetusten, määräysten ja omaehtoisen turvallisuuden hallintaa, joka muodostuu menetelmien ja toimintatapojen sekä ihmisten johtamisen yhdistelmänä. Organisaation riskienhallinnan tulee olla kokonaisvaltaista sekä kattaa strategiset, taloudelliset, operatiiviset ja vahinkoriskit. Riskienhallinta antaa perustan turvallisuuden johtamiselle osana organisaation strategista ja operatiivista johtamista.

Tutkimuksen perusteella voidaan todeta, että turvallisuuden hallinta ja johtaminen on keskittynyt pääosin yhteen osastoon. Muiden osastojen mukaan saaminen turvallisuustyöhön voi olla haasteellista ja vaikeuttaa organisaation yhteisten riskienhallintamenetelmien, turvallisuuskäytänteiden ja turvallisuuskulttuurin kehittymistä.

Lopputuloksena todetaan, että turvallisuuden johtaminen tulee perustua kokonaisvaltaiseen riskienhallintaan ja kaikki turvallisuuden osa-alueet huomioon ottavaan ajantasaiseen tilannetietoon sekä laajaan yhteistyöhön. Terveyden ja hyvinvoinnin laitoksen turvallisuuskulttuurin perustan muodostaa valtiohallinnon ohjeistus, hyvien käytänteiden ja esimerkkien hyödyntäminen sekä viestintä. Turvallisuusalan ammattilaisten johdolla ja kokonaisvaltaisen turvallisuuden johtamisen avulla voidaan Terveyden ja hyvinvoinnin laitosta viedä kohti turvallisempaa, hallittavampaa ja toimivampaa organisaatiota.

Asiasanat: Turvallisuus, johtaminen, riskienhallinta, jatkuvuuden hallinta, riskikulttuuri.

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Master of Business Administration

Mikael Inkinen

Development of Security and Safety Management at the Finnish institute for health and welfare

Year 2020 Pages 133

This thesis examines security and safety, risk management and continuity management in the comprehensive security management. The purpose of the development work is to examine what elements of safety and security management consist of and how it can be developed in the target organization. The Finnish institute for health and welfare is a diverse and traditional and constantly changing research and expert institution, which, as an actor in public administration, also has a significant responsibility for comprehensive Finnish society security.

The research method used is a qualitative case study, where the data collection methods are thematic interviews and document analysis. As a result of the study, two models of comprehensive safety and security management have been developed.

Security management is a comprehensive management of laws, regulations, ordinances and voluntary safety and security, which consists of a combination of methods and practices as well as people management. The risk management of the organization and departments must be comprehensive and cover strategic, financial, operational, and damage risks. Risk management provides the basis for security management as part of an organization's strategic and operational management.

Based on the study, it can be stated that security management is in practice concentrated in one department only. Getting other departments involved in safety and security work is challenging and hinders the development of the organization's common risk management methods, safety and security practices and security culture.

As a result of the development work, it is stated that security management should be based on comprehensive risk management and up to date information and should take into account all aspects of safety and security, as well as extensive cooperation. The organization’s safety culture is based on the guidelines of the state administration, the utilization of good practices and examples and communication. With security professionals and comprehensive security and safety management, the Finnish institute for health and welfare is able to be taken towards a safer, more manageable and more functional organization.
Keywords: Security, Leadership, Risk Management, Continuity Management, Risk Culture

Sisällys

1 Johdanto

Tässä opinnäytetyössä tarkastellaan, miten Terveyden ja hyvinvoinnin laitoksessa (THL) voidaan kehittää turvallisuuden johtamista. Edellytyksenä turvallisuuden kokonaisvaltaiselle johtamiselle on, että se perustuu riskienhallintaan, on sidottu johtamisjärjestelmään ja saa tarkoituksensa organisaation strategiasta. Työssä tarkastellaan turvallisuuden johtamisen nykytilaa ja kehittämiskohteita riskienhallinnan ja jatkuvuuden hallinnan kautta.

1.1 Tausta

Matias Virta on tehnyt vuonna 2014 opinnäytetyön, jossa on luotu riskienhallinnan järjestelmä Terveyden ja hyvinvoinnin laitoksessa. Siinä kappaleessa 5.3. ehdotetaan turvallisuusjohtamisen kehittämistä. Virran (2014, 65-66) mukaan Terveyden ja hyvinvoinnin laitoksella turvallisuudelle ja riskienhallinnalle voidaan löytää toiminnan tavoitteita yhdistäviä kontaktipintoja ja, että riskienhallinta ja turvallisuusjohtaminen yleisesti ottaen tukevat vahvasti toisiaan toimintana, jossa on vuorovaikutteisuutta, koska riskienhallinta ja turvallisuusjohtaminen vastaavat toistensa tarpeisiin. Hän korostaa, että riskienhallinnan merkitys on keskeinen, koska se luo organisaatiolle keinot uhkien tunnistamiseen, jonka pohjalta turvallisuusjohtamista voidaan kehittää niin, että nämä uhat voidaan torjua. Virta ehdottaakin, että organisaatiolle ryhdyttäisiin rakentamaan riskienhallintaan perustuvaa turvallisuusjohtamisjärjestelmää. Hän toteaa vielä, että mikäli organisaatiolla on riskienhallintajärjestelmä, saadaan sen avulla vahvat puitteet, periaatteet ja prosessit turvallisuusjohtamiselle. Hän myös ehdottaa, että laadittaisiin yhteinen politiikka riskienhallinnan ja turvallisuusjohtamisen taustalle. Sen avulla voitaisiin varmistua molempien tekijöiden vaikuttavuudesta ja valtuuksista. Hän myös mainitsee, että organisaation turvallisuusjohtamista ja sen hallinnollista kokonaisuutta on kehitettävä varmistamaan organisaation toiminnan jatkuvuus. Erityisiksi kehittämiskohteiksi nousi yhtenäinen hallinnoitu kokonaisuus, tavoitteiden asettelu, vastuiden selkeyttäminen, yhtenäisen raportoinnin suunnittelu, valtuuttava ja sitouttava politiikka, seuranta ja arviointi sekä kokonaisuuden selkeys.

Terveyden ja hyvinvoinnin laitoksen silloinen tietoturvapäällikkö Christian Jämsen on omassa turvallisuusjohdon koulutusohjelman tutkielmassa (2017, 45) tarkastellut miten turvallisuusjohtamisjärjestelmä on mahdollista integroida kohdeorganisaation (Terveyden ja hyvinvoinnin laitos) johtamisjärjestelmään. Hän toteaa: ”Turvallisuustoiminnan johtamisen organisointia tulee pohtia. Jos toiminta on vastuutettu monelle toimijalle organisaatiorajojen yli ja kenelläkään ei ole määritelty kokonaisvastuuta toiminnasta, asioiden priorisointi voi muodostua haasteelliseksi tai jopa mahdottomaksi. Toisaalta organisaation turvallisuusasioiden keskittäminen yhteen linjaan ei aina ole mahdollista tai käytännön syistä edes mielekästä. Kyse on

lähinnä siitä, että huolehditaan vastuiden selkeästä ja yhdenmukaisesta määrittelystä ja siitä, että kaikki tuntevat ne sekä osaavat ja uskaltavat toimia niiden mukaisesti. Turvallisuuden raportointivastuut tulee määritellä suoriksi ja välittömiksi. Ehdottoman tärkeää kuitenkin on, että päätöksentekolinjasta riippumatta on yhteisesti sovitut mekanismit suunnittelun ja toteutuksen yhteensovittamiseksi.” Hän mainitsee myös, että vastuiden selkeyttäminen ja pääperiaatteiden kommunikointi voisi tapahtua yhteisen turvallisuuspolitiikan kautta, jota organisaatiolla ei tällä hetkellä ole. Lisäksi hän mainitsee, että ”riskienhallinnan kehittäminen ja sen määrätietoisempi käyttäminen turvallisuusasioiden raportoimisen, suunnittelun ja seurannan välineenä on ehdottoman suositeltavaa” ja että ”yhteiskoordinaation kehittäminen esimerkiksi kattavan ja koordinoivan kokonaisturvallisuuden käsitteen ympärille rakentuvassa turvallisuusryhmässä on nähtävä toimivana ja mahdollisena osana turvallisuusjohtamisjärjestelmän kehittämistä ja integroimista.”

THL:ssä ollaan uudistamassa organisaatiota, uudistuksen nimi on THL2021. Organisaation rakenneuudistus toteutetaan 2020 ja se tulee voimaan 2021 alusta. Organisaation uudistuessa on hyvä tilaisuus tarkastella myös turvallisuuden johtamisen uudistamista kokonaisuutena. Matias Virran (2014) opinnäytetyön päätavoite eli riskienhallintajärjestelmän käyttöönotto on pääosin toteutettu implementoimalla Granite -riskienhallintajärjestelmä organisaatiossa ja hänen laatimansa turvallisuusjohtamisen kehittämissuunnitelma on toteutettu turvallisuusryhmän perustamisen myötä ja turvallisuuden osa-alueiden (EK 2020 mukaan) kehittämisen osalta ainakin osittain, mutta vastaako nykyinen toteutus kokonaisvaltaisen turvallisuusjohtamisen tarvetta, jota myös Jämsen (2017) on tutkielmassaan ehdottanut kehittämiskohteeksi ja onko se integroitu organisaation johtamisjärjestelmään? Tässä työssä tätä kokonaisuutta tarkastellaan riskienhallinnan, jatkuvuuden hallinnan ja turvallisuuden johtamisen näkökulmasta. Turvallisuuden johtaminen on osa riskienhallintaa, joten riskienhallinta on laajasti vallitsevan käsityksen mukaan (mm. turvallisuusjohtaminen 2010) laajempi kokonaisuus ja riskienhallinnan johtamisjärjestelmä sisältää myös kokonaisturvallisuuden johtamisjärjestelmän. Lanne (2007, 29) on väitöskirjassaan kuitenkin toista mieltä ja sanookin kyseessä olevan enemminkin tarkastelunäkökulman valinta kuin hierarkkinen suhde. Tätä ristiriitaa riskienhallinnan ja turvallisuusjohtamisen suhteista esiintyy laajemminkin alan kirjallisuudessa.

Tässä työssä keskitytään turvallisuuden johtamisen kehittämiseen, mutta kokonaisuutta tarkastellaan laajemmin riskienhallinnan ja myös jatkuvuuden hallinnan kautta ja erityisesti valtiohallinnon näkökulmasta. Riski määritellään ISO standardin mukaan (SFS-ISO 31000, 6-7) olevan epävarmuuden vaikutus tavoitteisiin ja organisaation riskienhallinta on koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta ja koska riskienhallinnan päämääränä on tunnistaa ja havaita ajoissa organisaation toimintaan ja tavoitteiden saavuttamiseen vaikuttavia positiivisia (liiketoiminta mahdollisuudet) ja negatiivisia (toimintaa uhkaavat riskit) tekijöitä, se käsittää myös muuhun kuin turvallisuuteen liittyvien riskien, kuten

talouteen, investointeihin, vakuutuksiin tai rekrytointeihin jne. liittyviä epävarmuuksia, joiden pohjalta tehdään liiketoimintapäätöksiä ja määritellään organisaation riskinkantokyky tai riskinottohalukkuus (SFS-ISO 31000). Lisäksi organisaatiolla voi olla taloudellisia, poliittisia tai toimintaympäristöön liittyviä kulttuurillisia riskejä. Näin laajasti organisaation riskienhallintaa ei tässä työssä käsitellä vaan keskitytään turvallisuuden johtamisen näkökulmaan, mutta riskienhallintaa muustakin kuin turvallisuuden johtamisen näkökulmasta sivutaan liitteessä, jossa on kerrottu riskienhallinnan standardeista ja hyvistä käytänteistä. Edellä mainituista syistä kirjoittaja on otsikoinut työn turvallisuusjohtamisen kehittämiseksi, riskienhallinnan johtamisen kehittämisen sijasta. Tässä siis keskitytään niihin tekijöihin, jotka uhkaavat organisaation tietoa, mainetta, omaisuutta, ympäristöä, henkilökuntaa, asiakkaita ja kumppaneita. Matias Virta toteaa vielä opinnäytetyönsä Turvallisuusjohtamisen kehittämissuunnitelman kappaleessa (Virta 2014, 66), että ”Turvallisuusjohtamisessa korostuu selkeät intressit riskienhallinnan kanssa, sillä toimintoihin on suunniteltava selkeät vastuut ja käsittelytasot”. Turvallisuusjohtamisen kehittämiselle riskienhallinnan kautta on johdonmukaiset perusteet ja siksi riskienhallinnalla on suuri osuus tietoperustaa.

Jatkuvuudenhallinnalla on erityinen asema kokonaisvaltaisessa turvallisuuden johtamisessa. Jatkuvuussuunnittelun tavoitteena on varmistaa organisaation ydintoimintojen mahdollisimman häiriötön toiminta. Jatkuvuussuunnittelu on osa organisaation kokonaisturvallisuutta, johon kuuluvat turvallisuusjohtaminen, riskienhallinta, jatkuvuuden hallinta, häiriötilanteiden hallinta ja johtaminen, tilannekuvan (tai riskikuvan) muodostaminen sekä huoltovarmuus ja varautuminen. (VM 2016). Kokonaisturvallisuuden kautta tässä työssä lähestytään Terveyden ja hyvinvoinnin laitoksen turvallisuuden johtamisen nykytilaa ja kehittämisen lähtökohtia. Kyberturvallisuus on myös jatkuvuuden hallinnan kokonaisuuteen liittyvä kriittinen osa ja siksi mukana omana kappaleena.

Riskienhallinnan johtaminen on organisaation ylimmän johdon vastuulla ja sen tulee sisältyä kaikkeen johtamiseen. Turvallisuuden johtaminen on keskeinen osa riskienhallinnan johtamista ja turvallisuuden johtamisesta vastaavan turvallisuuspäällikön, turvallisuusjohtajan, riskienhallintajohtajan tai vastaavalla nimikkeellä työskentelevän henkilön, jolla on kokonaisvastuu turvallisuuden johtamisesta ja kehittämisestä, tuleekin olla osa organisaation ylintä johtoa ja toimia täysipäiväisesti turvallisuuden johtamisen tehtävissä. Jämsen (2017, 45) muistuttaa, että yksinomaan yhteistyöryhmän perustaminen ei pitkällä tähtäimellä riitä, kun tavoitellaan turvallisuusasioiden parempaa hallittavuutta ja integroimista osaksi laajempaa kokonaisuutta, jonka vuoksi olisi syytä pohtia kehittämissuunnitelma niiden saavuttamiseksi. Lisäksi hän toteaa, että toimiakseen hyvin turvallisuustoiminta tarvitsee selkeät määritelmät toimintatavoista, valtuuksista ja vastuista sekä hyväksymisketjuista. Kiviharju (2015, 15) toteaa AaltoPron turvallisuusjohdon valtiohallinnon turvallisuusjohtamista käsittelevässä tutkielmassaan, että turvallisuusvastuita ajaudutaan usein kantamaan oman toimen ohella (OTO), eikä organisaatiossa kiinnitetä riittävästi huomiota vastuuhenkilöiden mahdollisuuteen

hoitaa turvallisuusjohtamisen vastuitaan. Lisäksi hän toteaa saman mitä Jämsenkin, että oman toimen ohella tapahtuva turvallisuustyö viittaa kehittämistä vailla olevaan organisaation johtamiseen.

Tässä työssä on turvallisuuden kokonaisvaltaisuuden ja kaiken tavoitteellisen toiminnan sisälleen sulkevuuden korostamiseksi eroteltu käsitteet ”turvallisuusjohtaminen” ja ”turvallisuuden johtaminen”. Turvallisuusjohtamisella tarkoitetaan määritelmän mukaista järjestelmällistä organisaation hyvinvoinnin turvaamista ihmisiä, mainetta, ympäristöä, tietoa ja omaisuutta suojaamalla, kun taas turvallisuuden johtamisella tarkoitetaan kokonaisuutta, joka käsittää kaikki organisaation turvallisuustavoitteisiin liittyvät asiat. Turvallisuusjohtaminen – käsitettä käytetään niissä yhteyksissä, missä puhutaan nimenomaan käsitteestä ja ”turvallisuuden johtaminen” -termiä silloin, kun puhutaan turvallisuuden johtamisesta laajana kokonaisuutena eri konteksteissa. Nämä termit ovat yleensä kirjallisuudessa synonyymeja, mutta kirjoittaja on halunnut korostaa turvallisuuden johtamisen kokonaisvaltaisuuttaa erottamalla ne niissä kohdissa missä se on tarkoituksenmukaista ja selventää tekstiä.

1.2 Tavoite

Tämän opinnäytetyön ja kehittämishankkeen tavoitteena on tarkastella, miten turvallisuuden johtamista voitaisiin kehittää niin, että sen avulla voidaan paremmin hallita Terveyden ja hyvinvoinnin laitoksen toimintaa uhkaavia riskejä kokonaisvaltaisesta. Tavoitteena on kehittää toimintaa siten, että kaikki eri toimijat tulevat kokonaisarvioinnissa huomioiduksi ja samalla tuottaa turvallisuuden johtamisen malleja, joita soveltamalla turvallisuuden johtaminen olisi kiinteä osa laitoksen johtamisjärjestelmää. Terveyden ja hyvinvoinnin laitoksessa on useita turvallisuuteen liittyviä tehtäviä ja nimikkeitä, mutta ei selkeää, näkyvillä olevaa organisaatiokuvausta, jossa turvallisuus olisi osana johtamista ja jonka kautta saisi kuvan siitä, miten turvallisuuden johtamisen kokonaisuus laitostasoisesti ja ylimmän johdon alaisena johdetaan. Turvallisuus -nimikkeellä olevat henkilöt ovat lähes yksinomaan (6/8) yhden osaston, mutta kuitenkin viiden yksikön alaisuudessa. Osasto, josta turvallisuutta johdetaan ei kuitenkaan ole turvallisuusosasto tai vastaava ja osa tehtävistä on vastuutettu oman toimen ohella (OTO) tehtäväksi. Terveyden ja hyvinvoinnin laitoksessa on vuonna 2015 ensimmäisen kerran ja uudelleen vuonna 2019 asetettu turvallisuusryhmä, jonka tehtävänä on mm. kokonaisturvallisuuden hallinta. Tarkastelen tässä työssä, miten ryhmä käytännössä toimii ja miten sen toiminta vastaa kokonaisvaltaisen turvallisuuden johtamisen haasteisiin ja onko turvallisuusryhmän jäsenten sijoittuminen lähes yksinomaan vain yhteen osastoon tarkoituksenmukaista. Kirjoittaja on työn kuluessa kehittänyt omia, eri näkökulmista johtamista katsovia turvallisuusjohtamisen malleja, joilla on tässä työssä kokonaisuuden ja johtopäätösten osalta tärkeä osa.

1.3 Rajaus

Opinnäytetyö on kvalitatiivinen tutkimus, jossa lähestymistapana on tapaustutkimus (Case Study), jossa tarkastellaan riskienhallintaa, jatkuvuussuunnittelua, varautumista ja turvallisuusjohtamista tietoperustan kautta ja valtiohallinnossa yleensä ja sen jälkeen, miten turvallisuuden johtaminen on toteutettu näiden avulla Terveyden ja hyvinvoinnin laitoksella ja miten sitä tulisi kehittää.

1.4 Keskeiset käsitteet

Opinnäytetyössä ja sen sisällä toteutetussa tutkimuksessa on keskeisessä asemassa riskienhallintaan, turvallisuuteen ja johtamiseen liittyviä käsitteitä. Teoksessa kehittämistutkimus opinnäytetyönä (Kananen 2012, 57-58) määritellään, että käsite on abstraktio, jolla ilmiötä voidaan luokitella niitä yhdistävien ja erottavien piirteiden tai ominaisuuksien mukaan. Käsitteet ovat alan ilmiöiden ymmärtämisen kannalta olennaisen tärkeitä. Käsitteiden avulla voidaan tunnistaa alan ongelmia ja ratkaista niitä tehokkaasti.

Tämän opinnäytetyön keskeiset käsitteet ovat johtaminen, riskienhallinta, jatkuvuuden hallinta, turvallisuusjohtaminen ja riskikulttuuri sekä turvallisuuskulttuuri.

Johtaminen
Johtaminen voidaan määritellä sosiaaliseksi vuorovaikutusprosessiksi, jossa asetetut tavoitteet saavutetaan ryhmän toimintaan vaikuttamalla (Yukl 2002). Johtaminen jaetaan usein asiajohtamiseen, joka keskittyy organisointiin ja suunnitelmiin sekä henkilöjohtamiseen, joka keskittyy työt ohjaaviin linjauksiin ja henkilöiden motivointiin.

Riskienhallinta
Riskienhallinta on koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta ja sen tarkoitus on arvon luominen ja säilyttäminen. Riskienhallinta parantaa suorituskykyä ja tukee innovointia ja tavoitteiden saavuttamista. (SFS-ISO 31000, 6-7)

Jatkuvuuden hallinta
Jatkuvuuden hallinta (tai jatkuvuudenhallinta) tarkoittaa toimintamallia, jolla organisaatio tunnistaa ja arvioi toimintaansa liittyvät riskit, häiriötilanteet ja riippuvuudet, organisoi ja toteuttaa menettelytavat erilaisten häiriötilanteiden varalle, varmistaa kriittisten kumppaneidensa kyvyn toimia erilaisissa häiriötilanteissa sekä suojaa toimintansa intressit ja arvontuotantokykynsä. (Turvallinen Suomi 2018, 95).

Kokonaisturvallisuuden sanaston (2017, 31) mukaan jatkuvuuden hallinta on yleensä omatoimista strategista ja operatiivista toimintaa, jolla on johdon hyväksyntä ja jolla organisaatio varautuu häiriötilanteiden hallintaan ja jatkamaan toimintaansa ennakkoon määritellyllä

hyväksyttävällä tasolla. Jatkuvuudenhallinnan painopiste on normaaliolojen häiriötilanteissa, mutta prosessi voi sisältää myös varautumista poikkeusoloihin. Joillakin organisaatioilla jatkuvuudenhallinta on lakisääteistä toimintaa, joka velvoittaa varmistamaan toiminnan jatkuvuus kaikissa olosuhteissa.

Turvallisuusjohtaminen

Turvallisuusjohtamisella tarkoitetaan järjestelmällistä ja organisoitua toimintaa, jolla yrityksen tai organisaation tietoon, maineeseen, omaisuuteen, ympäristöön ja henkilökuntaan sekä asiakkaisiin kohdistuvia vahingoittavia tapahtumia ennaltaehkäistään. Turvallisuusjohtamiseen liittyy myös organisaation johtamisjärjestelmä, joka on henkilöstön, resurssien, toimintapolitiikkojen yhdistelmä organisaation kaikilla tasoilla ja joiden välillä on organisoitua vuorovaikutusta strategisten tavoitteiden ja operatiivisen toiminnan välillä. Turvallisuusjohtamisen päämääränä on turvata organisaation hyvinvointi eli ihmiset, maine, tieto, omaisuus ja ympäristö. (Turvallisuusjohtaminen 2010, 5; Katakri 2015)

Riskikulttuuri

Riskikulttuurilla tarkoitetaan lopputulemaa yksilön ja ryhmän käyttäytymisen arvoista, asenteesta ja toimintamalleista. (Hopkin 2018, 288). Hilsson (2013) kuvaa riskikulttuurin muodostuvan ABC-mallista, jossa A on Risk Attitude ja tarkoittaa asennetta riskeihin, B on Risk Behaviour ja tarkoittaa riskikäyttäytymistä ja C on Risk Culture, joka tarkoittaa organisaation riskikulttuuria. Nämä liittyvät toisiinsa siten, että asenne riskeihin muokkaa riskikäyttäytymistä, joka muodostaa riskikulttuurin. Toisaalta organisaation riskikulttuuri vaikuttaa sekä riskikäyttäytymiseen, että asenteeseen riskejä kohtaan.

Turvallisuuskulttuuri

Turvallisuuskulttuuri -käsitteellä on pyritty korostamaan niitä periaatteita, jotka vallitsevat organisaation toiminnan taustalla ja jotka ohjaavat päivittäistä toimintaa ja päätöksentekoa. Käsite on lähellä organisaatiokulttuuria -käsitettä, joka esiintyy organisaatiotutkimuksen kentässä, mutta turvallisuuskulttuurilla halutaan korostaa organisaation toimintaa nimenomaan suhteessa turvallisuuteen. (Ooedewald & Reiman 2006, 27). Health and Safety Executive (HSE 1997, 16) on määritellyt turvallisuuskulttuurin seuraavasti: "Organisaation turvallisuuskulttuuri on tulema yksilön ja ryhmän arvoista, käsityksistä, asenteista, osaamisesta ja käyttäytymistavoista, jotka määrittelevät organisaation turvallisuusjohtamisen tyylin ja tason sekä sitoutumisen siihen. Organisaatioissa, joissa on positiivinen ja hyvä turvallisuuskulttuuri on tunnistettu piirteitä, kuten keskinäiselle luottamukselle perustuva kommunikaatio, yhteinen käsitys turvallisuuden tärkeydestä sekä luottamus ennakoivien toimenpiteiden tehokkuuteen."

1.5 Kohdeorganisaatio

Kohdeorganisaatio on Terveyden ja hyvinvoinnin laitos, jossa kirjoittaja itse työskentelee tietohallinnon kehittämistehtävissä. Laitos on monimutkainen jatkuvasti kehittyvä, pitkän historian omaava valtion laitos, jolla on vaativa tehtävä valtiohallinnossa ja suomalaisten terveyden ja hyvinvoinnin vaalimisessa. Tiedon ja tiedonhallinnan merkitys laitoksen toiminnassa on aina ollut suuri ja tämän päivän kokonaisvaltainen turvallisuusympäristö, jossa tietoa uhkaa niin internetin kautta yhä kehittyvämmät menetelmät kuin bittien ja atomien maailman entistä tiiviimmän yhdistymisen kautta tulevat tahalliset ja tahattomat turvallisuusuhat, on yhä kriittisempi tekijä laitoksen toiminnassa ja korostaa turvallisuuden ja riskienhallinnan merkityksen kasvua laitoksen toimintavarmuuden ja jatkuvuuden hallinnassa. Kirjoittaja ei pääasiassa työskentele turvallisuustehtävissä, mutta on havainnut, että laitoksen strategia viidelle vuodelle (2019-2023) on haastava ja kunnianhimoinen ja turvallisuuden eri osa-alueiden merkitys laitoksen toiminnassa kasvaa ja monipuolistuu vastuiden ja velvoitteiden kasvaessa. Terveyden ja hyvinvoinnin laitos on saanut vastuulleen entisten toimintojen lisäksi monia uusia toimintoja, mutta resurssit eivät ole kasvaneet samassa suhteessa. Johtamisella on aivan keskeinen merkitys ja turvallisuusjohtamisella erityinen tehtävä tässä toimintaympäristössä. Valtiohallinnon toimijana ja vuosikymmenien aikana kerättyjen terveyteen liittyvän tutkimustietojen haltijana, Terveyden ja hyvinvoinnin laitoksella on myös merkittävä rooli suomalaisen yhteiskunnan kokonaisturvallisuudessa.

Terveyden ja hyvinvoinnin laitos (THL) on yksi valtion 80 virastosta ja toimii sosiaali- ja terveysministeriön (STM) hallinnonalalla. Terveyden ja hyvinvoinnin laitoksen toimintaa ohjaa Laki Terveyden ja hyvinvoinnin laitoksesta (L668/2008). Laissa Terveyden ja hyvinvoinnin laitoksen tehtävä määritellään näin: ”Väestön hyvinvoinnin ja terveyden edistämiseksi, sairauksien ja sosiaalisten ongelmien ehkäisemiseksi sekä sosiaali- ja terveydenhuollon ja sen palvelujen kehittämiseksi on Terveyden ja hyvinvoinnin laitos. Laitos on sosiaali- ja terveysministeriön (STM) alainen.” (THL 2020)

Terveyden ja hyvinvoinnin laitosta johtaa pääjohtaja. Vuoden 2018 alusta viisivuotisen kautensa aloitti lääketieteen tohtori Markku Tervahauta. Pääjohtajan valitsee STM. Vuoden 2019 lopussa laitoksella on aloittanut myös tietoylijohtaja, joka korostaa THL:n roolia tietotalona.

THL jakaantuu johdon lisäksi seitsemään osastoon, joita johtavat osastonjohtajat. Näiden lisäksi on vuonna 2019 aloittanut tietolupaviranomainen (Findata), joka toimii THL tiloissa ja käyttää THL infrastruktuuria, mutta on riippumaton viranomainen tietolupapäätöksissään. Tietolupaviranomaisen toiminta on käynnistynyt valmistelujen jälkeen 1.1.2020. Työntekijöitä Terveyden ja hyvinvoinnin laitoksessa on noin 1400 ja toimintaa on Helsingin lisäksi Oulussa, Tampereella, Turussa joissa toimii pääasiassa oikeuslääketieteelliset yksiköt ja Kuopiossa lisäksi ympäristöterveyden tutkimukseen keskittynyt yksikkö. Kaikki Suomen

oikeuslääketieteelliset ruumiinavaukset tehdään Terveyden ja hyvinvoinnin laitoksen toimesta. Terveyden ja hyvinvoinnin laitos vastaa näiden lisäksi Suomen vankiloiden vankiterveydenhuollosta, valtion koulukodeista ja valtion mielisairaaloista Niuvanniemessä ja Vanhan Vaasan sairaalassa. Vankiterveydenhuollon toimipisteitä on yli 30 ja koulukoteja noin 20. (THL organisaatio)

”Terveyden ja hyvinvoinnin laitos tutkii ja seuraa väestön hyvinvointia ja terveyttä ja kehittää toimenpiteitä niiden edistämiseksi. Keräämme ja tuotamme tutkimukseen ja tietoaineistoihin perustuvaa tietoa. Lisäksi tarjoamme asiantuntemusta ja ratkaisuja, joita sidosryhmämme voivat käyttää päätöksenteossa ja työnsä tukena.” (THL 2020).

Terveyden ja hyvinvoinnin laitoksen strategia on uudistettu vuonna 2019 ja siinä visiona on olla ”maailman vaikuttavin terveys- ja hyvinvointialan tutkimuslaitos”. Tarkempi määrittely on, että ”teemme korkeatasoista tutkimus- ja asiantuntijatyötä. Kumppaniemme kanssa saamme aikaan merkittävän muutoksen: väestön terveys, toimintakyky ja osallisuus paranevat sekä ihmisten mahdollisuus pitää huolta omasta ja läheistensä hyvinvoinnista vahvistuu. Rakennamme työllämme tasa-arvoista, yhdenvertaista ja kestävää yhteiskuntaa. Pidämme huolta heikommista.” (THL strategia 2019).

Terveyden ja hyvinvoinnin laitos on tutkimuslaitos ja sen toiminnassa tiedolla on luonnollisesti suuri arvo. Tieto on epäilemättä THL:n arvokkain pääoma, mutta asiantuntevuus voidaan sanoa olevan tärkein ominaisuus, eikä unohtaa sovi noin viiden miljoonan näytteen muodostama kokonaisuutta, joinka ylläpito on laitoksen vastuulla. Uudessa strategiassa tiedolle on asetettu seuraavat tavoitteet: vastaamme tietotarpeisiin laadukkaasti ja oikea-aikaisesti, laajennamme tietotuotantoa olennaisille katvealueille, huolehdimme toimintamme digitaalisesta turvallisuudesta ja varaudumme kyberuhkiin.” (THL strategia 2019). Tätä voidaan pitää koko Terveyden ja hyvinvoinnin laitoksen strategisena tavoitteena teknologian näkökulmasta.

THL arvot ovat, että luottamuksen arvoinen THL on:

Vastuullisesti rohkea	Se tarkoittaa, että Osaamme. Kokeilemme. Uudistamme.
Inhimillinen vuorovaikuttaja	Se tarkoittaa, että Arvostamme. Kuulemme. Keskustelemme.
Yhdenvertaisuuden suunnannäyttäjä	Se tarkoittaa, että Osallistamme. Kannustamme. Haastamme.

Toimintaympäristönä THL on hyvin monialainen ja monimutkainen sisältäen laboratorioita, viranomaistoimintaa, oikeustoksikologiaa, oikeusgenetiikkaa ja oikeuslääketieteellisiä ruumiinavauksia, tutkimustoimintaa, biopankkitoimintaa, laajojen tietovarantojen ja näyteomaisuuden käsittelyä ja hallintaa sekä tavallista toimistotyöskentelyä perinteisessä ja monitilaympäristössä.

Terveyden ja hyvinvoinnin laitoksella on merkittävä rooli suomalaisen yhteiskunnan terveyden ja hyvinvoinnin asioiden hallinnassa ja viraston toiminta pitääkin olla sujuvaa ja häiriötöntä

kaikissa olosuhteissa. Toimintaympäristö on hyvin haastavaa monien lakien, määräysten, asetusten ja vaatimusten ohjatessa toimintaa. Tämä asettaa suuren haasteen myös riskienhallinnalla, jatkuvuussuunnittelulla ja turvallisuuden johtamisella.

2 Tietoperusta

Tutkimukselliseen kehittämistyöhön kuuluu vahvana osana tietoperusta (käytetään myös nimitystä teoreettinen viitekehys). Tietoperusta jäsentää opinnäytetyön tarkoitusta ja rajaa tutkimus- tai kehittämistehtävää. Tietoperusta muodostuu aiheeseen liittyvästä teoriasta. Tietoperusta pohjautuu aikaisempaan tietoon, joka kehittyy opinnäytetyön analyysin pohjalta synteesiksi. Tekijä kokoaa tietoperustaa aikaisempien tutkimusten, kirjallisuuden, työelämäkokemuksen sekä intuition perusteella. Aiempaa tietoa ja aiemmin saatuja tuloksia voidaan esitellä, ja samalla tarkastella niiden luotettavuutta, yleistettävyyttä ja suhdetta omaan opinnäytetyöhön. (JAMK 2020)

Alasuutari (2007, 81) määrittelee, että teoreettinen viitekehys on tietty, eksplisiittinen näkökulma havaintoaineistoon. Havaintoa pidetään johtolankoina, joka johdattaa tutkijaa tutkimuksen tuloksena esitettyihin johtopäätöksiin tai toisinpäin sanottuna hypoteesien puolesta puhuvana todisteena.

Tieteellisten tulosten tulee olla julkisia ja tiedeyhteisön taholta kriittisesti arvioitavia. itsekorjautuvuudella tarkoitetaan sitä, että tutkimuksen virheet ja puutteet voidaan poistaa uusilla tutkimuksilla. Tutkimuskohteen ominaisuudet ovat tutkijan mielipiteistä tai muista auktoriteeteista riippumattomia. (Haaparanta & Niiniluoto 2016; Salminen 2011, 1)

Tämä opinnäytetyön tietoperusta käsittelee riskienhallintaa ja sen yhteyttä turvallisuusjohtamiseen ja organisaation riskikulttuuriin sekä jatkuvuuden hallintaan. Tietoperusta on kerätty eri lähteistä hyödyntäen kohdeorganisaation nykytilan kuvausta, aikaisempia tutkielmia, valtionhallinnon ohjeistusta, riskienhallinnan- ja turvallisuusalan kirjallisuutta sekä turvallisuustutkimuksia. Teorian tarkoituksena on perustella tapaustutkimuksessa käytettyjä menetelmiä. Teoriatiedon tarkoitus on myös osoittaa, miten kohdeorganisaatio voi hyödyntää viitekehyksen kautta saatua tietoa kehittämistyössään.

Käytetty tutkimustapa on laadullinen tapaustutkimus ja käytetty tiedonkeruumenetelmä on kohdeorganisaation kirjallinen materiaali verkkosivuilla ja organisaation sisäverkossa, valtiohallinnon ohjeet ja käytänteet sekä alan kirjallisuus ja tutkimukset, joiden pohjalta on tehty dokumenttianalyysia sekä kohdeorganisaatiossa toteutetut teemahaastattelut.

Lähtökohtana kvalitatiivisessa tutkimuksessa on todellisen elämän kuvaaminen, johon sisältyy ajatus, että todellisuus on moninainen, mutta tutkimuksessa on otettava huomioon, että

todellisuuden voi mielivaltaisesti pirstoa osiin. Eri tapahtumat muovaavat samanaikaisesti toisiaan ja tutkimuksen kuluessa onkin mahdollista löytää suhteita, jotka ulottuvat moneen suuntaa. Kvalitatiivisen tutkimuksen ominaispiirre on, että siinä kohdetta pyritään tutkimaan mahdollisimman kokonaisvaltaisesti. (Hirsjärvi, Remes & Sajavaara 2018, 16)

Kvalitatiivisessa tutkimuksessa haastattelu on päämenetelmä. Haastattelun suurena etuna muihin tiedonkeruumuotoihin on, että siinä voidaan säädellä aineiston keruuta joustavasti tilanteen edellyttämällä tavalla ja vastaajia myötäillen. Haastatteluaiheiden järjestystä on mahdollista säädellä, samoin on enemmän mahdollisuuksia tulkita vastauksia kuin esimerkiksi postikyselyssä. Haastattelun etuna on myös, että haastateltavat henkilöt saadaan mukaan tutkimukseen, jolloin haastateltavat on mahdollista tavoittaa myöhemmin uudelleen, jos on tarpeen täydentää aineistoa. (Hirsjärvi ym. 2018, 205-206)

Kvalitatiivisen tutkimuksen yksi haastattelumenetelmä on teemahaastattelut. Teemahaastattelu eli puolistrukturoitu haastattelu on lähellä syvähaastattelua. Teemahaastattelussa edetään tiettyjen keskeisten etukäteen valittujen teemojen ja niihin liittyvien tarkentavien kysymysten varassa. Teemahaastattelun etuna on se, että haastattelussa voidaan tarkentaa ja syventää kysymyksiä haastateltavien vastauksiin perustuen. Metodologisesti teemahaastattelussa korostetaan ihmisten tulkintoja asioista, heidän asioille antamiaan merkityksiä sekä sitä miten merkitykset syntyvät vuorovaikutuksessa. (Hirsjärvi & Hurme 2007; Tuomi & Sarajärvi 2018, 88)

2.1 Tutkimuksen reliabiliteetti ja validiteetti

Tutkimuksessa pyritään välttämään virheiden syntymistä, mutta silti tulosten luotettavuus ja pätevyys vaihtelevat. Tämän vuoksi kaikissa tutkimuksissa pyritään arvioimaan tehdyn tutkimuksen kautta luotettavuutta eli reliabiliteettia. Tutkimuksen luotettavuuden arvioinnissa voidaan käyttää monenlaisia mittaus- ja tutkimustapoja. Tutkimuksen luotettavuus tarkoittaa mittaustulosten toistettavuutta ja pätevyys eli validiteetti tarkoittaa mittarin tai tutkimusmenetelmän kykyä mitata juuri sitä, mitä on tarkoituskin mitata. On selvää, että nämä tutkimuksen reliabiliteetti ja validiteetti on vaikeita osoittaa kvalitatiivisessa tutkimuksessa ja ne ovatkin saaneet erilaisia tulkintoja. Termit ovat syntyneet kvantitatiivisen tutkimuksen parissa ja kvalitatiivisessa tapaustutkimuksessa voidaan ajatella, ettei ole kahta samanlaista tapausta, joten perinteiset luotettavuuden ja pätevyyden arvioinnit ei tule kysymykseen. (Hirsjärvi ym. 2018, 231)

Tutkimuksen luotettavuutta ja pätevyyttä on kuitenkin jollain tavalla kyettävä arvioimaan myös kvalitatiivisessa tutkimuksessa ja Janesickin (2000, 393) mukaan ydinasioita laadullisessa tutkimuksessa ovat henkilöiden, paikkojen ja tapahtumien kuvaukset. Validiteetti merkitsee kuvausten ja siihen liitettyjen selitysten ja tulkintojen yhteensopivuutta. Laadullisessa tutkimuksessa luotettavuutta kohentaa tutkijan tarkka selostus tutkimuksen toteuttamisesta.

Tarkkuus koskee tutkimuksen kaikkia vaiheita. Aineiston tuottamisen olosuhteen tulisi kertoa selvästi ja totuudenmukaisesti koskien olosuhteita ja paikkoja, joissa aineisto kerättiin sekä siihen käytettyä aikaa, mahdollisia häiriötekijöitä, virhetulkintoja haastattelussa ja myös oma itsearviointi tilanteesta. (Hirsjärvi ym. 2018, 232)

Tämä työ on kvalitatiivinen tapaustutkimus ja sen vuoksi tutkimuksen reliabiliteetti on haastava todentaa. Tutkimuksen pätevyyttä haetaan runsaalla lähdeaineistolla ja haastattelujen olosuhteiden, teemojen ja tulosten kirjaamisella niin että lukija saa mahdollisimman tarkan kuvan tutkimuksen toteuttamisesta. Tarkkaa litterointia haastattelusta ei ole kuitenkaan tarkoituksenmukaista tehdä, vaan haastattelujen teemakohtaisilla yhteenvedoilla pyritään antamaan kokonaisvaltainen kuva kustakin teemasta.

Työn validiteetti tulee paljolti samoista lähtökohdista kuin työn reliabiliteetti. Valtiohallinnon toimintamallien kuvaamisen, tutkimuksen viitekehyksen ja tarkan kuvaamisen kautta lukija saa käsityksen miksi juuri nämä teemat ovat tärkeitä haastatteluissa selvittää, kun tutkitaan turvallisuuden johtamista Terveyden ja hyvinvoinnin laitoksen kontekstissa. Kirjoittaja on kuitenkin linjannut, että haastateltavia henkilöitä ei tässä työssä esitellä, eikä heidän vastauksiaan sellaisenaan kirjata tutkimuksiin. Haastateltavien lukumäärä ja tehtäväkenttä esitetään ja haastatteluista tehdään teemakohtaiset yhteenvedot. Toimintamalli tukee teemahaastattelun ajatusta, joka Ojasalon, Moilasen ja Ritalahden mukaan (2018, 41) sopii sellaisiin tilanteisiin, joissa ei täysin tunneta tutkimuksen kohdetta etukäteen, eikä haluta liikaa ohjata vastaajia. Teemahaastattelussa haastatteluteemat on suunniteltu huolellisesti etukäteen, mutta sanamuodot sekä kysymysten järjestys ja painotukset saattavat vaihdella haastattelun kesken.

2.2 Kokonaisvaltainen riskienhallinta ja turvallisuuden johtaminen

Työsuojeluhallinnon mukaan (Turvallisuusjohtaminen 2010, 5-6) turvallisuusjohtaminen on kokonaisvaltaista, niin lakisääteisen, kuin omaehtoisen turvallisuuden hallintaa, jossa yhdistyy sekä menetelmien ja toimintatapojen, että ihmisten johtaminen. Se sisältää ajatuksen jatkuvista toimista turvallisuuden ja terveellisyyden edistämiseksi työpaikalla. Turvallisuusjohtaminen pitää sisällään jatkuvan suunnittelun, toiminnan ja seurannan. Turvallisuusjohtamiseen on sekä johdon, että henkilöstön sitouduttava. Vasta henkilöstön sitoutuminen varmistaa, että turvallisuusjohtamisajattelu ja sen kautta tulevat toiminnot kehittävät turvallisuuskulttuuria. Riskienhallinta on osa turvallisuusjohtamista. Se on järjestelmällistä työtä toiminnan jatkuvuuden ja henkilöstön turvallisuuden varmistamiseksi. Riskienhallinta tarkoittaa kaikkea organisaatiossa tehtävää toimintaa riskien pienentämiseksi tai poistamiseksi. Käytännön työelämässä riskienhallinta on turvallisuusjohtamisen työväline.

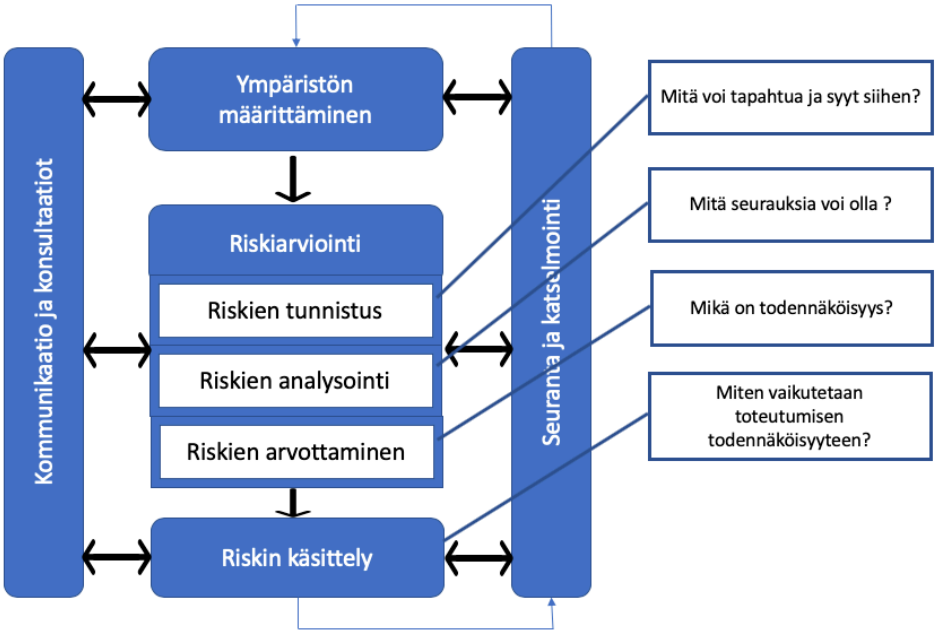
Organisaatiota johdetaan ja ohjataan riskienhallinnan avulla. Sen tulee olla kokonaisvaltaista sekä kattaa strategiset, taloudelliset, operatiiviset ja vahinkoriskit. Turvallisuusjohtaminen on osa riskienhallintaa. (Martikainen 2016, 13)

Turvallisuusjohtamisen ja riskienhallinnan suhteesta on siis kaksi eri näkemystä (Turvallisuusjohtaminen 2010, 5-6; Martikainen 2016, 13). Lanne muistuttaa väitöskirjassaan (Lanne 2007, 29), että kyseessä on kuitenkin enemminkin tarkastelunäkökulman valinta kuin hierarkkinen suhde. Organisaatioturvallisuuden johtamisen näkökulmasta katsottuna riskienhallinnan menettelytapoja ja käytänteitä (kuten riskien arviointi tai riskianalyysi) voidaan hyödyntää yhtenä johtamisen välineenä.

Kirjoittaja on tässä työssä useassa kohdassa linjannut, että riskienhallinnan johtaminen on laajempi kokonaisuus ja turvallisuusjohtaminen on sen osajoukko ja noudattelee Martikaisen näkemystä. Ilmosen ym. (2016, 46-47) kokonaisvaltainen riskienhallinta lähtee yrityksen arvoista ja strategiasta ja on systemaattinen tapa hallita kaikki yrityksen riskejä ja siitä on tullut modernin yrityksen johdon työkalu. He syventävät kokonaisvaltaista riskienhallintaa johtamisen välineenä vielä mainitsemalla, että hyvän käytännön mukaan se on prosessi, jota suorittavat ylin johto (hallitus), toimiva johto (johtoryhmä) sekä kaikki työntekijät ja että sitä toteutetaan kaikissa yrityksen prosesseissa ja kaikilla organisaation tasoilla.

Tässä työssä käytetään käsitettä turvallisuuden johtaminen kuvaamaan toimintamallia, jossa turvallisuus ja johtaminen on kokonaisvaltaista. Kirjoittaja on määritellyt turvallisuuden johtamisen tarkoittavan laajaa kokonaisuutta, joka käsittää turvallisuusjohtamisen, riskienhallinnan, ihmisten johtamisen ja muut toiminnot, jolla turvataan organisaation strategiset ja operatiiviset toiminnot normaalioloissa ja normaaliolojen häiriötilanteissa sekä poikkeusoloissa.

Riskienhallinnan standardina toimii SFS-ISO 31000 ja siinä määritellään riskienhallinta prosessi. Riskikompassi esittää sen alla olevan kuvion perusteella. Sama kuvio on kappaleessa Riskienhallinta prosessi, mutta tässä kuvaan on lisätty selittäviä elementtejä, jotka selkeyttävät vaiheiden tarkoitusta.



Kuvio 1: Riskien hallintaprosessi (Nylander 2017, 144)

Riskien arvioimiseksi ne tulee ensin tunnistaa. Tunnistaminen tapahtuu arvioimalla mitä negatiivisia tapahtumia on mahdollista sattua organisaation ympäristössä ja mikä niitä voi aiheuttaa. Kun riski(t) on tunnistettu, jatketaan pohtimista sillä, mitä seurauksia kyseisen tapahtuman johdosta voi ympäristössä tapahtua, mikäli se tapahtuu. Seuraavassa vaiheessa mietitään mikä on todennäköisyys tälle tapahtumalle. Tästä muodostuu riskiarviointi, jonka seurauksena on riskin käsittelyn vaihe. Siinä mietitään, mitä riskille voitaisiin tehdä.

Ilmonen, Kallio, Koskinen ja Rajamäki (2016, 33) määrittelee SFS-ISO 31000 standardin mukaiset periaatteet, joiden mukaan riskienhallinta

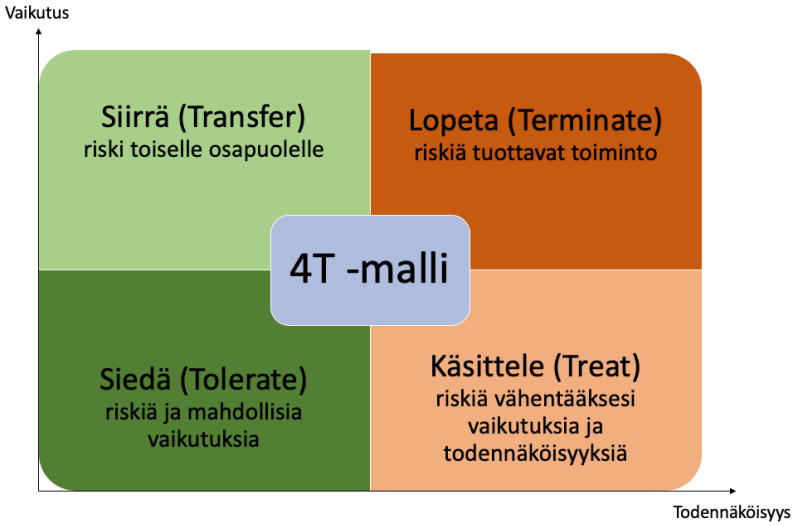
- luo lisäarvoa ja säilyttää sen
- on olennainen osa kaikkia organisaation prosesseja
- on osa päätöksentekoa
- pitää lähtökohtana epävarmuuden huomioon ottamista
- on järjestelmällistä, jäsenneltyä ja ajantasaista
- perustuu parhaaseen saatavilla olevaan tietoon
- toteutetaan organisaation tarpeiden mukaan
- ottaa inhimilliset ja kulttuuriset tekijät huomioon
- on avointa ja kattavaa
- on dynaamista, toistuvaa ja muutoksiin reagoivaa
- tukee organisaation jatkuvaa kehittämistä

Nylander (2017, 144) on määritellyt seuraavat riskikompassin mukaiset päävaiheet riskien hallintaprosessille:

1. Riskien tunnistaminen
2. Riskien arviointi
3. Riskien hallinnan suunnitelma ja tarvittavat toimenpiteet
4. Toimintasuunnitelma vahingon sattuessa ja toipumissuunnitelma vahingosta
5. Tilanteen ja toimenpiteiden vaikutusten seuranta ja tarvittaessa raportointi yrityksen ylimmälle johdolle riskitilanteesta, erityisesti merkittävistä riskeistä
6. Toteutuneista riskitapahtumista oppiminen

Riskienhallinnan merkitys organisaation johtamisessa on keskeinen. Tuomalla mukaan systemaattisen riskienhallinnan organisaation tavoitteiden saavuttamista ja strategian toteutumista kyetään tukemaan ihan eri tavalla. Riskit ja niiden hallinta liittyvät olennaisesti organisaation toiminnan johtamiseen, sillä toimintaan liittyy aina riskejä, on sitten kyse mahdollisuuksien hyödyntämisestä tai uhkien torjunnasta. (Riskikompassi 2020)

Riskien käsittelyssä käytetään yleisesti mm. Hopkinin esittelemää 4T -mallia, jossa tunnistetun riskin käsittelylle on neljä vaihtoehtoista tapaa.



Kuvio 2: Riskimatriisi ja vahingonhallinnan 4T -malli (Hopkin 2018, 175)

- Riskin siirtäminen voi tapahtua vakuuttamalla tai maksamalla kolmannelle osapuolelle siitä, että se ottaa riskin kantaakseen. Tämä vaihtoehto sopii erityisesti talousriskien ja arvo-omaisuuteen kohdistuvien riskien, mutta myös henkilöriskien hallintaan.
- Riskin sietäminen tarkoittaa, että ollaan valmiita hyväksymään tunnistetun riskin jäännösriski tai että riski on sellainen, jolle ei voi tehdä mitään ja siksi se vaan täytyy

sietää. Tähän kuuluvat myös riskit, joiden käsittely tulee kalliimmaksi, kuin niiden sietäminen ja siksi sille ei kannata tehdä mitään.

- Toiminnan lopettaminen koskee tunnistettuja riskejä, joita ei voida muulla tavalla käsitellä tai joita ei ole mahdollista vähentää hyväksyttävälle tasolle. On huomattava, että toiminnan päättäminen ei aina ole mahdollista valtiohallinnossa tai yleisesti julkisella, toisin kuin yksityisellä sektorilla.
- Suurin osa riskeistä voidaan jollain tavalla käsitellä ja siten hallita. Tällöin tunnistetulle riskille tehdään käsittely, jolla riski saadaan siedettävälle tasolle tai poistettua kokonaan. (SFS-ISO 31000 standardi käsittelee tätä kohtaa)

Turvallisuusjohtamista toteutetaan riskienhallinnan, turvallisuusdokumentoinnin ja -koulutuksen, proaktiivisen viestinnän, kriisiviestinnän, kiinteistö- ja turvallisuustekniikan, lainsäädännön seurannan ja vaatimusten täyttymisen sekä hallinnollisen johtamisen kautta. Turvallisuusjohtamisen toteutumista myös seurataan, mitataan, analysoidaan ja kehitetään. (Keskiuudenmaan pelastuslaitos 2012)

Riskienhallinta liittyy ihmisen kokemaan turvallisuuteen. Turvallisuuttaa voidaan tarkastella muun muassa henkilökohtaisella, kansallisella tai kansainvälisellä tasolla. Nykyisin yhä useammin turvallisuus käsitetään laajana ilmiönä, joka kattaa myös yksilötason inhimillisen turvallisuuden. Tämä tarkoittaa arjen tai perustarpeiden turvallisuutta, kuten ihmisoikeuksien toteutumista kansalaisuudesta tai valtiosta riippumatta. (Heinonen, Keinänen & Paasonen 2013, 7)

Riskienhallinnan johtamisen tarkoitus on helpottaa ja luoda puitteet velvollisuuksille ja vastuille tehokkaasta ja tuloksellisesta toiminnasta ja eettisestä käytöksestä. Sen pitäisi luoda turvallisuutta johtajille ja työntekijöille heidän työssään ja viimeiseksi sen pitäisi vakuuttaa sidosryhmät siitä, että organisaatio kykenee saavuttamaan arvoa, jota nämä tahot siltä odottavat. (Hopkin 2018, 333)

Elämme bittien keskellä tai paremminkin bittien vaikutuksen alaisena, jokainen meistä, joka päivä. Digitaalinen maailman tuo meille mahdollisuuksia, nautintoa ja helpottaa elämää ja samalla luotamme siihen, että bittien maailma on turvallinen. Kybermaailmasta ja kyberturvallisuudesta on tullut erottamaton osa arkipäiväämme. Maailmantalous, yhteiskuntien turvallisuus, yritysten toiminta ja elämäntapamme ovat tänä päivänä hyvin riippuvaisia bittien toimivuudesta. Megatrendi maailmassa on, että riippuvuutemme bittien turvallisesta toiminnasta lisääntyy kiihtyvällä tahdilla. Tämä avaa meille yhä upeampia mahdollisuuksia hyödyntää maantieteellisesti ja ajallisesti rajatonta digitaalista maailmaa, mutta samalla riippuvuuden kääntöpuoli eli haavoittuvuus lisääntyy. Turvallisuus on ihmisten, yritysten, yhteiskuntien ja valtioiden perustarve. Hyvin moni inhimillinen toiminta on selitettävissä turvallisuuden tavoittelun tai turvattomuuden kokemisen kautta. Bittien ottaessa yhä enemmän valtaa fyysisestä atomien maailmasta meidän on pakko kiinnittää enemmän huomiota kybermaailman

turvallisuuteen. Kybermaailma ei ole pienen asiantuntijajoukon juttu, vaan se koskettaa läheisesti meitä kaikkia, ja meistä jokainen on siitä myös vastuussa. (Limnéll, Majewski, Salminen 2014, 13)

Kun riskienhallinta integroidaan kaikkiin johtamisprosesseihin, se helpottaa keskittymistä olennaiseen. Yritystoiminnan perimmäisen tarkoituksen voi pelkistää maksimaalisen voiton tavoittelemiseksi pienimmällä mahdollisella panostuksella. Riskienhallinnankaan tarkoitus ei ole pyrkiä hallitsemaan kaikki tunnistettuja riskejä samalla tavalla. Niin liiketoimintamahdollisuuksien kuin riskienkin analysoinnin tarkoitus on oikeastaan auttaa löytämään ne positiiviset ja negatiiviset asiat, joihin panostaminen tuo yritykselle liiketoimintaa (positiivinen) tai johtaa onnettomuuksiin ja vahinkoihin (negatiivinen).

2.2.1 Riski käsitteenä

Riski voidaan määritellä monin eri tavoin. Kirjassa ”Fundamentals of Risk Management” (Hopkin 2018, 15) käytetään Oxfordin sanakirjaa, joka määrittelee riskin olevan mahdollisuus vaaralle, menetykselle, onnettomuudelle tai jollekin haitalliselle tapahtumalle ja että riski on jotain, joka altistaa vaaralle. Riski nähdään tässä yhteydessä aiheuttavan aina negatiivisia seurauksia. Riskin ottaminen voi kuitenkin johtaa myös positiivisiin seurauksiin ja kolmantena mahdollisuutena on, että riskin ottaminen johtaa epävarmoihin seurauksiin.

Kokonaisturvallisuuden sanasto (2017, 41) määrittelee riskin olevan kielteisen seikan tai tapahtuman todennäköisyyden ja vaikutusten yhdistelmä. Riski lasketaan tapahtuman todennäköisyyden (t) ja vaikutuksen (v) tulona (riski = t * v). Riskit voivat kohdistua esimerkiksi ihmisiin, eläimiin, omaisuuteen, tietojärjestelmiin, ympäristöön tai yhteisöllisiin arvoihin.
Riski eroaa arkikielessä yleisemmin käytetyistä sanoista kuten vaarasta ja uhkasta siten, että vaara on hyvin todennäköisesti toteutuva tai jo toteutunut, parhaillaan vaikuttava haitallinen tapahtuma tai kehityskulku ja uhka taas mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku. Uhka eroaa vaarasta siten, että uhka on epävarmempi kehityskulku ja vaara puolestaan käytännöllinen ja riskienhallinnallisin toimenpitein käsiteltävä asia.

SFS-ISO 31000 standardissa (2018) riskin määritellään olevan epävarmuuden vaikutus tavoitteisiin ja tarkennetaan, että vaikutus on poikkeama odotetusta. Se voi olla myönteinen, kielteinen tai molempia, ja se voi käsitellä, luoda tai saada aikaan mahdollisuuksia ja uhkia. Lisäksi tarkennetaan, että tavoitteilla voi olla eri näkökohtia ja luokkia, ja niitä voidaan soveltaa eri tasoihin. Riski voidaan standardin mukaan ilmaista tavallisesti riskin lähteiden, mahdollisten tapahtumien, niiden seurausten ja niiden todennäköisyyden yhdistelmänä.

IRM (Institute of Risk Management) määrittelee riskin olevan yhdistelmä tapahtuman todennäköisyydestä ja sen seurauksista. Tämä määritelmä perustuu standardiin ISO/IEC Guide 73.

Kaikentyyppisissä organisaatioissa on potentiaalinen mahdollisuus tapahtumiin, joilla on seurauksena hyötyjä tai uhkia menestykselle. (IRM 2002, 2)

Hopkinin (2018, 17) mukaan riskit voidaan jakaa neljään kategoriaan

- Säännösten laiminlyöntiin liittyvät riskit (compliance or mandatory risks)
- Onnettomuuden tai sattuman aiheuttamat riskit (hazard or pure risks)
- Epävarmuuden aiheuttamat riskit (control or uncertainty risks)
- Mahdollisuuksia sisältävät riskit (opportunity or speculative risks).

Yleisesti ottaen organisaatiot etsivät keinoja minimoida säännöksiin liittyvät, vähentää onnettomuuksien aiheuttamia riskejä, hallinnoida epävarmuuden aiheuttamia riskejä ja tarttua mahdollisuuksia sisältäviin riskeihin.

Kirjallisuudessa näyttää eniten käytettävän SFS-ISO 31000 standardin määritelmää riskistä eli että se on epävarmuuden vaikutus tavoitteisiin. Riskiä ajatellessa ja riskejä otettaessa organisaatiossa on hyvä muistaa, että standardin tarkoittamat epävarmuudet voivat olla negatiivisia, mutta myös positiivisia. On hyvä muistaa, että liiketoimintaa ei synny ilman riskin ottamista, siksi puhtaasti negatiivisilta riskeiltä suojaava lähestymistapa ei hyödynnä riskienhallinnan kokonaisvaltaisia mahdollisuuksia. (Ilmonen ym. 2016, 16)

Ilmonen ym. (2016, 77) nostavat Hopkinin (2018, 17) tavoin esiin myöskin neljä (negatiivista) riskilajia, jotka ovat strategiset riskit, taloudelliset riskit, operatiiviset riskit ja siihen liittyvät projektiriskit sekä vahinkoriskit. Ilmonen muistuttaa kuitenkin, että vaikka nämä ovat lähtökohtaisesti negatiivisia riskejä, voi tavoitteiden saavuttamiseen liittyvän epävarmuuden ymmärtää myös positiivisena mahdollisuutena eli minkä epävarmuuden tulisi toteutua, jotta se tukisi tavoitteen saavuttamista.

- Strategiset riskit liittyvät organisaation pitkän aikavälin strategisiin tavoitteisiin.
- Operatiiviset riskit ovat organisaation päivittäisiin toimintoihin liittyviä välittömien tai välillisten vahinkojen tai maineen riskejä, jotka voivat seurata yrityksen riittämättömistä tai epäonnistuneista sisäisistä prosesseita, henkilöstöstä, järjestelmistä tai ulkoisista tapahtumista
    - Projektiriskit tulevat nykyisin yleistyneestä projektimuotoisesta työskentelystä, jossa yleisiä riskejä ovat aikataulun ja budjetin ylittyminen. Riskit voivat liittyä myös projektin kohteeseen, tavoitteisiin, laatuun tai ulkoisiin tekijöihin, kuten rahoitukseen, markkinatilanteen muutoksiin tai sopimuksiin
- Taloudelliset riskit liittyvät monenlaisiin yrityksen rahaprosessia uhkaaviin riskeihin
- Vahinkoriskit ovat esimerkiksi henkilöstön työkyvyttömyyteen tai työtapaturmiin liittyvät riskit. Henkilöturvallisuuteen liittyviä vahinkoriskejä ovat mm. työvoiman puutteeseen tai riittämättömään osaamiseen liittyvät riskit, toistuvat poissaolot,

ulkomaan matkoihin liittyvät riskit, avainhenkilöiden menettämiseen tai epälojaalisuudesta työnantajaa kohtaan aiheutuvat vahinkoriskit. Tähän ryhmään kuuluu myös erilaiset ympäristöriskit, jotka voivat liittyä saastuttamiseen, työperäisiin sairauksiin, niiden tartuttamiseen, vaarallisten aineiden käsittelyn riskit ja epäonnistuminen organisaation ympäristövastuun hoitamisessa.

2.2.2 Riskienhallinta käsitteenä

Kokonaisturvallisuuden sanasto (TSK 2017, 50) määrittelee riskienhallinnan olevan järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet. Varautumisessa riskienhallinta on useiden eri tahojen yhteistyötä. Sitä tekevät sekä yritykset, eri toimialat ja viranomaiset, kunnat ja valtio. Viranomaisilla ja joillain yrityksillä on lakisääteinen velvollisuus laatia valmiussuunnitelmia, johon riskienhallinta kuuluu tärkeänä osana. Riskienhallintaan kuuluu myös riittävien resurssien määrittäminen. Riskienhallinnan keinoja ovat riskin välttäminen, siirtäminen, pienentäminen jakamalla ja vahingontorjunnalla sekä riskin ottaminen.

Riskienhallinnalla tarkoitetaan menettelyjä, joilla tunnistetaan, arvioidaan ja hallitaan tavoitteiden saavuttamista heikentäviä uhkia, jotka ovat kielteisiä ja epäedullisia sekä niiden todennäköisyyksiä ja avautuneiden mahdollisuuksien menettämistä ja uhkaavat organisaation tavoitteita. (VM 2005, 11; Ilmonen ym. 2016; Turpeinen 2017, 9)

Paul Hopkinin (2018, 55) mukaan riskienhallinnan (engl. Risk Management) pääperiaate on, että se tuottaa arvoa organisaatiolle, toisin sanoen riskienhallinnan toimenpiteet on suunniteltu siten, että ne tuottavat parhaan mahdollisen lopputuleman ja vähentävät ailahtelevaisuutta tai epävarmuutta tässä lopputulemassa.

SFS-ISO 31000 (2018) standardi määrittelee riskienhallinnan olevan koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta. (SFS-ISO 31000, 6). Tässä korostuu se, että riskienhallinnan tulee olla osa organisaation johtamisjärjestelmää. Samaa korostaa myös IRM standardi (2002) sanomalla, että riskienhallinta on osa organisaation strategista johtamista ja että se on prosessi, jolla organisaatiot käsittelevät metodologisesti eli järjestelmällisesti siihen liittyviä riskejä, saavuttaakseen tavoitteeksi asettamansa hyödyn erityisissä toiminnoissa ja kaikessa toiminnassa, johon organisaatio osallistuu. (IRM 2002, 2)

COSO-ERM riskienhallinnan viitekehyksen Executive Summary (2017) korostaa riskienhallinnan saralla organisaation resilienssiä eli kyvykkyyttä olla joustava ja sopeutuva muutoksiin. Organisaation pitää strategisella tasolla miettiä miten hallita ja johtaa kasvavaa maailman ailahtelevaisuutta, monimutkaisuutta ja moniselitteisyyttä, erityisesti yrityksiä, joilla on pitkä ja menestynyt historia ja panokset ovat korkeat. (COSO-ERM 2017).

Riskienhallinnan tavoite on tukea päätöksentekoa yrityksessä (tai organisaatiossa yleensä) siten, että yrityksen johto voisi tehdä merkittävät liiketoimintapäätöksensä tietoisena siitä, mikä on yrityksen riskikuva eli yrityksen merkittävimpien riskien kokonaisuus ennen päätöksen tekemistä ja miten tehtävä päätös todennäköisesti muuttaa yrityksen riskikuvaa. Päätöksen jälkeen riskienhallinnan tavoitteena on tukea päätöksen toimeenpanoa niin, että tavoite myös saavutetaan ja jopa ylitetään. (Ilmonen ym. 2016, 10)

Riskienhallinnan käsite voitaisiin tiivistää toteamalla, että se on organisaation strategian mukainen arvoa tuottava johtamisjärjestelmään integroitu johdon työkalu, jolla tuotetaan järjestelmällistä toimintaa, jossa tunnistetaan, arvioidaan ja hallitaan tavoitteita uhkaavia riskejä sekä organisaation jatkuvasti päivittyvä riskikuva, jolla tuetaan päätöksentekoa.

Nyt kun eletään vuotta 2020, joka tulee jäämään historiaan koronavuotena, ollaan nähty miten monet yritykset ovat oppineet joustamaan ja muuttamaan strategiaansa nopeasti tai sitten ovat joutuneet ennennäkemättömiin vaikeuksiin. Riskienhallinta osana johtamisjärjestelmää on saanut aivan uuden merkityksen.

2.2.3 Riskienhallinnan standardi SFS-ISO 31000

Standardi SFS-ISO 31000 auttaa organisaatiota luomaan riskienhallinnan puitteet, joiden avulla voidaan tehokkaasti tunnista, arvioida ja käsitellä riskien vaikutusta organisaation tavoitteiden saavuttamiseen. Standardin tavoitteena on luoda organisaation riskienhallinnan kulttuuri, jossa henkilöstö ja sidosryhmät ovat tietoisia riskien seurannan ja hallinnan merkityksestä. (SFS-ISO 31000)

SFS-ISO 31000 on standardointiorganisaation ISO (International Organization for Standardization) julkaisema standardi, joka antaa selkeän rakenteen organisaation riskienhallinnan kehittämiseen. Standardissa riskienhallinta jaetaan kolmeen pääkohtaan:

1. Riskienhallinnan periaatteet
   Tarkoittaa organisaation johdon päättämiä riskienhallintaan liittyviä periaatteita ja tavoitteita, jotka on kuvattu ”Riskienhallintapolitiikka” tai ”Riskienhallinnan periaatteet" dokumentissa.
2. Riskienhallinnan puitteet
   Koostuvat osatekijöistä, jotka yhdessä muodostavat organisaation riskienhallinnan suunnittelun, toteutuksen, seurannan, katselmoinnin ja jatkuvan kehittämisen perustan ja organisoinnin.
3. Riskienhallinnan prosessi
   Sisältää hallintaperiaatteiden, menettelyjen ja -käytäntöjen järjestelmällisen soveltamisen viestintään ja tiedonvaihtoon sidosryhmien kanssa, toimintaympäristön

määrittelemiseen liittyviin toimintoihin sekä riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan ja katselmointiin.)

SFS-ISO 31000 -standardi on kaupallinen kansainvälinen riskienhallinnan malli, joka soveltuu sellaisenaan riskienhallinnan viitekehykseksi tai sillä voidaan täydentää muiden ISO-hallintajärjestelmästandardien (mm. SFS-ISO 9000 Laadunhallinta, SFS-ISO 14000 Ympäristöjohtaminen, SFS-ISO 26000 Yhteiskuntavastuu, SFS-ISO 27000 Tietoturvallisuuden hallinta, SFS-ISO 55000 Omaisuudenhallinta, OHSAS 18001 Työterveys- ja työturvallisuusjohtaminen ym.) vaatimustenmukaisuutta.

SFS-ISO 31000 standardin (2018) johdannossa sanotaan, että standardi on tarkoitettu käyttäjille, jotka luovat ja säilyttävät arvoa organisaatiossa hallitsemalla riskejä, tekemällä päätöksiä, asettamalla ja saavuttamalla tavoitteita ja parantamalla suorituskykyä.

Standardin johdanto sitoo riskienhallinnan johtamiseen sanomalla. että riskienhallinta on osa hallintotapaa ja johtajuutta, ja se on keskeinen tekijä siinä, kuinka organisaatiota johdetaan kaikilla tasoilla. Riskienhallinta edesauttaa johtamisjärjestelmä kehittämistä. Riskienhallinta on osa kaikkia organisaatioon liittyviä toimintoja, ja se kattaa myös vuorovaikutuksen organisaation sidosryhmien kanssa. (SFS-ISO 31000)

SFS-ISO 31000 standardissa (2018) annettuja ohjeita sovelletaan organisaatioiden kohtaamien riskien hallintaan. Ohjeita voidaan soveltaa organisaatioon ja sen toimintaympäristöön sopivalla tavalla. Standardissa esitetään kaiken tyyppisten riskien hallintaan soveltuva yleinen toimintamalli, jota voidaan hyödyntää kaikilla toimialoilla. Standardia voidaan käyttää organisaation elinkaaren kaikissa vaiheissa, ja sitä voidaan soveltaa kaikkiin toimintoihin, myös päätöksentekoon organisaation kaikilla tasoilla.

Muita riskienhallinnan standardeja ja hyviä käytänteitä on esitetty liitteessä 4.

2.3 Riskienhallinta turvallisuusjohtamisen kontekstissa

Riskienhallinnan englanninkielinen termi ”Risk Management” kertoo, että riskienhallinnalla tarkoitetaan riskien johtamista. Riskienhallinnan tulee olla osa johtamisjärjestelmää ja se on yksi tärkeimmistä johtamisen työvälineistä. Kokonaisvaltaisesta riskienhallinnasta onkin tullut keskeinen osa nykypäivän johtamisjärjestelmää, kun organisaatio mukautuu jatkuvasti muuttuvan toimintaympäristön tuomiin haasteisiin. Riskienhallinnan todellinen arvo nähdään vasta silloin, kun se on jalkautettu organisaatioon ja tullut osaksi organisaation jokapäiväistä operatiivista toimintaa. Jalkauttamisesta koordinoi turvallisuudesta vastaava organisaatio, joka toimii riskienhallinnan ytimessä. Voidaankin sanoa, että riskienhallinta on koko organisaation yhteinen asia, jota johtaa ylin johto ja sitä koordinoi turvallisuusorganisaatio.

Organisaation johtamiseen liittyvä riskienhallinta korostuu Turpeisen (2017, 9) ja Ilmosen ym. (2016, 16-17) määrittelyissä, jossa riskienhallinnalla tarkoitetaan menettelyjä, joilla tunnistetaan, arvioidaan ja hallitaan tavoitteiden saavuttamista heikentäviä uhkia, jotka ovat kielteisiä ja epäedullisia sekä niiden todennäköisyyksiä ja niiden kautta avautuneiden mahdollisuuksien menettämistä. Organisaation johto on vastuussa tavoitteiden asettamisesta ja niiden saavuttamisesta sekä mahdollisuuksien hyödyntämisestä.

Valtiovarainministeriön julkaisussa (VM 2017a, 11) painotetaan, että riskienhallinnan tarkoituksena on mahdollistaa organisaation menestyminen, toiminnan jatkuvuuden takaaminen ja tavoitteiden saavuttaminen. Riskienhallinta on julkaisun mukaan järjestelmällistä ja tavoitteellista toimintaa, jolla tuetaan lisäksi organisaation johtamista ja kehittymistä. Usein sanaa riski käytetään uhka -sanan synonyyminä, mutta pohjimmiltaan riski voi olla myös positiivinen asia, mahdollisuus saada hyötyä jollain toimenpiteellä. Riskienhallinnan tarkoituksena on löytää organisaation menestymiseen ja tuloksellisuuteen sekä henkilöstön hyvinvointiin vaikuttavat tekijät.

Ilmonen ym. (2016, 16) nostaa myös esiin riskin positiivisen puolen toteamalla, ettei liiketoimintaa ole ilman riskin ottamista. Sen vuoksi puhtaasti negatiivisilta riskeiltä suojaava lähestymistapa ei ota kokonaisvaltaisesti hyötyä riskienhallinnan mahdollisuuksista. Laajasti ymmärrettynä riski ja riskienhallinta kattavat myös mahdollisuudet ja niiden tunnistamisen, arvioinnin ja hallinnan. SFS-ISO 31000 standardin määritellessä riskin olevan epävarmuuden vaikutus tavoitteisiin, unohdetaan usein, että standardin tarkoittamat epävarmuudet voivat olla sekä negatiivisia, että positiivisia.

Ilmonen ym. (2016, 14) muistuttaa myös, että johdon tehtävä on varmistaa, että riskienhallintajärjestelmä on olemassa ja että se on mahdollisimman toimiva ja systemaattinen ja että sitä kehitetään jatkuvasti. Riskienhallintajärjestelmän on otettava huomioon kaikki riskit, myös sellaiset, jotka eivät ole oikeastaan kenenkään hallittavissa yrityksessä. Nekin pitää huomioida, niitä pitää tarkkailla ja keskeisimpien riskien varalle pitää tehdä jatkuvaa suunnittelua, joka on johdon vastuulla.

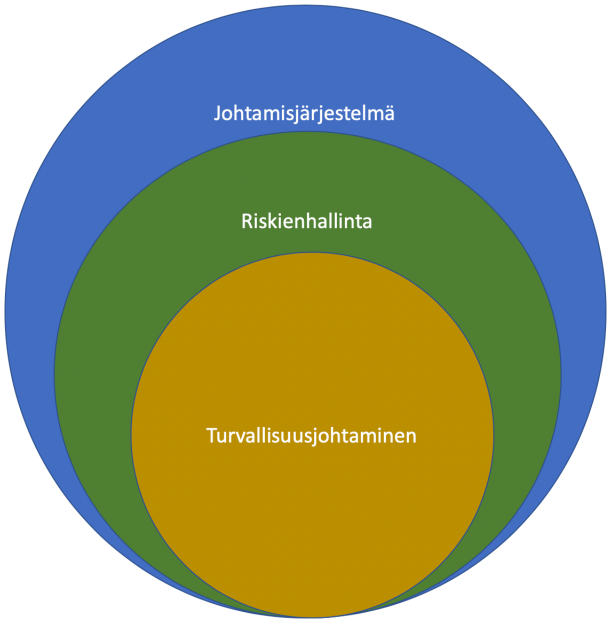
Valtiovarainministeriön julkaisu (VM 2017a, 12) sitoo riskienhallinnan johtamiseen toteamalla riskienhallinnan oleva osa johtamisen ja toiminnan prosesseja sekä suunnittelua ja seurantaa. Julkaisun mukaan tavoitteena on, että organisaatiolla on johtamista ja päätöksentekoa varten ajantasainen, oikea ja riittävän kattava käsitys sekä selkeästi määritellyt riskienhallinnan vastuut ja seurantajärjestelmä. Riskienhallinta ei koske vain johtamista, vaan organisaation jokaista työntekijää. Se voi tarkoittaa esimerkiksi normaalista toiminnasta poikkeavien havaintojen ilmoittamista omalle esimiehelle tai kirjaamista niitä riskienhallintajärjestelmään.

Sisäinen valvonta ja riskienhallinta liittyvät läheisesti yhteen. Sisäinen valvonta huolehtii myös riskienhallinnan asianmukaisuudesta. Vahti -ohjeen (2016) mukaan sisäisen valvonnan

avulla varmistetaan talouden ja toiminnan laillisuus ja tuloksellisuus sekä varojen ja omaisuuden turvaaminen. Johto vastaa sisäisen valvonnan asianmukaisuudesta. Sisäinen tarkastus arvioi sisäisen valvonnan ja riskienhallinnan asianmukaisuutta ja riittävyyttä. (VM 2016). Sisäisen valvonnan ja riskienhallinnan neuvottelukunta on valmistellut valtiohallinnon riskienhallintapolitiikkamallin, josta valtiovarain controller -toiminto on antanut suosituksen 3.5.2017, jossa sanotaan, että riskienhallinta on osa sisäistä valvontaa ja siten jokaisen valtion viraston lakisääteinen tehtävä. Sisäisen valvonnan järjestämisestä säädetään valtion talousarviosta annetussa laissa (L423/1988). Sisäisestä valvonnasta ja riskienhallinnasta on tarkempia säännöksiä talousarvioasetuksessa (L1243/1992). (VM 2017c)

Kokonaisvaltainen, riskiperusteinen turvallisuusjohtaminen pohjautuu riskienhallintaan, jatkuvaan parantamiseen ja elinkeinoelämän keskusliiton (EK) organisaatioturvallisuuden malliin (Martikainen 2016, 13-14). Turvallisuusjohtaminen on kiinteä osa organisaation järjestelmällistä johtamista, jonka tavoitteena on ihmisten, ympäristön, omaisuuden, tiedon ja maineen suojaaminen. (EK yritysturvallisuus 2016)

Turvallisuusjohtamisen ja riskienhallinnan suhdetta koko organisaation johtamiseen voidaan kuvata seuraavalla kaaviolla.



Kuvio 3: Turvallisuusjohtamisen, riskienhallinnan ja johtamisjärjestelmän keskinäiset suhteet (Virta 2014, 11)

Turvallisuusjohtaminen perustuu riskienhallinnan kautta määritellyille toimenpiteille. Organisaation ylin johto on aina kokonaisvastuussa riskienhallinnasta ja riskienhallina on kiinteä osa organisaation johtamisjärjestelmää. Turvallisuusorganisaatio on koordinoiva toimija, joka toteuttaa riskienhallinnan jalkauttamisen ohjeistuksen ja koulutuksen kautta koko henkilöstölle

ja huolehtii tietoon, maineeseen, omaisuuteen, ympäristöön, henkilökuntaan ja asiakkaisiin kohdistuvien vahingoittavien tapahtumien ennaltaehkäisystä. Ilman kokonaisvaltaista riskienhallintaa tämä ei olisi mahdollista. Riskienhallinta luo perustan turvallisuusjohtamiselle ja siksi se tässäkin työssä on keskeisessä roolissa.

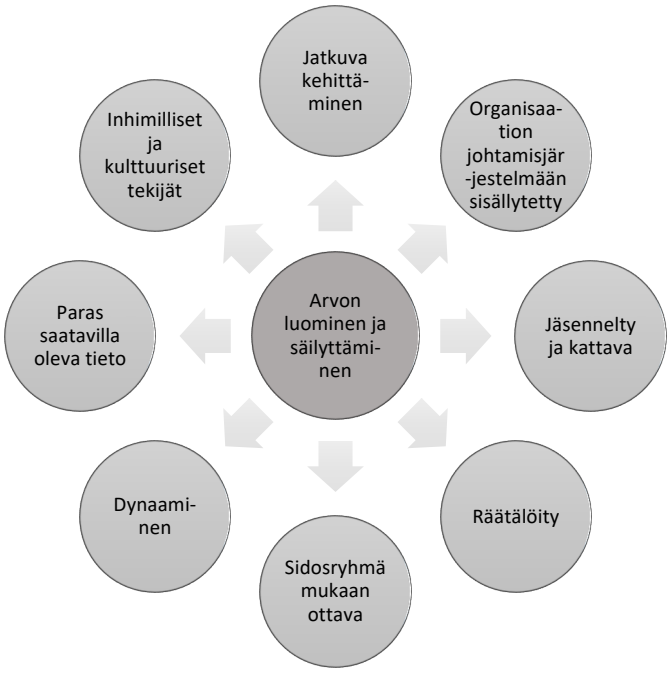
Riskienhallinnan periaatteiden, puitteiden ja prosessien kuvaaminen perustuu pääosin SFS-ISO 31000 stardardiin. Seuraavassa on avattu näitä käsitteitä ja määritelty standardiin pohjautuen, miten ne liittyvät organisaation turvallisuuden johtamiseen.

2.3.1 Riskienhallinnan periaatteet

Riskienhallinnan tarkoitus on arvon luominen ja säilyttäminen. Se parantaa suorituskykyä ja tukee innovointia ja tavoitteiden saavuttamista. (SFS-ISO 31000)

Riskienhallinnan periaatteilla voidaan tarkoittaa myös riskienhallintapolitiikkaa, mutta tässä yhteydessä tarkoitetaan nimenomaan SFS-ISO 31000 standardissa (2018) määriteltyjä periaatteita, jotka kuvaavat vaikuttavan ja tehokkaan riskienhallinnan ominaisuuksia, viestivät sen arvosta ja esittävät sen tavoitteet ja tarkoituksen. Nämä periaatteet ovat perustana riskienhallinnalle, ja ne olisi otettava huomioon, kun määritellään organisaation riskienhallinnan puitteita ja prosesseja. Näiden periaatteiden avulla organisaation pitäisi kyetä hallitsemaan epävarmuuden vaikutusta organisaation tavoitteisiin.

Vaikuttavaan riskienhallintaa tarvitaan seuraavan kuvan osatekijöitä.



Kuvio 4: Riskienhallinnan periaatteet. (Muokattu lähteestä SFS-ISO 31000, 8)

Riskienhallinnan periaatteet kuvaavat vaikuttavan ja tehokkaan riskienhallinnan ominaisuuksia, viestivät sen arvosta ja esittävät sen tavoitteet ja tarkoituksen. Nämä periaatteet ovat perustana riskienhallinnalle, ja ne olisi otettava huomioon, kun määritellään organisaation riskienhallinnan puitteita ja prosesseja. Näiden periaatteiden avulla organisaation pitäisi kyetä hallitsemaan epävarmuuden vaikutusta organisaation tavoitteisiin. (SFS 31000)

Riskienhallinnan periaatteiden käsitteiden sisältö kuvataan tarkemmin seuraavassa taulukossa

Organisaation johtamisjärjestelmään sisällytetty	Riskienhallinta on olennainen osa kaikkia organisaation toimintoja.
Jäsennelty ja kattava	Jäsennelty ja kattava toimintamalli tekee tuloksista yhdenmukaisempia ja vertailukelpoisempia.
Räätälöity	Riskienhallinnan puitteet ja prosessi sovitetaan organisaation tavoitteisiin liittyvään ulkoiseen ja sisäiseen toimintaympäristöön sopiviksi.
Sidosryhmät mukaan ottava	Sidosryhmien ottaminen sopivalla tavalla ja oikeaan aikaan mukaan riskienhallintaan mahdollistaa sidosryhmien tietämyksen, näkemysten ja havaintojen huomioon ottamisen. Näin lisätään tietoisuutta riskienhallinnasta ja varmistetaan parhaimpaan saatavilla olevaan tietoon perustuva riskienhallinta.
Dynaaminen	Riskejä voi ilmaantua ja ne voivat muuttua tai hävitä organisaation sisäisen ja ulkoisen toimintaympäristön muuttuessa. Riskienhallinnan avulla ennakoidaan, havaitaan ja varmistetaan muutokset ja tapahtumat sekä reagoidaan niihin sopivalla tavalla ja oikeaan aikaan.
Paras saatavilla oleva tieto	Riskienhallinnan lähtötiedot perustuvat historiatietoihin ja nykyisiin tietoihin, sekä tulevaisuutta koskeviin odotuksiin. Riskienhallinnassa otetaan huomioon myös tällaisiin tietoihin ja odotuksiin liittyvät rajoitukset ja epävarmuudet. Tietojen olisi oltava oikea-aikaisia, selkeitä ja olennaisten sidosryhmien saatavilla.
Inhimilliset ja kulttuuriset tekijät	Ihmisten käyttäytyminen ja kulttuuri vaikuttavat merkittävästi kaikkiin riskienhallinnan näkökohtiin kaikilla tasoilla.
Jatkuva kehittäminen	Riskienhallintaa kehitetään jatkuvasti oppimisen ja kokemusten myötä.

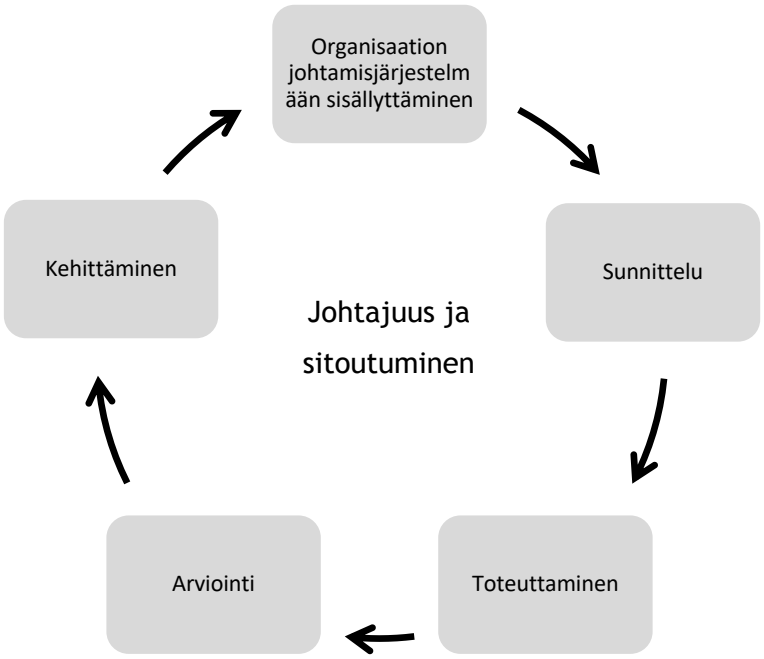
Taulukko 1: Riskienhallinnan periaatteiden selitykset. (SFS 31000)

Riskienhallinnan periaatteet muodostavat organisaation tukirangan, jonka avulla riskejä hallitaan. Lähtökohtana on organisaation arvon luominen ja säilyttäminen, jota vaalitaan ulottamalla riskienhallinta kaikkialle organisaatioon niin, että se kattaa kaikki toiminnot ja vastuuttaa kaikki organisaation jäsenet sekä ottaa huomioon sidosryhmien näkemykset tietämyksen ja havainnoinnit. Riskienhallinta perustuu parhaaseen saatavilla olevan tietoon ja se on dynaaminen ja joustava, muuttuen toimintaympäristön muutosten vaatimalla tavalla sekä huomioi kulttuuriset ja inhimilliset tekijät ja on jatkuvan kehittämisen keskiössä. Paras saatavilla oleva tieto perustuu organisaation tilannekuvaan. Tilannekuva muodostuu monista eri tekijöistä, joiden avulla muodostetaan näkemys sekä normaaliajan, että kriisiajan tilanteesta päätöksenteon perustaksi.

2.3.2 Riskienhallinnan puitteet

Riskienhallinnan puitteiden tarkoitus on auttaa organisaatiota yhdistämään riskienhallinta keskeisiin toimintoihinsa ja tehtäviin. Riskienhallinnan vaikuttavuus riippuu sen sisällyttämisestä organisaation hallintotapaan ja päätöksentekoon. Tämä vaatii tukea sidosryhmiltä, etenkin ylimmältä johdolta. (SFS-ISO 31000)

Riskienhallinnan puitteiden kehittämiseen kuuluu riskienhallinnan sisällyttäminen organisaation johtamisjärjestelmään ja riskienhallinnan suunnittelu, toteuttaminen, arviointi ja kehittäminen koko organisaatiossa. Seuraava kuva esittää riskienhallinnan puitteiden osatekijöitä.



Kuvio 5: Riskienhallinnan puitteet (SFS-ISO 31000, 9)

Organisaation olisi arvioitava nykyisiä riskienhallinnan käytäntöjään ja prosessejaan, arvioitava mahdolliset puutteet ja otettava ne huomioon riskienhallinnan puitteissa. Riskienhallinnan puitteiden osat ja se, miten ne toimivat kokonaisuutena, olisi sovitettava organisaation tarpeiden mukaiseksi. (SFS-ISO 31000)

Taulukossa on avattu riskienhallinnan puitteiden käsitteitä, joita edellä olevassa kuviossa esiintyy.

Johtajuus ja sitoutuminen	Ylimmän johdon ja hallituksen olisi varmistettava, että riskienhallinta sisällytetään kaikkiin organisaation toimintoihin, sekä osoitettava johtajuutta ja sitoutumista. Ylin johto on vastuussa riskienhallinnasta, ja hallitus (johtoryhmä tms.) riskienhallinnan valvonnasta.

Organisaation johtamisjärjestelmään sisällyttäminen	Riskienhallinnan sisällyttäminen organisaation johtamisjärjestelmään perustuu ymmärrykseen organisaatiorakenteista ja toimintaympäristöstä. Organisaatiorakenteet vaihtelevat organisaation tarkoituksen, tavoitteiden ja monimutkaisuuden mukaan. Riskejä hallitaan organisaatiorakenteen jokaisessa osassa. Jokaisella organisaatiossa on vastuu riskienhallinnasta.
Suunnittelu	Organisaation riskienhallinnan puitteiden suunnittelussa tulee tarkastella ulkoista ja sisäistä toimintaympäristöä ja muodostettava niistä käsitys. Ylimmän johdon ja hallituksen olisi sisällytettävä suunnitteluun sitoutuneisuutta, rooleja, vastuita ja valtuuksia sekä resurssien kohdentamista ilmaisevat seikat sekä luotava viestintä- ja tiedonvaihtomallit.
Toteuttaminen	Riskienhallinnan puitteiden onnistunut toteuttaminen vaatii niistä tiedottamista sidosryhmille ja sidosryhmien mukaan ottamista toteutukseen. Riskienhallinnan puitteiden ansiosta organisaatiot voivat käsitellä epävarmuutta suoraan päätöksenteossa ja varmistaa samalla, että uudet tai tulevat epävarmuudet voidaan ottaa huomioon niiden ilmetessä. Oikein suunniteltuna ja toteutettuna riskienhallinnan puitteet varmistavat, että riskienhallintaprosessi on osa kaikkia organisaation toimintoja, myös päätöksentekoa, ja että muutokset ulkoisessa ja sisäisessä toimintaympäristössä pystytään ottamaan huomioon.
Arviointi	Jotta riskienhallinnan puitteiden vaikuttavuutta voidaan arvioida, organisaation olisi mitattava säännöllisin väliajoin riskienhallinnan puitteiden toimivuutta suhteessa niiden tarkoitukseen, toteuttamissuunnitelmaan, indikaattoreihin ja odotettuun käyttäytymiseen sekä määritettävä, soveltuvatko riskienhallinnan puitteet edelleen organisaation tavoitteiden tukemiseen.
Kehittäminen	Organisaation olisi kehitettävä jatkuvasti riskienhallinnan puitteiden soveltuvuutta, tarkoituksenmukaisuutta ja vaikuttavuutta sekä tapaa, jolla riskienhallintaprosessi on sisällytetty organisaatioon. Kun tunnistetaan olennaisia puutteita tai kehittämismahdollisuuksia, organisaation olisi laadittava suunnitelmat ja tehtävät ja määriteltävä niiden toteutuksesta vastaavat tahot. Kun parannukset on toteutettu, niiden olisi osaltaan kehitettävä riskienhallintaa.

Taulukko 2: Riskienhallinnan puitteiden soveltaminen organisaation toimintaan. (SFS-ISO 31000)

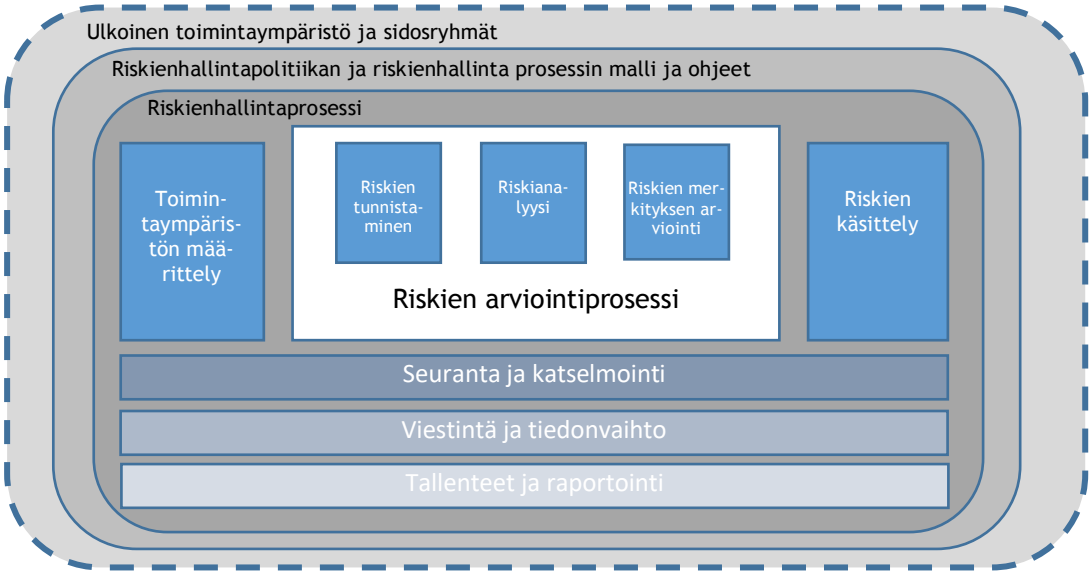
Riskienhallinnan puitteet muodostavat keskeiset toimintamallit organisaation riskienhallinnalle. Johdon tärkein tehtävä riskienhallinnan kannalta on itsensä sitouttaminen, omien vastuiden ymmärtäminen sekä koko henkilöstön sitouttaminen riskienhallintaan. Johdon tulee myös luoda suuntaviivat ja varmistaa resurssit riskienhallinnan suunnittelulle, toteuttamiselle, arvioinnille ja jatkuvalle kehittämiselle.

2.3.3 Riskienhallinnan prosessi

Jokainen organisaatio on itse vastuussa päätöksistään, jotka koskevat riskien käsittelyä ja niiden perusteella tehtäviä toimenpiteitä (VM 2017a)

Riskienhallintaprosessiin kuuluu toimintaperiaatteiden, menettelyjen ja käytäntöjen järjestelmällinen soveltaminen viestintään ja tiedonvaihtoon sidosryhmien kanssa, toimintaympäristön määrittelemiseen sekä riskien arviointiin, käsittelyyn, seurantaan, katselmointiin, kirjaamiseen ja raportointiin. (SFS-ISO 31000)

Seuraavassa kuvassa on esitetty riskienhallinnan prosessi, jossa määritellään osa-alueet, joilla organisaation riskienhallintaa toteutetaan. Taulukossa olevat määritelmät täydentävät kuvan ymmärrettävyyttä.



Kuvio 6: Riskienhallinnan prosessi SFS-ISO 31000 standardin mukaisesti. (Muokattu lähteistä VM 2017a, 12; SFS 31000)

Riskienhallintaprosessin tulee olla olennainen osa johtamista ja päätöksentekoa. Se myös tulee olla sisällettynä organisaation rakenteeseen, toimintoihin ja prosesseihin. Riskienhallintaa voidaan soveltaa sekä strategisella, että operatiivisella tasolla tai ohjelman, kuten myös projektin tasolla. Riskienhallintaprosessilla on monia käyttökohteita organisaatiossa. Prosessi voidaan räätälöidä tavoitteiden saavuttamista varten sekä ulkoiseen että sisäiseen toimintaympäristöön. (SFS-ISO 31000)

Kaikissa vaiheissa tulisi huomioida ihmisten käyttäytymisen ja kulttuurin dynaaminen ja muuttuva luonne. Riskienhallintaprosessi esitetään usein järjestyksessä etenevänä, mutta käytännössä se on iteratiivinen ja jatkuvasti tarkentuva prosessi. (SFS-ISO 31000)

Seuraavassa on lyhyesti kuvattu kuvassa esiintyvien riskienhallinnan viitekehyksen osa-alueita

Ulkoinen toimintaympä-ristö ja sidosryhmät.	Kuvastaa organisaation ulkopuolisten toimintaympäristöä, jonka puitteissa organisaatio pyrkii saavuttamaan tavoitteensa. Riskinkäsittelytapoja valitessaan organisaation olisi huomioitava sidosryhmien arvot, näkemykset ja mahdollinen osallistuminen sekä sopivimmat viestintä- ja tiedonvaihtotavat organisaation ja sidosryhmien välillä.
Riskienhallintapolitiikan ja riskienhallintapro-sessin malli ja ohjeet	Organisaation hyväksymä ja noudattama riskienhallintapolitiikka sekä prosessimalli, ohjeet ja käytänteet, joilla riskienhallintaa toteutetaan.
Riskienhallintaprosessi	Toimintaperiaatteiden, menettelyjen ja käytäntöjen järjestelmällinen soveltaminen viestintään ja tiedonvaihtoon sidosryhmien kanssa, toimintaympäristön määrittelemiseen sekä riskien arviointiin, käsittelyyn, seurantaan, katselmointiin, kirjaamiseen ja raportointiin.

<table>
<tr><td>Toimintaympäristön määrittely</td><td>Riskienhallintaprosessin olisi oltava olennainen osa johtamista ja päätöksentekoa, ja se olisi sisällytettävä organisaation rakenteeseen toimintoihin ja prosesseihin. Sitä voidaan soveltaa strategisella tai operatiivisella tasolla tai ohjelman tai projektin tasolla.</td></tr>
<tr><td>Riskien arviointiprosessi</td><td>Riskien arviointiprosessi on kokonaisvaltainen prosessi, joka kattaa riskien tunnistamisen, riskianalyysin ja riskien merkityksen arvioinnin
<table>
<tr><td>Riskien tunnistaminen</td><td>Tarkoitus on löytää, havaita ja kuvata riskit, jotka voivat auttaa organisaatiota sen tavoitteiden saavuttamisessa tai estää organisaatiota saavuttamasta tavoitteitaan.</td></tr>
<tr><td>Riskianalyysi</td><td>Tarkoitus on ymmärtää riskin luonne ja sen ominaisuudet sekä tarvittaessa riskitaso. Riskianalyysissä tarkastellaan yksityiskohtaisesta epävarmuuksia, riskin lähteitä, seurauksia, todennäköisyyttä, tapahtumia, skenaarioita ja hallintakeinoja ja niiden vaikuttavuutta.</td></tr>
<tr><td>Riskien merkityksen arviointi</td><td>Tarkoitus on tukea päätöksentekoa. Riskien merkityksen arviointiin kuuluu riskianalyysin tulosten vertaaminen määriteltyihin riskikriteereihin, jotta voidaan määrittää, tarvitaanko lisätoimenpiteitä.</td></tr>
</table></td></tr>
<tr><td>Riskien käsittely</td><td>Tarkoitus on valita ja toteuttaa vaihtoehdot riskien käsittelyyn. Riskien käsittely on toistuvat prosessi, johon kuuluvat seuraavat vaiheet.
riskien käsittelyn vaihtoehtojen kehittäminen ja valinta
Riskien käsittelyn suunnittelu ja toteuttaminen
Riskien käsittelyn vaikuttavuuden arvioiminen
Päätös siitä, onko jäljelle jäävä riski hyväksyttävä
Riskin käsittelyn jatkaminen, mikäli jäännösriski ei ole hyväksyttävissä.</td></tr>
<tr><td>Seuranta ja katselmointi</td><td>Tarkoitus on varmistaa prosessin suunnittelun, toteutuksen ja tulosten laatu ja vaikuttavuus ja parantaa niitä. Riskienhallintaprosessin ja sen tulosten jatkuvan seurannan ja säännöllisen katselmoinnin olisi oltava suunniteltu osa riskienhallintaprosessia, ja vastuut olisi määriteltävä selkeästi.

Seurannan ja katselmoinnin olisi oltava osa kaikkia prosessin vaiheita. Seurantaan ja katselmointiin kuuluu suunnittelu, tiedon kerääminen ja analysoiminen, tulosten kirjaaminen ja palautteen antaminen.</td></tr>
<tr><td>Viestintä ja tiedonvaihto</td><td>Viestinnän ja tiedonvaihdon tarkoitus on auttaa olennaisia sidosryhmiä ymmärtämään riskejä, päätöksenteon perusteita ja syitä siihen, miksi tiettyjä toimenpiteitä tarvitaan. Viestinnällä pyritään lisäämään ymmärrystä riskeistä, kun taas tiedonvaihtoon sisältyy päätöksentekoa tukevan palautteen ja tiedon hankkiminen.</td></tr>
<tr><td>Tallenteet ja raportointi</td><td>Riskienhallintaprosessi ja sen tulokset olisi dokumentoitava ja raportoitava tarkoituksenmukaisella tavalla. Tallenteiden ja raportoinnin tavoite on
Auttaa viestimään riskienhallinnan toiminnoista ja tuloksista koko organisaatiossa
Antaa tietoa päätöksentekoon
Kehittää riskienhallintatoimia
Edistää vuorovaikutusta sidosryhmien kanssa, muun muassa niiden sidosryhmien kanssa, joilla on vastuita riskienhallintatoimista.</td></tr>
</table>

Taulukko 3: Riskienhallinnan viitekehyksen osa-alueet ja vaiheet. (VM 2017a, 12; SFS 31000 2018, 14-19)

2.3.4 Riskienhallintapolitiikka

Riskienhallintapolitiikka voidaan lyhyesti määritellä olevan organisaation päättämät, kuvaamat ja dokumentoimat riskienhallintaan liittyvät periaatteet ja tavoitteet. Riskienhallintapolitiikasta voidaan käyttää myös nimitystä riskienhallinnan periaatteet. (VM 2017a, 13). Organisaatiossa voi olla tarpeen erottaa milloin tarkoitetaan SFS-ISO 31000 mukaisia riskienhallinnan

periaatteita ja milloin taas organisaation omia riskienhallinnan periaatteita, jonka vuoksi voisi olla hyvä puhua edellisistä riskienhallinnan periaatteina ja jälkimmäisessä riskienhallintapolitiikasta.

Riskienhallintapolitiikassa määritellään viraston riskienhallinnan tavoitteet, periaatteet, vastuut ja keskeiset menettelytavat. Riskienhallintapolitiikan avulla varmistetaan, että riskienhallinnasta tulee osa viraston ohjaus- ja johtamisjärjestelmää ja että se kattaa koko toiminnan ja on yhtenäinen läpi koko organisaation. (VM 2017b)

Riskienhallinta luo perustan ja linjaukset riskienhallinnan puitteiden toteuttamiselle. Politiikan sisältö on laadittava organisaation tarpeita vastaavaksi. Yksi hyvä sisältömalli ei sellaisenaan sovellu toiselle organisaatiolle, vaan sisältöön vaikuttavat erityispiirteet on huomioitava organisaatiokohtaisesti. (VM 2017b)

Riskienhallinta muodostaa perustan turvallisuusjohtamiselle. Organisaatiossa se tarkoittaa, että edellä kuvatut riskienhallinnan periaatteet, puitteet ja prosessi tulee jalkauttaa organisaatiossa siten, että koko henkilöstö ja sidosryhmät ovat velvollisia siihen osallistumaan. Samalla pitää luoda käytänteet ja toimintamallin, että henkilöstöllä ja sidosryhmille on mahdollista osallistua riskienhallintaa. Riskienhallinnan ollessa osa organisaation johtamisjärjestelmää se voidaan onnistuneesti turvallisuusjohdon koordinoimana jalkauttaa, viestiä organisaatiossa ja sisäistää kokonaisvaltaisesti niin että kaikki haluavat ja voivat siihen osallistua.

2.4 Turvallisuusjohtaminen

Turvallisuusjohtaminen on oma erityistä osaamista vaativa ammatti, jota tehtävää hoitavan tulee olla jatkuvassa vuorovaikutuksessa ja antaa tukeaan organisaation ylimmälle johdolle riskienhallinnan ja turvallisuuden erityisosaamisen alueella. Turvallisuusjohtamisen vaikutuksenarviointia tulee tehdä ja sille on asetettava mitattavissa olevat tavoitteet, jotta tavoitteiden saavuttamista voidaan säännöllisin väliajoin seurata ja arvioida. Tässä työssä on eroteltu käsitteet turvallisuusjohtaminen ja turvallisuuden johtaminen.

Turvallisuusjohtaminen on kokonaisvaltaista sekä lakisääteisen, että omaehtoisen turvallisuuden hallintaa. Siinä yhdistyy eri menetelmien ja toimintatapojen, että ihmisten johtaminen. Turvallisuusjohtaminen sisältää ajatuksen jatkuvasta terveellisyyden ja turvallisuuden edistämisestä työpaikoilla ja erilaisissa organisaatioissa. Turvallisuusjohtaminen pitää sisällään jatkuvan toiminnan suunnittelun, toiminnan ja seurannan. (Turvallisuusjohtaminen 2010, 6)

Lanne (2007, 12) on väitöskirjassaan määritellyt turvallisuusjohtamisen olevan organisaatioissa tapahtuvaa järjestelmällistä ja organisoitua ihmisiä, ympäristöä, omaisuutta, tietoa ja mainetta vahingoittavien tapahtumien ennaltaehkäisemiseen tähtäävää johtamista. Turvallisuusjohtamisen prosessi on jatkuva, ja se etenee kehänä politiikasta ja tavoitteista

suunnitteluun, toteutukseen, seurantaan ja arviointiin sekä uudelleen kehitys- ja korjaustoimien kautta jatkuvaan parantamiseen. Turvallisuusjohtaminen nivoutuu organisaation normaaliin johtamisprosessiin.

Turvallisuusjohtaminen muodostuu sanoista ”turvallisuus” ja ”johtaminen”, joten on syytä käsitellä nämä molemmat sanat erikseen.

Turvallisuus on kokonaisturvallisuuden sanaston (TSK 2017, 16) mukaan tila, jossa uhkat ja riskit ovat hallittavissa. Turvallisuudella voidaan tarkoittaa myös toimintaa tai toimintojen kokonaisuutta, jolla pyritään siihen, että uhkat ja riskit ovat hallinnassa, tai tunnetta siitä, että uhkat ja riskit ovat hallinnassa. Englanninkielessä turvallisuudella on kaksi vastinetta, ”security” ja ”safety”. Security viittaa erityisesti ”kovaan” turvallisuuteen eli tarkoitukselliselta vahingoittavalta toiminnalta (kuten aseellisen voiman käyttö, väkivalta, rikollinen toiminta) suojassa olemiseen (esimerkiksi valtion tai rakennuksen turvallisuus hyökkääjiä vastaan). Safety puolestaan viittaa ”pehmeään” turvallisuuteen, siis turvallisuuteen, joka ei vaarannu tarkoituksellisen toiminnan vuoksi vaan esimerkiksi tapaturmien, onnettomuuksien tai virheiden vuoksi (kuten työturvallisuus, potilasturvallisuus, tuotteiden käyttöturvallisuus). Termi security on kokonaisturvallisuuden aihepiirin yhteydessä yleisempi, ja sitä voidaan käyttää esimerkiksi, kun puhutaan turvallisuudesta yhteiskunnan toimijoiden toimintana, jolla pyritään uhkien ja riskien hallitsemiseen, tai tällaisella toiminnalla saavutettuna tilana. Usein sanoja security ja safety käytetään yhdessä (esimerkiksi organisaationimissä, kuten ”Department of Security and Safety”). Suomenkielisenä terminä turvallisuus on moniulotteinen ja kontekstisidonnainen, mutta käsitteenä kuitenkin sellainen, että sitä voidaan käyttää sellaisenaan niin että se ymmärretään tarkoittavan tilaa, jossa uhkat ja riskit ovat hallittavissa ja ihminen kokee olevansa turvassa.

Suomenkielinen termi ”johtaminen” jaetaan englanninkielisessä kahteen käsitteeseen eli ”management” ja ”leadership”. ”Management” tarkoittaa suomeksi asioiden johtamista ja ”leadership” ihmisten johtamista eli johtamisessa yhdistyy vastuu ihmisistä ja arjen asioista. Turvallisuusjohtaminen pitää sisällään nämä molemmat. Työturvallisuuskeskus (2020) määrittelee, että Ihmisten johtamisen tavoitteena on saada tarvittavat asiat tapahtumaan ja ihmiset toimimaan halutulla tavalla organisaation tavoitteen saavuttamiseksi. Johtaminen on ennen kaikkea yhteistyössä toimimista. Tulokset saadaan aikaan ihmisten avulla ja heidän kanssaan. Organisaatiotasolla sovitut yhtenäiset johtamiskäytännöt luovat oikeudenmukaista ja tasavertaista johtamista. Asioiden johtaminen on taas organisaation toimintaprosessien hallintaa, suunnittelua, organisointia, arviointia, kontrollointia sekä niihin liittyvää päätöksentekoa. Työhyvinvointia tuottava asioiden johtaminen on systemaattista toimintaa, jossa tavoitteet ja järjestelmät tukevat toimintaa. Johtaminen perustuu organisaation missiolle, visiolle, arvoille ja strategialle. Organisaation sovitut toimintamallit, suunnitelmia ja pelisäännöt eivät

muutu henkilöiden vaihtuessa. Organisaation johtaminen ja turvallisuus yhdistyvät organisaatioturvallisuuden käsitteessä.

Organisaatioturvallisuudella (vastaa käsitettä ”yritysturvallisuus”) tarkoitetaan organisaation henkilöstön, tiedon ja kaiken toiminnan kattavaa turvallisuutta. Kokonaisturvallisuuden sanaston (TSK 2017, 17) mukaan organisaatioturvallisuudella varmistetaan organisaation toiminnan jatkuvuus kaikissa tilanteissa ja se on organisaation henkilöstöä, tietoa, materiaalia, teknistä infrastruktuuria ja ympäristöä koskeva turvallisuus, jossa organisaatio voi olla esimerkiksi yritys, virasto tai kunta.

Elinkeinoelämän keskusliitto (EK) on kiteyttänyt organisaatioturvallisuuden malliksi kokonaisuuden, jossa keskiössä on liiketoiminnan jatkuvuus, turvallisuus ja vaatimustenmukaisuus ja jossa turvallisuusjohtaminen on jaettu yhdeksään osa-alueeseen: tietoturvallisuus, toimitila- ja kiinteistöturvallisuus, väärinkäytösten ja poikkeamien hallinta, varautuminen ja kriisinhallinta, pelastusturvallisuus, henkilöstöturvallisuus, ympäristöturvallisuus, työturvallisuus sekä tuotannon ja toiminnan turvallisuus. Turvallisuuden johtamisen taustalla on riskienhallinta ja sen taustalla organisaation strategia, jota arvioidaan Demingin ympyrän kautta jatkuvasti (PDCA tarkoittaa Plan, Do, Check, Act). (EK yritysturvallisuus 2016.) Elinkeinoelämän keskusliiton organisaatioturvallisuuden kuvio on esitetty kappaleessa ”Organisaatioturvallisuus”.

Sosiaali- ja terveysministeriön (STM 2011, 7) mukaan turvallisuusjohtaminen on osa organisaation johtamisjärjestelmää ja turvallisuustyön edellyttämä riskienhallinta ja turvallisuustyö [turvallisuuden johtaminen, kehittäminen, jalkauttaminen] sekä niiden suunnittelu ja seuranta sisältyvät normaaliin johtamiseen, ohjaukseen ja päätöksentekoon. Johto vaikuttaa omalla esimerkillään koko organisaation turvallisuuskulttuuriin ja sen tehtävänä on antaa tietoa turvallisuudesta sekä luoda sen edistämiseksi ja ylläpitämiseksi myönteistä asennetta. Johdon vastuulla on myös huolehtia turvallisuusjohtamisen tehtävien edellyttämien resurssien riittävyydestä ja sillä on jakamaton kokonaisvastuu turvallisuusjohtamisesta ja riskienhallinnasta.

Turvallisuuden kannalta positiivisia tuloksia saavutetaan toteuttamalla turvallisuusjohtamista käytännön teoissa ja jokapäiväsessä työssä. Turvallisuusjohtaminen ei ole vain turvallisuushenkilöstön vastuulla, vaan osa jokaisen organisaation jäsenen tehtäviä ja turvallisuustyön tulisikin tavalla tai toisella olla osa jokaisen työntekijän jokapäiväistä työnkuvaa. (Turvallisuusjohtaminen 2010, 6-9.) Kerko (2001, 23) toteaa, että käytännön työssäkin turvallisuusjohtaminen on aivan samanlaista kuin mikä tahansa muukin johtaminen, jossa turvallisuusasioiden hoitaminen ei muodosta erillistä saareketta johtamiskentässä. Kerko korostaa myös sitä, että turvallisuusasiat ovat koko organisaation yhteinen asia, eikä pelkästään työntekijöiden ja

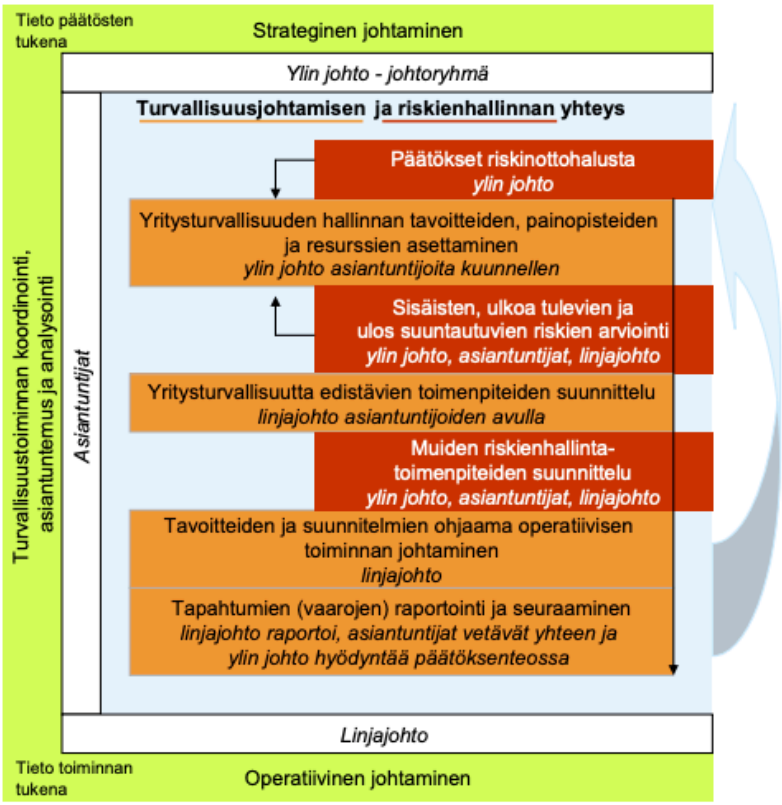
työnjohdon välistä asioiden hoitamista. Koko organisaation turvallisuuteen voidaan vaikuttaa omalla, hyvällä esimerkillä.

Katakri (2015) eli ”Kansallisen Turvallisuuden Auditointikriteerit” on viranomaisten käyttöön tarkoitettu tietoturvallisuuden auditointityökalu, jolla arvioidaan kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Osa-alue 3 (T) on nimetty ”Turvallisuusjohtamiseksi” ja siinä käsitellään niitä menetelmiä, joilla turvallisuus ja sen hallinta jalkautetaan osaksi koko organisaation toimintaa. Katakrin (2015, 6) mukaan turvallisuusjohtamisen osa-alue kattaa hallinnollisen turvallisuuden ja henkilöstöturvallisuuden. Turvallisuudenjohtamisen vaatimuksilla pyritään siihen, että organisaatiolla on toimiva turvallisuuden hallintajärjestelmä sekä riittävät menettelyt sen varmistamiseksi. että viranomaisen salassa pidettäviä tietoja käsittelevä henkilöstö toimii asianmukaisesti. Hallinnollisen turvallisuuden kohdassa on määritelty kolme vaatimusta, jotka organisaatiossa tulee olla toteutettu. Nämä ovat

1. Organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet [turvallisuuspolitiikka], jotka kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan.
2. Turvallisuusperiaatteet ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset.
3. Turvallisuusperiaatteet ohjaavat turvallisuustoimintaa. Turvallisuusperiaatteiden toteutumisesta raportoidaan ja niiden toteutumista seurataan säännöllisesti.

Organisaation turvallisuusperiaatteilla tavoitellaan sitä, että johto sitoutuu organisaation turvallisuustyöhön ja että turvallisuustyö tukee organisaation toimintaa. Turvallisuusperiaatteet viestinnästä henkilöstölle ja tarvittaville sidosryhmille tulee huolehtia.

Lanne (2007, 29) on väitöskirjassaan koonnut turvallisuusjohtamisen kokonaisuuden oheiseen kuvaan.



Kuvio 7: Turvallisuusjohtamisen ja riskienhallinnan yhteys organisaatioturvallisuuteen (Lanne 2007, 29)

Lanne muistuttaa, että turvallisuusjohtamisen ja riskienhallinnan suhdetta pyritään usein määrittelemään asettamalla toinen käsite toisen yläkäsitteeksi. Kyseessä on kuitenkin enemminkin tarkastelunäkökulman valinta kuin hierarkkinen suhde. Organisaatioturvallisuuden johtamisen näkökulmasta katsottuna riskienhallinnan menettelytapoja ja käytänteitä (kuten riskien arviointi tai riskianalyysi) voidaan hyödyntää yhtenä johtamisen välineenä. Kun asiaa katsotaan riskienhallinnan näkökulmasta, havaitaan, että turvallisuusjohtamisen keinot auttavat useiden eri riskien todennäköisyyden ja seurausten vähentämisessä eli riskin pienentämisessä (Lanne 2007, 29)

2.5 Kyberturvallisuus ja jatkuvuuden hallinta

Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta turvataan. (Suomen kyberturvallisuuden strategia 2013). Kokonaisturvallisuuden sanaston (TSK 2017, 35) mukaan se on tila, jossa kybertoimintaympäristöstä yhteiskunnan elintärkeille toiminnoille tai muille kybertoimintaympäristöstä riippuvaisille toiminnoille koituvat uhkat ja riskit ovat hallinnassa. Kokonaisturvallisuuden sanasto liittää kyberturvallisuuden ja tietoturvallisuuden yhteen määrittelemällä, että ”Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten

kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään mm. toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot.” (TSK 2017, 35)

Kybertoimintaympäristö voidaan käsittää samana asiana kuin digitaalinen toimintaympäristö, joka kehittyy yhteiskunnan osana ja palveluina nopeasti ja on sähköisessä muodossa olevan informaation käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö, jolle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. (Suomen kyberturvallisuusstrategia 2019). Aalto-yliopiston kyberturvallisuuden professori Jarmo Limnéll puhuukin yleensä kyberturvallisuuden sijasta digitaalisesta turvallisuudesta ja nykyisin vain turvallisuudesta, tarkoittaen fyysisen maailman ja bittien maailman yhdistävä toimintaympäristön turvallisuudesta (mm. Luennot Aalto-yliopistossa 2016-2017; Talous ja koti 2019)

Kyberturvallisuus on jo nykypäivänä läpäisevänä läsnä ihmisten arjessa ja sen merkitys korostuu väistämättä lähitulevaisuudessa mm. digitalisaation voimistumisen ja esineiden internetin (IoT) kehittymisen myötä. Yhteiskunnat ovat yhä riippuvaisempia digitaalisesta ympäristöstä, ja digitalisoituvassa maailmassa tietoliikenteen, palveluiden sekä tietoverkkojen ja tietovarantojen turvallisuus on yhteiskuntien toiminnan kannalta keskeisen tärkeää. (Pelkonen ym. 2016, 7)

Limnéll, Majewski ja Salminen (2014, 14) muistuttavat, että kyberturvallisuus on malliesimerkki kokonaisturvallisuusajattelun välttämättömyydestä yhteiskunnassa ja yrityksissä. Kybermaailma on kaikkialla läsnä ja läpäisee kaikki turvallisuuden tasot ja ulottuvuudet. Yksiselitteistä jakoa fyysiseen ja bittien maailmaan ei voi eikä kannata tehdä, koska kyberulottuvuuden tapahtumilla on selkeitä fyysisiä seurauksia. Arkipäivämme toimivuus on riippuvainen bittien maailmasta. Siksi kaikkien on oltava tietoisia kyberuhista ja omista toimenpiteistään niihin liittyen.

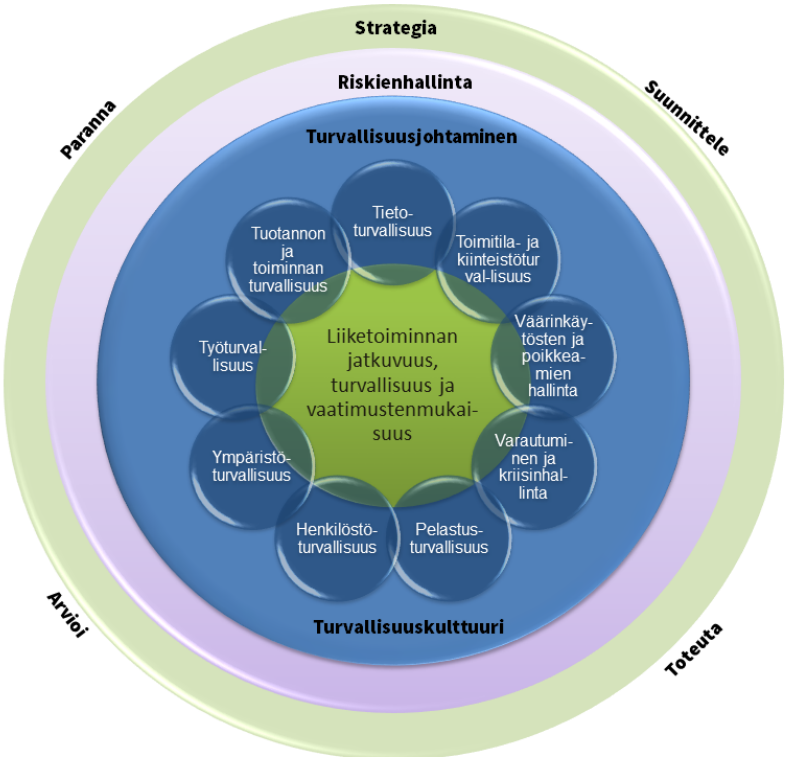
Jatkuvuuden hallinta liittyy olennaisesti kyberturvallisuuteen. Jatkuvuuden hallinnan tarkoituksena on mahdollistaa organisaation häiriötön toiminta kehittämällä varautumis-, jatkuvuus-, toipumis- ja valmiussuunnittelua. Suunnitelmien avulla organisaatio voi varautua erilaisiin normaaliolojen häiriötilanteisiin sekä poikkeusoloihin. Jatkuvuuden hallinta edellyttää toimintaan liittyvien riskien ja muiden toimintaan vaikuttavien riippuvuuksien tunnistamista. (VM 2017b). Fyysinen maailma ja bittien maailma yhdistyy kyberturvallisuusajattelussa. Digitaalisista järjestelmistä riippuvaisen toimintaympäristön häiriötön toiminta osaltaan varmistetaan kyberturvallisuustoimenpiteillä. Varmistamalla ettei atomien maailmaa horjuteta bittien maailmasta tulevilla kyberhyökkäyksillä, voidaan organisaation häiriötön toiminta varmistaa yhdessä muiden toimenpiteiden kanssa.

2.6 Organisaatioturvallisuus

Kokonaisturvallisuussanaston (TSK 2017, 17) mukaan organisaatioturvallisuus on organisaation henkilöstöä, materiaalia, tietoa, teknistä infrastruktuuria ja ympäristöä koskeva turvallisuus, jolla varmistetaan organisaation toiminnan jatkuvuus kaikissa tilanteissa ja jossa organisaatio voi olla esim. yritys, virasto tai kunta. Lanne (2007, 13) on väitöskirjassaan määritellyt, että organisaation turvallisuus koostuu poikkitieteellisten tutkimusalueiden tiedon soveltamisesta ja tutkimuksen näkökulmat voivat kohdistua tekniikkaan, kulttuuriin, käyttäytymiseen, johtamiseen, ympäristötekijöihin, päästöihin sekä yhteiskunnallisiin että sosiaalisiin vaikutuksiin. Koska näkökulmia on monta, on niiden yhdistäminen yhdeksi organisaatiokulttuurin määritelmäksi. Tässä työssä näkökulma on johtamisessa, joten organisaatioturvallisuuden määritelmäksi voidaan ajatella ihmistä, ympäristöä ja omaisuutta vahingoittavien tapahtumien ennaltaehkäisevien ratkaisujen löytäminen ja vahinkojen torjuminen. Määritelmänä voidaan käyttää, että organisaatioturvallisuus on toimenpiteitä, joilla pyritään organisaation toiminnan jatkuvuuden ja kustannustehokkuuteen, työntekijöiden, asiakkaiden ja sidosryhmien turvallisuuden varmistamiseen sekä organisaation ympäristön ja omaisuuden suojaamiseen. (EK yritysturvallisuus 2016; Virtanen 2002)

Organisaation kokonaisturvallisuutta tarkasteltaessa käytetään termiä organisaatioturvallisuus. Yrityksen näkökulmasta organisaatioturvallisuus käsittää kokonaisuuden, jolla suojataan yrityksen arvoja, joten on tarkoituksenmukaista puhua yritysturvallisuudesta. Elinkeinoelämän keskusliiton mukaan yritysturvallisuus käsittää kaiken yrityksen toimintojen turvallisuuden, jolloin yritysturvallisuustoiminnalla voidaan suojata yritykselle tärkeitä arvoja kuten henkilöitä, tietoa, mainetta, omaisuutta tai ympäristöä. (EK yritysturvallisuus 2016). Nämä ovat luonnollisesti samoja arvoja, joita minkä tahansa organisaation tulee turvallisuusratkaisuillaan suojata. Tämä opinnäytetyön kohdeorganisaatio on valtiohallinnon organisaatio, jonka vuoksi on luontevaa käyttää termiä ”organisaatioturvallisuus” (Organisational Security, Organisational Safety) sen sijaan, että puhuttaisiin ”yritysturvallisuudesta”, mutta käsitteiden sisällöt ovat yhtenevät.

Organisaationturvallisuus on yläkäsite organisaation eri toimintojen turvallisuudelle ja niiden johtamiselle. Organisaatioturvallisuus voidaan jakaa yhdeksään osa-alueeseen, jotka voidaan kuvata seuraavalla Elinkeinoelämä keskusliiton tekemällä kaaviolla



Kuvio 8: Organisaatioturvallisuuden osa-alueet. (EK yritysturvallisuus 2016)

Organisaatioturvallisuuden keskiössä on toiminnan jatkuvuus, turvallisuus ja vaatimustenmukaisuus, joita jokaista toteutetaan turvallisuusjohtamisen kautta yhdeksällä eri osa-alueella. Toiminta ohjaa ja synnyttää organisaation turvallisuuskulttuuria ja riskienhallinnalla tunnistetaan, analysoidaan ja arvioidaan toimintaan kohdistuvia riskejä ja niiden vaikutusta. Strategiassa määritellään suojattavat arvot. Organisaatioturvallisuus on jatkuva prosessi, jossa syklisesti suunnitellaan, toteutetaan, arvioidaan ja parannetaan organisaation turvallisuustoimintoja. (EK yritysturvallisuus 2016).

Organisaatioturvallisuuden osa-alueita on yhdeksän, joista seuraavassa taulukossa on sisällön lyhyt kuvaus kustakin (EK yritysturvallisuus 2016)

Toimitila- ja kiinteistö-turvallisuus	Toimitilojen turvallisuusluokittelun ja luokituksen mukaisen suojaamisen, rakenteellisen turvallisuuden toimenpiteet (aidat, portit, lukitukset, valaistus, murtosuojaus, kiinteistötekniikka, väestönsuojelu, esteettömyys) Turvallisuusvalvonta (kamerat, kulunvalvonta, rikosilmoitin, vartiointi, vierailijat, kokous- ja neuvottelutilat) Sopimusten hallinta (ulkoistukset, huolto, ylläpito, rakennushankkeet, vakuuttaminen)
Väärinkäytösten ja poikkeamien hallinta	Toimintaan, henkilöstöön ja omaisuuteen kohdistuvat haitalliset tapahtymat (havainnointi, ratkaisumallit, raportointi) Väärinkäytösten hallintakeinot (ennaltaehkäisy, paljastavat toimet, sisäinen tarkastus ja selvitykset, yhteistyö viranomaisten kanssa, toiminta rikostapauksissa) Vakuuttaminen (rikosriskit)

Varautuminen ja kriisinhallinta	Jatkuvuussuunnittelu (liiketoimintariskien ennakointi, tuotannon keskeytyminen tai pysähtyminen, suunnittelu ja resilienssi) Kriisinhallinta (ennaltaehkäisy ja arviointi, toiminta kriisitilanteissa, toipumissuunnitelmat, oppiminen) Valmiussuunnittelu eli poikkeustilanteisiin varautuminen (Velvoitteiden tunnistaminen, tuotannon ja toiminnan suunnittelu)
Pelastusturvallisuus	Pelastussuunnitelma ohjaavana dokumenttina (vaaratilanteiden ennakointi, työpaikkakohtaiset järjestelyt, ulkoalueet, varautuminen suuronnettomuuksiin, toimenpiteet uhkien torjumiseksi) Paloturvallisuus (rakennusten paloturvallisuus, pelastus- ja sammutuskaluston kunnossapito, määräaikaistarkastukset ja huolto, tulitöiden turvallisuus) Vakuuttaminen (vakuutusyhtiöiden suojeluohjeet ja -ehdot
Henkilöstöturvallisuus	Työntekijöiden, asiakkaiden ja avainhenkilöiden suojaaminen rikoksilta ja onnettomuuksilta (asiakkaiden ja vieraiden turvallisuus, matkustusturvallisuus ja ulkomailla työskentely, avainhenkilöiden turvallisuus, kodin ja perheen turvallisuus) Toiminnalle kriittisten henkilöresurssien varmistaminen (varahenkilöjärjestelyt ja sijaisuudet, tavoitettavuusjärjestelyt) Toiminnan suojaaminen estämällä rikollisten tms. soluttautuminen (huolellinen ja laadukas rekrytointimenettely, turvallisuusselvitykset, salassapitosopimukset, huumausainetestaukset, koeostotoiminta)
Ympäristöturvallisuus	Kestävän kehityksen periaate (elinkaariajattelu, ekotase) Energiatehokkuus Ympäristövaikutusten huolellinen arviointi Ilmoitus- ja lupamenettelut Vaarallisten aineiden käsittely ja säilytys Ympäristönsuojelun hallintajärjestelmä ja toimintaohjelma Ilmastonsuojelu ja päästökauppa Vesien ja maaperän suojelu Meluntorjunta ja maisemansuojelu Kemikaalivalvonta Jätehuolto
Työturvallisuus (työterveyshuolto ja työsuojelu)	Turvallinen työ ja työntekijöiden hyvinvointi – riskien ennaltaehkäisy ja hyvä yrityskuva (työsuojeluvastuut, työturvallisuus työpaikalla, koneiden, laitteiden ja työvälineiden turvallisuus, työpaikan sisäinen liikenne, fysikaaliset tekijät, vaarallisten aineiden käsittely, henkilösuojaimet, väkivallan kohtaaminen, työhyvinvointi) Työsuojeluorganisaatio (työsuojelutoimikunta, työsuojelupäällikkö, työsuojeluvaltuutetut, työsuojeluasiamiehet Toimintaohjelma (tavoitteet, koulutus, mittarit, tilastot)
Tuotannon ja toiminnan turvallisuus	Tuotevastuu ja -turvallisuus (huolellisuus- ja ilmoitusvelvoitteet, valvontaviranomaiset, riskiarviointi, merkinnät (esim. CE)) Palveluiden turvallisuus Maksuliikenteen turvallisuus Arvo-omaisuuden säilytys Logistiikkaturvallisuus eli kuljetus ja varastointi (toimitustapahallinta, vastuiden määrittely)

	Verkostot (alihankkijat ja palvelutoimittajat, sopimushallinta) Vakuuttaminen (vastuuvakuutukset, omaisuusvakuutukset, tuotevakuutukset, keskeytysvakuutukset, projektivakuutukset, kuljetusvakuutukset)
Tietoturvallisuus	Tietojen merkityksen arviointi (kriittisen tiedon tunnistaminen, tiedon käytettävyys, eheys ja luottamuksellisuus) Tietojen luokittelu ja käsittely (luokittelutavat, käsittelyohjeet) Hallinnollinen tietoturvallisuus (käyttö- ja pääsyoikeuksien hallinta, turvallisuusselvitykset, salassapitosopimukset) Tekninen tietoturvallisuus (palomuurit yms. ratkaisut, haittohjelmien torjunta, tiedonsiirron suojaaminen, päätelaitteiden suojaus, salaustekniikan hyödyntäminen, laitteisto- ja ohjelmistoturvallisuus, varmuuskopiointi ja muut varmistukset, käyttöturvallisuus) Järjestelmien ja prosessien jatkuvuuden varmistaminen (havainnointikyvyn kehittäminen, sieto- ja palautumiskyvyn kehittäminen, ympäristön fyysinen turvallisuus)

Taulukko 4: Organisaatioturvallisuuden osa-alueet (EK yritysturvallisuus 2016)

Organisaation turvallisuuden osa-alueiden suojaus tulee perustua riskiarvioon ja olla kustannustehokasta. Taulukosta on helppo huomata, kuinka monisäikeinen organisaatioturvallisuuden kokonaisuus on ja kuinka monta eri osa-alueen ammattilaista sen hallitseminen vaatii. Turvallisuus on muuttuva kokonaisuus, joka vaatii jatkuvaa parantamista. Organisaatioturvallisuuden jatkuva parantaminen tapahtuu Demingin ympyrän jatkuvan parantamisen periaatteen mukaisesti eli PDCA-kehän avulla. PDCA-kehä on Edwards Demingin kehittämä systemaattisen toiminnan kehä (kuva 8), jossa P (Plan) kuvaa suunnitteluvaihetta, D (Do) tekemisen vaihetta, C (Check) arviointia ja A (Act) parannusvaihetta. Demingin ympyrä toimii myös DMAIC-mallin mukaisesti iteratiivisesti, jossa kehitysprosessi alkaa uudelleen lakkaamatta. Menetelmää on alun perin kutsuttu nimellä Shewhart-ympyrä, koska Walter Shewhart on keksinyt mallin jo 1920-luvulla. 1950-luvulla japanilaiset kuitenkin nimesivät kehän uudelleen Demingin mukaan. (Laakkonen 2017, 20; Beckford 1998, 67; Andersson & Tikka 1997, 53.)

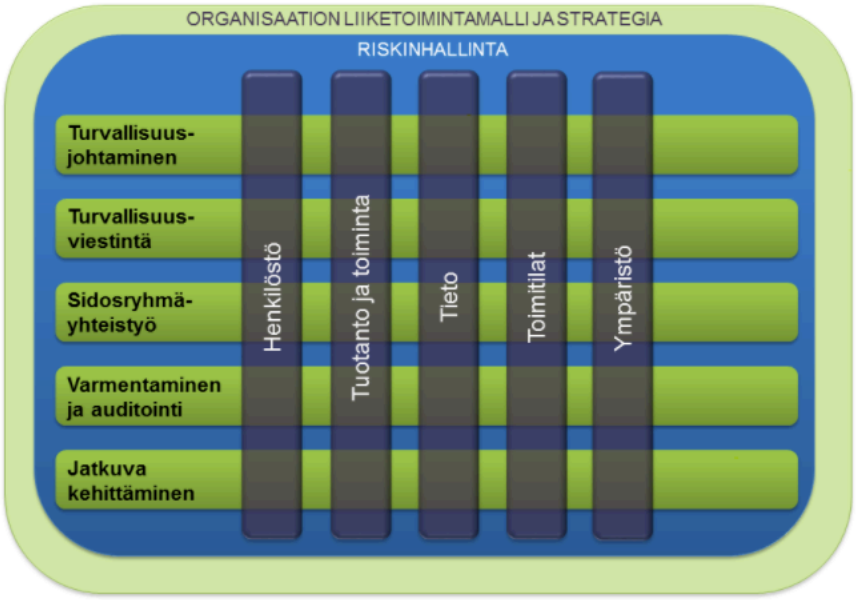
Kuvio 9: Demingin ympyrä (PDCA-kehä) toiminnan kehittämiseen (Beckford 1998, 67)

Turvallisuusjohtamiseen sovellettuna PDCA-kehä tarkoittaa, että

1. Plan tarkoittaa, että organisaatiolla on suunnitelma turvallisuuden hallintaa eli organisaatiolla on turvallisuuspolitiikka, jossa määritellään turvallisuustoiminnan päämäärät.
2. Do tarkoittaa, että organisaatio on arvioinut toimintaan kohdistuvat riskit, ottanut huomioon lainsäädännön ja valtiohallinnon vaatimukset, tehnyt henkilöstöä koskevat ohjeistukset ja implementoinut turvallisuustoimenpiteet organisaatiossa.
3. Check tarkoittaa, että organisaatiossa on määritelty vastuujaot, on huolehdittu viestinnästä ja koulutuksesta, on varmistettu että dokumentoinnit ovat ajantasaisia ja että riskienhallintajärjestelmä on kaikkien saatavilla ja että on valmistauduttu normaaliolojen häiriötilanteisiin ja poikkeusoloihin.
4. Act tarkoittaa, että organisaatiolla on mittarit, joilla turvallisuuden toteutumista seurataan, on menetelmät, joilla poikkeamat tunnistetaan ja niillä on korjaustoimenpiteet, on huolehdittu sisäisestä auditoinnista ja johdon katselmukset on tehty.

Demingin ympyrän idea on, että edellä mainitut toimenpiteet ovat jatkuvia ja kun ollaan päästy vaiheeseen 4, aloitetaan alusta vaiheesta 1. Parantamisen on oltava jatkuvaa, suunniteltua ja määrätietoista. (Seppälä 2017, 37-38; Katakri 2015, 5-12)

Organisaatioturvallisuus voidaan myös hahmottaa matriisina. Matriisi kuvaa sen mitä ympyräkuviossa (kuvio 8) ei ole kuvattu eli miten turvallisuusjohtaminen, turvallisuusviestintä, sidosryhmä yhteistyö, varmentaminen ja auditointi sekä jatkuva kehittäminen läpileikkaavat organisaation riskienhallinnan avulla suojeltavat arvot eli henkilöstön, tuotannon ja toiminnan, tiedon, toimitilat ja ympäristön. Erona tässä kuviossa on EK:n ympyräkuvioon se, että turvallisuuden osa-alueita on vain viisi, kun niitä EK:n ympyräkuviossa on yhdeksän. Syynä on, että puuttuvat neljä kohtaa (väärinkäytösten ja poikkeamien hallinta, varautuminen ja kriisinhallinta, pelastusturvallisuus ja työturvallisuus) eivät ole yksittäisinä toimintoina erotettavissa organisaatioturvallisuuden kokonaisuudessa, mutta turvallisuusjohtamisessa ne tulee olla erikseen huomioituina ja johdettuina.



Kuvio 10: Organisaatioturvallisuuden matriisissa eri osa-alueet risteävät toimintojen kanssa (EK yritysturvallisuus 2016)

Matriisin vaakatasolla on kokonaisturvallisuuden elementit kuten turvallisuusjohtaminen ja jatkuva kehittäminen ja pystytasolla on ne organisaation arvot, joita riskienhallinnalla suojataan. Näiden ohjaavana elementtinä taustalla on organisaation strategia ja yrityksen liiketoimintamalli. Elinkeinoelämän keskusliitto (EK 2020) muistuttaakin, että uhkien tunnistaminen, riskien arviointi ja käsittely ovat keskeinen edellytys organisaatioturvallisuuden määrittämiselle ja mitoittamiselle.

2.7 Turvallisuuskulttuuri ja riskikulttuuri

Kulttuuria on vaikea määritellä, mutta yleisesti hyväksytty määritelmä on, että se on heijastuma yleisestä asenteesta, joka näkyy organisaation eri osa-alueilla. Organisaation kulttuuri määrittelee kuinka yksilöt käyttäytyvät tietyssä tilanteessa ja myös sen, miten nähdään velvollisuudeksi käyttäytyä tietyissä tilanteissa. (Hopkin 2018, 288).

Turvallisuuskulttuurin käsite sai alkunsa käytännöllisistä lähtökohdista. Sitä käytettiin ensimmäisen kerran Tśernobylin ydinvoimalaonnettomuuden tutkinnan yhteydessä havainnollistamaan sitä, että onnettomuudet eivät johdu pelkästään teknisistä vioista tai yksittäisen ihmisen tekemistä inhimillisistä virheistä. Turvallisuuskulttuurikäsitteen avulla haluttiin tuoda esiin se, että johtamiseen, organisaatioon, työyhteisöön tai jopa yhteiskuntaan liittyvät tekijät vaikuttavat onnettomuuksien syntymiseen. (Reiman ym. 2008, 18)

Oedewald & Reiman (2006, 27) sanoo turvallisuuskulttuurin olevan selvästi normatiivinen käsite. Se on tapa arvioida organisaation toiminnan ”hyvyyttä” suhteessa turvallisuuteen ja se

myös asettaa vaatimuksia organisaatiolle. Heidän mukaan kaikilla organisaatioilla on kulttuuri, mutta vain osalla on turvallisuuskulttuuri. Turvallisuuskulttuurin tason mittaamisessa voidaan tarkastella seuraavia seikkoja, kuten

- Henkilöstön suhtautuminen turvallisuusmääräyksiin ja sen aiheuttamiin käytännön järjestelyihin.
- Johdon suhtautuminen turvallisuuden varmistamiseksi tarvittaviin kustannuksiin ja heidän näyttämänsä esimerkki alaisille.
- Päätöksenteossa turvallisuuden suhde taloudellisiin investointeihin.
- Suhtautuminen virheisiin ja niiden käsittelyyn.
- Suhtautuminen virheistä oppimiseen ja toiminnan jatkuvaan parantamiseen.
- Riskialttiiden päätösten kyseenalaistaminen.

Listasta nähdään, että turvallisuuskulttuuri sisältää turvallisuuskriittisen organisaation kriteereitä ja oman toiminnan jatkuvaa reflektointia.

Turpeinen (2017, 9) muistuttaa, että turvallisuuskulttuuri muodostuu organisaatio määrittelemillä toimintarajoituksilla ja -vaatimuksilla, joiden tarkoitus on varmistaa organisaation turvallisuus täyttämällä näitä vaatimuksia, joiden avulla luodaan rakenteellisia ja psykologisia toimintaedellytyksiä sekä tekemällä työtä näissä puitteissa. Turvallisuuskulttuuri on organisaation kykyä ja tahtoa ymmärtää turvallisen toiminnan edellytykset sekä toimintaa kohtaavat vaarat ja niiden ehkäisykeinot. Toimivan turvallisuuskulttuurin edellytyksenä on siis kyky ja halu toimia turvallisesti ja ehkäistä vaaroja ja edistää turvallisuutta.

Työsuojeluhallinto (2010) kuvaa turvallisuuskulttuurin alla olevalla kaaviolla.

Kuvio 11: Turvallisuuskulttuuri (Turvallisuusjohtaminen 2010, 6)

Turvallisuuskulttuuri heijastaa organisaation perusarvoja, normeja, olettamuksia ja odotuksia, jotka sisältyvät yrityksen toimintaperiaatteisiin. Turvallisuuskulttuuri muodostuu turvallisuuden hallinnan menettelytavoista ja turvallisuusjohtamisen toteuttamisesta. Turvallisuusjohtaminen jakaantuu menetelmien ja toimintatapojen johtamiseen ja ihmisten johtamiseen.

Turvallisuuskulttuuri luo perustan organisaation riskienhallinnalle. Turvallisuuskulttuuri muodostuu organisaatiokulttuurin sekä johdon ja henkilöstön arvojen, asenteiden kokemuksen ja näkemysten perusteella. Organisaatiokulttuuri on opittu ilmiö, joka ilmaisee tavan, miten organisaation ihmiset jakavat keskenään tunteet, havaitsemisen ja ajattelun. (STM 2011, 8) Turvallisuuskulttuuri muodostuu organisaation määritellessä turvallisuuden varmistamisesta seuraavia toimintavaatimuksia ja rajoituksia ja vastatessa näihin toiminnassaan. Olemukseltaan turvallisuuskulttuuri on organisaation kykyä ja tahtoa ymmärtää, millaista turvallinen toiminta on, millaisia vaaroja organisaation toimintaan liittyy ja miten niitä voidaan ehkäistä, sekä kykyä ja tahtoa toimia turvallisesti, ehkäistä vaarojen toteutumista ja edistää turvallisuutta. Turvallisuuskulttuuri on dynaaminen ja muokkautuva tila. Tämä tekee turvallisuuskulttuurista vaikeasti tartuttavan ilmiön, mutta myös asian, johon voidaan vaikuttaa. (Reiman, Pietikäinen & Oedewald 2008, 3)

Hyvällä riskikulttuurilla tarkoitetaan Hopkinin (2018) mukaan lopputulemaa yksilön ja ryhmän käyttäytymisen arvoista, asenteesta ja toimintamalleista. (Hopkin 2018, 288). Turvallisuuskulttuurista puhutaan myös riskikulttuurina (Risk Culture) (esim. Hopkin 2018). Myös ISO 31000 standardin (2018) esittelyssä puhutaan standardin tavoitteista riskikulttuurin muodostamisessa. Siinä sanotaan, että ”standardin tarkoitus on kehittää riskienhallinnan kulttuuri, jossa työntekijät ja sidosryhmät ovat tietoisia riskien seurannan ja hallinnan merkityksestä.”

Riskienhallinnan viitekehys COSO ERM (2017), muistuttaa että riskikulttuuri on hyvin erilainen organisaation elinkaaren eri vaiheissa. Aloittelevat yritykset joutuvat sietämään ja ottamaan enemmän riskejä menestyäkseen paremmin jatkossa, kun taas pidempään toimineiden yritysten kuolemaksi saattaa muodostua riskikulttuurin estämä välttämätön muutos ja toiminnan uudistaminen. (Pwc 2017)

Kuten Oedewald & Reimankin toteaa (2006, 27) on jokaisella organisaatiolla kulttuuri, mutta vain osalla turvallisuuskulttuuri. Toisaalta tämä toteamus voidaan haastaa, sillä tiedostamattakin organisaation jäsenten suhtautuminen turvallisuuteen on aina jollain tavalla olemassa oman kokemuksen ja tarpeiden kautta läsnä jokapäiväisessä toiminnassa, sillä turvallisuus on ihmisen perustarve (esim. Mielenihmeet 2018). Yksinkertaistaen voidaan todeta, että suhtautuminen turvallisuuteen operatiivisessa toiminnassa heijastelee organisaation johdon suhtautumista turvallisuuden osa-alueisiin kuten työturvallisuuteen tai tietoturvallisuuteen. Jos turvallisuuskulttuuria ei tietoisesti luoda, se todennäköisesti muodostuu itsestään ihmisten asenteiden kautta hallitsemattomasti ja ajautumalla. Sellainen tilanne tuskin on toivottava, siksi

turvallisuuskulttuuria pitää tietoisesti luoda. Martikaisen (2016, 13) mukaan organisaation kulttuuri vaikuttaa siihen, miten tärkeäksi turvallisuus koetaan ja mitä turvallisuuden hyväksi tehdään.

Ilmonen ym. (2016, 88) määrittelevät yrityskulttuurin sisältävän kolme tasoa, joihin kaikkiin tulee pyrkiä vaikuttamaan, jotta turvallisuuskulttuuri tai riskienhallintakulttuuri juurtuu organisaatioon. Näitä ovat

- Näkyvät artefaktit eli yrityksessä työntekijän kokemat konkreettiset keinot, jotka vaikuttavat jokaiseen työpäivään, joista esimerkkinä voidaan mainita kulunvalvonta, jonka työntekijä kohtaa joka kerta tullessaan ja poistuessaan työpaikalta
- Ääneen sanotut ja dokumentoidut periaatteet eli johdon kannanotot yrityksen tahtotilasta riskienhallinnan suhteen. Kaikkien turvallisuuteen ja riskienhallintaan liittyvien dokumenttien tulisi olla helposti ja nopeasti saatavilla ja löydettävissä ja jokaisella työntekijällä tulisi olla mahdollisuus milloin vain tarkistaa mitä johto on todennut ja päättänyt asioista.
- Ääneen sanomattomat yksilölliset käsitykset asioiden tilasta, joka tarkoittaa kunkin työntekijän omakohtaista käsitystä siitä, miten tulisi toimia. Näiden käsitysten perusteella työntekijät tekevät riskienhallintatyötä ja edistävät turvallisuutta silloin kun ohjeistus ei ole käytettävissä. Riskienhallintakulttuurin voidaan sanoa olevan hyvällä tasolla, kun henkilöstön yksilölliset käsitykset vastaavat sitä henkeä ja tavoitetilaa, jota johto tavoittelee ja joka on asetettu riskienhallinnan periaatteiksi.

Ilmosen ym. (2016, 41) mukaan tavoitteena on saada riskienhallinta osaksi yrityksen normaalia toimintaa. Kun riskienhallintaa tehdään systemaattisesti ja tavoitteellisesti, kasvattaa se parhaiten riskitietoisuutta. Riskitietoisuuden kasvaessa riskienhallinnasta tulee vähitellen olennainen osa yrityksen kulttuuria ja yleistä tapaa tehdä töitä yrityksessä. Lopulta riskienhallinnasta tulee olennainen osa jokaisen työntekijän jokapäiväisiä työtehtäviä ja siitä tulee yksi työtehtävän olennainen osa tai vaihe. Tällöin voidaan jo puhua erittäin kehittyneestä riskienhallintakulttuurista.

Turvallisuuskulttuuriin ja turvallisuusjohtamiseen kuuluu myös, että organisaatio kykenee varautumaan sekä normaaliolojen häiriötilanteisiin, että poikkeusoloihin. Tämä tapahtuu jatkuvuudenhallinnan kautta.

2.8 Jatkuvuussuunnittelu ja varautuminen valtiohallinnossa

Terveyden ja hyvinvoinnin laitoksen toiminta nojaa Suomen lainsäädäntöön ja jatkuvuussuunnittelua ja varautumista koskeviin valtion virastoille annettuihin ohjeistuksiin ja määräyksiin. Tässä kappaleessa määritellään niitä periaatteita ja ohjeistuksia, joilla jatkuvuussuunnittelu tehdään ja joilla varaudutaan normaaliolojen häiriötilanteisiin ja poikkeusoloihin sekä

käsitellään jatkuvuuden hallintajärjestelmiä. Kappaleessa linjataan myös periaatteita, joilla häiriötilanteiden tilannekuva muodostetaan.VM

Valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmän VAHTI -ohjeen (VM 2016) mukaan jatkuvuussuunnittelun tavoitteena on varmistaa organisaation ydintoimintojen mahdollisimman häiriötön toiminta. Jatkuvuussuunnittelu on osa organisaation kokonaisturvallisuutta, johon kuuluvat mm. turvallisuusjohtaminen, riskienhallinta, jatkuvuuden hallinta, häiriötilanteiden hallinta ja johtaminen, tilannekuvan muodostaminen sekä huoltovarmuus ja varautuminen.

Hopkin (2018, 203) määrittelee British Standardin (BS 2011) mukaan jatkuvuuden hallinnan (BCP, Business Continuity Planning) olevan kokonaisvaltainen johtamisen prosessi, jossa tunnistetaan mahdolliset uhat ja jotka toteutuessaan voivat vaikuttaa organisaation toimintaan. Jatkuvuuden hallinta myös määrittelee toimintamallin, jolla rakennetaan organisaation resilienssiä eli sietokykyä ja kyvykkyyttä, joilla voidaan tuottaa tehokkaita turvallisuusratkaisuja, jotka vaikuttavat organisaation sidosryhmiin, maineeseen, mielikuvaan ja arvoa tuottaviin toimintoihin.

Varautuminen tarkoittaa Yhteiskunnan turvallisuusstrategian (2017) mukaan toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesti poikkeavat toimenpiteet normaaliolojen häiriötilanteissa ja poikkeusoloissa. Varautumistoimenpiteitä on mm. valmiussuunnittelu, jatkuvuuden hallinta, etukäteisvalmistelut, koulutus ja valmiusharjoitukset. Varautuminen perustuu valmiuslain (L1552/2011), pelastuslain (L379/2011) ja muun erityislainsäädännön varautumisvelvollisuuteen. Varautumisen päämääränä on huolehtia onnettomuuksien ja häiriötilanteiden ehkäisystä, valmistautumisesta toimintaan niiden uhatessa tai sattuessa ja suunnitella toipuminen. Yhteiskunnan varautumisen tavoitteena on suojata elintärkeät toiminnot oikeusvaltioperiaate huomioon ottaen. (Turvallisuuskomitea 2017, 9)

Varautumisella tarkoitetaan toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen kaikissa tilanteissa. Varautumistoimenpiteitä ovat esimerkiksi riskien arviointi, jatkuvuus- ja valmiussuunnittelu, tekniset ja rakenteelliset etukäteisvalmistelut, koulutus, harjoitukset sekä tilojen ja kriittisten resurssien varaukset. Varautuminen jakaantuu suunnitteluun, sen edellyttämiin käytännön valmistelutoimenpiteisiin, näiden toteuttamiseen ja kehittämiseen sekä harjoitteluun. (VM 2016, 23)

Jatkuvuussuunnittelu - Osa kokonaisturvallisuutta	Varautuminen - Lakisääteistä toimintaa
Turvallisuusjohtaminen Riskienhallinta Jatkuvuuden hallinta Häiriötilanteiden hallinta ja johtaminen	Valmiussuunnittelu Jatkuvuuden hallinta Etukäteisvalmistelut Riskien arviointi

Tilannekuvan muodostaminen Huoltovarmuus Varautuminen	Jatkuvuussuunnittelu Valmiussuunnittelu Koulutus Valmiusharjoitukset Tilojen ja kriittisten resurssien varaukset

Taulukko 5: Jatkuvuussuunnittelun ja varautumisen ohjeellinen sisältö. (Turvallisuuskomitea 2017; VM 2016)

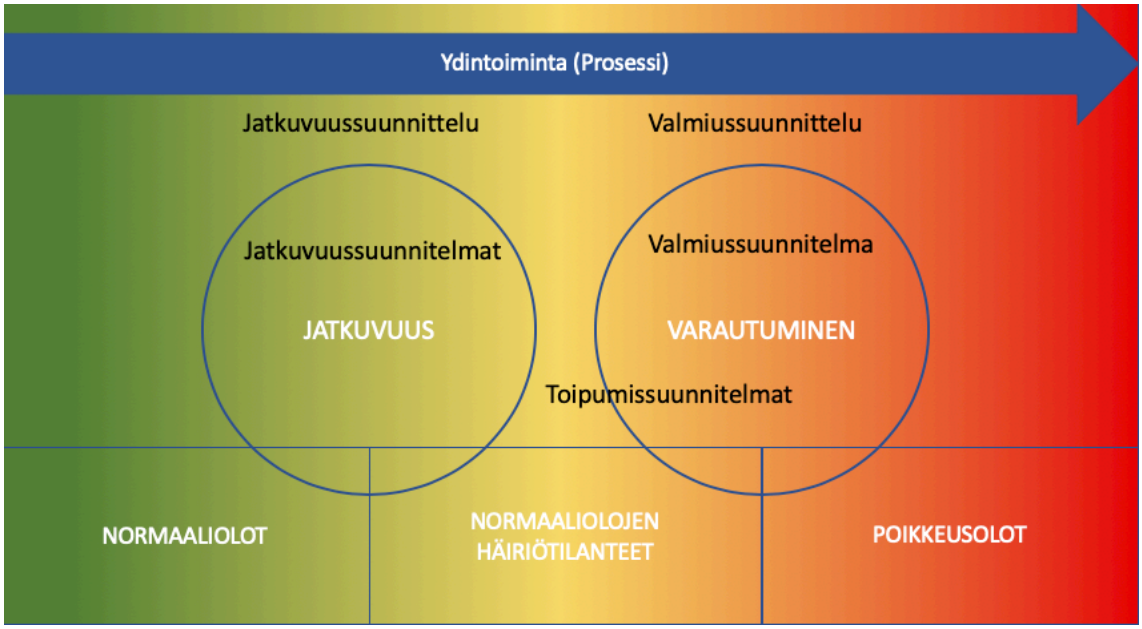
Taulukosta huomataan, että termistö on vaikeaselkoista ja moniselitteistäkin. Taulukossa esimerkiksi jatkuvuussuunnitteluun kuuluu varautuminen, kun samalla varautumiseen kuuluu jatkuvuussuunnittelu. Kirjoittaja on halunnut tällä taulukolla tuoda esille sen, että termistöä on paljon, eikä niiden riippuvuussuhteet ole kovin selkeitä. Yksittäisinä termeinä ne sen sijaan ovat helpommin ymmärrettäviä.

Jatkuvuuden hallinta voidaan kuitenkin ymmärtää yläkäsitteenä, jonka avulla varaudutaan normaaliolojen häiriöihin ja joka sisältää suunnitelmat, miten tästä häiriöstä palaudutaan normaaliin toimintaan. Jatkuvuuden hallinnan (normaaliolot) voidaan ajatella alla olevan kuvion mukaisesti johtavan varautumiseen häiriöihin (poikkeusolot) ja niistä toipumiseen (normaaliolojen häiriötilanne).

Kuvio 12: Jatkuvuuden hallinnan toimenpiteillä varaudutaan toiminnan häiriöihin ja niistä toipumiseen.

Jatkuvuuden hallintaa tehdään jatkuvuussuunnittelulla ja se sitä tehdään normaaliolojen aikana. Suunnitelmien tekeminen, niiden päivittäminen ja harjoittelu on osa organisaation riskienhallinnan vuosikellon mukaista toimintaa. Varautuminen tarkoittaa varautumista poikkeusoloihin ja se perustuu organisaation valmiussuunnitteluun. Poikkeusolojen jälkeen organisaatio siirtyy normaalioloihin toipumisen kautta. Tilanne on silloin normaaliolojen häiriötilanne, jolloin ollaan vasta palautumassa normaalioloihin, mutta ei vielä olla normaalitilassa.

Seuraavassa kuviossa on kuvattu jatkuvuussuunnitelman termien suhteita toisiinsa. Kuvio kertoo siitä, mitä erilaisia organisaation tekemät jatkuvuuden hallinnan suunnitelmia sovelletaan normaalioloihin, normaaliolojen häiriötilanteisiin sekä poikkeusoloihin.



Kuvio 13: Jatkuvuussuunnittelun ja valmiussuunnittelun termien ja määritelmien suhde toisiinsa. (Muokattu lähteestä VM 2016, 23)

Häiriöitä voi esiintyä sekä normaalioloissa, että poikkeusoloissa. Normaalioloissa häiriöt hallitaan viranomaisten tavanomaisin toimivaltuuksin tai voimavaroin. Normaalioloissa rakennettavat järjestelmät ja varautumistoimenpiteet luovat perustan toiminnalle poikkeusoloissa. Vastaavasti poikkeusolojen varalle luotuja järjestelyitä voidaan hyödyntää normaaliolojen häiriötilanteiden hallinnassa. Poikkeusoloissa tilanteen hallitseminen voi edellyttää lisätoimivaltuuksia tai voimavaroja. (Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J., Salminen, M. 2018, 15)

Valmiussuunnittelun tarkoituksena on varmistaa elintärkeiden toimintojen jatkuminen häiriötilanteissa ja poikkeusoloissa niin, että ihmisten elinmahdollisuudet, yhteiskunnan toimintakyky ja kansallinen itsenäisyys turvataan aina. Valmiuslain mukaan valtion viranomaisten, valtion liikelaitosten ja kuntien lakisääteinen velvollisuus on varmistaa tehtäviensä häiriötön hoitaminen kaikissa oloissa. (VM 2016, 24)

Jatkuvuussuunnittelu on osa varautumista mahdollisiin häiriöihin ja se tarkoittaa niitä toimia, joiden avulla pyritään pienentämään ja lyhentämään toimintaa haittaavien tapahtumien vaikutusta ja kestoa. Se sisältää varajärjestelyjä sekä toimenpiteitä, jotka parantavat toimintaa häiriötilanteissa tai toipumista ongelmien jälkeen. Jatkuvuussuunnittelu sisältää myös suunnitelmat, joissa kuvataan johtaminen, vastuut ja toimenpiteet, joiden mukaan toimintoja voidaan jatkaa erilaisissa häiriötilanteissa. (VM 2016, 24)

Toipumissuunnitelmat kuvaavat operatiivisella tasolla ja konkreettisesti järjestelmien palauttamista häiriötilanteista. Ne sisältävät ohjeet vakavasta häiriöstä toipumiseen, normaaliin

toimintaan paluusta ja toiminnan jatkamisesta. Jatkuvuussuunnitelma ohjaa toipumissuunnitelmien toteutusta. (VM 2016, 24)

Jatkuvuuden hallinnan yksi näkyvä ulottuvuus on organisaation vuosikello, joka kertoo vuoden aikana tapahtuvien toimenpiteiden aikataulun ja toimii muistilistana. Vuosikello voidaan esittää sanallisena tai kuvana ja sitä käytetään pidemmän aikajakson tapahtumien hahmottamiseen kokonaisuutena. (VM 2016, 27)

2.8.1 Tilannekuva

Jatkuvuuden hallinnassa tilannekuvan muodostamisella tavoitellaan oikeaa ja oikea-aikaista tilannetietoisuutta eri lähteistä saadun informaation perusteella, jotta voidaan soveltaa mahdollisimman optimaalisia toimenpiteitä juuri silloin kun niitä tarvitaan. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisu Kyberturvallisuuden strateginen johtaminen Suomessa (2018) kertoo tilannekuvan olevan tarpeen perusteella valittu yksittäisistä tiedoista koottu esitys tilanteesta ja suorituskyvystä, mikä antaa perusteet tilannetietoisuudelle. Vastaavasti tilanneymmärrys on päättäjien ja heitä avustavien henkilöiden ymmärrys tapahtuneista asioista, niihin vaikuttaneista olosuhteista, eri osapuolten tavoitteista ja tapahtumien kehitysvaihtoehdoista, joita tarvitaan päätösten tekemiseksi tietystä asiasta tai asiakokonaisuudesta” (Lehto ym. 2018, 38).

Tilannekuva on kaksitahoinen. Ensiksi se on yhteinen turvallisuustilannetta kuvaava reaaliaikainen kuva vallitsevista tapahtumista. Tieto tilannekuvaa varten kootaan havaintojärjestelmistä, julkisista lähteistä ja organisaation omista tietolähteistä. Toiseksi tilannekuva sisältää nykytilan analyysin ja arvion tulevista tapahtumista. Tilannekuva antaa kokonaiskäsityksen siitä, mitä on tapahtunut, tapahtumassa tai tulee tapahtumaan. (Lehto ym. 2018, 39)

Valtion tasolla valtioneuvoston kanslian tehtäviin kuuluu antaa valtioneuvoston yhteinen tilannekuva, jota käytetään päättäjien informoimiseksi. Valtioneuvoston kanslia vastaa myös varautumisesta ja turvallisuudesta sekä sovittaa yhteen häiriötilanteiden hallinnan. Suomessa valtioneuvoston kanslia on siis keskeinen toimija, kun puhutaan valtion turvallisuudesta ja tilannekuvasta. Olennainen osa tilannekuvaa on onnistunut ja oikea-aikainen viestintä. (VNK 2019)

Voidakseen tehdä oikeita ratkaisuja päätöksentekijöiden on tiedettävä päätöstensä perusta, seuraukset sekä se miten muut niihin reagoivat ja mitä riskejä päätöksiin sisältyy. Tästä syystä päätöksentekijöillä tulee olla kaikilla toimintatasoilla riittävä tilannetietoisuus ja -ymmärrys, joka on lähtökohta oikea-aikaiseen päätöksentekoon ja toimintaan. (Lehto ym. 2018, 40)

Kriisin keskellä on vaikea tai mahdotonta arvioida, tehdäänkö juuri sillä hetkellä oikeita asioita. Tilannetietoisuus lisää todennäköisyyttä, että tehdään oikein mitoitettuja ja oikeansuuntaisia asioita, mutta tilanteen arviointia tai syitä tilanteen syntymiselle ei kannata etsiä tilanteen ollessa päällä. Kriisin seuraukset ja vaikutukset ovat tärkeämpiä kuin se miksi kriisi on syntynyt tai ketä on syyllinen. Niiden aika tulee vasta jälkeenpäin.

2.8.2 Jatkuvuuden hallintajärjestelmä

Jatkuvuuden hallintajärjestelmän muodostavat kaikki ne prosessit, toimenpiteet, työkalut ja suunnitelmat, joiden avulla varmistetaan organisaation toiminnan jatkuvuus. Hallintajärjestelmä perustuu jatkuvaan kehittämiseen, vaatimusten seuraamiseen ja päivittämiseen. Siihen rakennetaan mekanismit, joilla tunnistetaan uusien sidosryhmien vaatimukset ja pystytään vastaamaan muuttuneeseen toimintaympäristöön. Jatkuva kehittäminen ja toiminnan optimointi perustuvat suunnittelulle asetettuihin tavoitteisiin ja mittareihin, joita tarkastellaan säännöllisesti. (VM 2016, 29)

Jatkuvuuden hallinnan onnistumiseksi tulee organisaation määritellä ja tunnistaa kriittiset toimintonsa. Kun ne on tunnistettu, niihin voidaan kohdistaa suunnittelun kannalta tärkeitä toimenpiteitä, kuten riskienhallinnan ja toiminnan keskeytysanalyysi. Ei ole mielekästä tai kustannustehokasta toteuttaa jatkuvuussuunnittelua kaikelle toiminnalle tai kompteneteille, jotka eivät ole kriittisiä tai toteuta organisaation ydintehtävää. (VM 2016,29)

2.8.3 Jatkuvuuden hallinnan johtaminen

Johtaminen on elintärkeä toiminto, joka luo pohjan muiden toimintojen turvaamiselle. Johtamiskyky on kyettävä turvaamaan kaikissa tilanteissa ja kaikilla toimintatasoilla. Tehokas häiriötilanteiden hallinta edellyttää tiivistä yhteistyötä johtamisen, tilannekuvan ja viestinnän välillä. (Turvallisuusstrategia 2017, 15)

Johtaminen on kiinteä osa varautumista ja valmiutta. Elintärkeisiin toimintoihin kohdistuvien uhkien hallinta edellyttää kaikkien tarvittavien turvallisuustoimijoiden yhteistoimintaa johtamisen tukena. Varoitus- ja ennakointijärjestelmien tiedon jakaminen hyvissä ajoin edesauttaa häiriötilanteiden ennaltaehkäisyä ja vähentää haittavaikutuksia. (Turvallisuusstrategia 2017, 15)

VAHTI ohjeen 2/2016 (VM 2016, 31) mukaan jatkuvuuden hallinnan onnistumisen edellytys on johdon sitoutuminen ja tuki. Jatkuvuuden hallinnan vastuuhenkilöt ovat johdon nimeämät ja toimintojen, palvelujen ja prosessien omistajien vastuulla on, että toiminnassa huomioidaan jatkuvuuden vaatimat toimenpiteet. Vastuuhenkilön tehtävä on esitellä jatkuvuuden hallinnan keskeisimmät suunnitelmat johdolle, joka hyväksyy ne mahdollisten muutosten jälkeen.

Toimintojen omistajat puolestaan nimeävät ja valtuuttavat organisaatiossa ne, jotka vastaavat jatkuvuuden hallinnan käytännön toimenpiteistä.

Ylimmän johdon tulee hyväksyä jatkuvuuden hallinnan periaatteet tai linjaukset, jotka ovat organisaation ydintehtävien mukaiset ja varmistavat jatkuvan kehittämisen. Periaatteet tulee dokumentoida ja niiden tulee olla selkeitä ja helposti ymmärrettäviä. Jatkuvuuden hallinnan periaatteet ovat johtamisen näkökulmasta seuraavat:

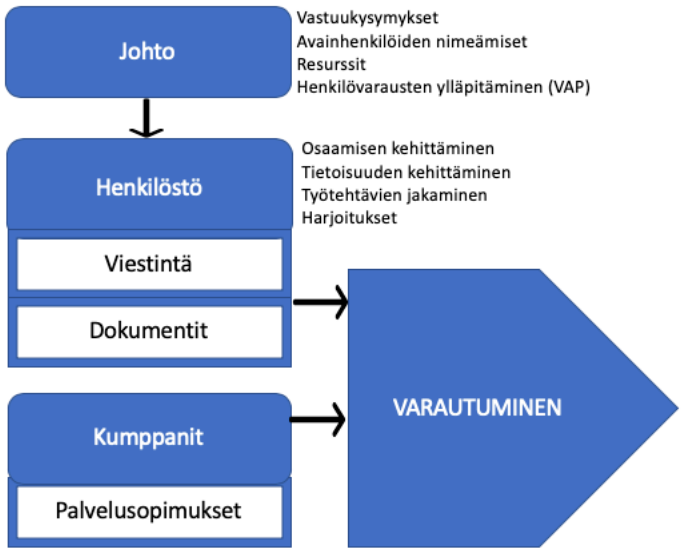
- Johdon sitoumus
- Linkitys organisaation strategiaan
- Vaatimukset (ml. säätely) jatkuvuuden hallinnalle
- Jatkuvuuden hallinnan tavoitteet
- Sitoutuminen jatkuvuuden hallinnan jatkuvaan parantamiseen
- Roolit ja vastuut jatkuvuuden hallinnan johtamiselle
- Viittaukset tarkentaviin periaatteisiin tai ohjeisiin.

Yhteiskunnan turvallisuusstrategian (2017, 15) mukaan hyvä jatkuvuuden hallinnan johtaminen edellyttää

- Selkeää johtovastuuta, toimijoiden roolitusta ja toimivaltaisten viranomaisten päätöksentekokykyä
- Kriisiviestintää
- Tiedon jakamista ja sitä tukevia teknisiä ratkaisuja
- Toiminnan jatkuvuuden hallintaa
- Yhteistoimintaa.

Yhteiskunnan elintärkeitä toimintoja uhkaavien häiriötilanteiden hallinta nojautuu kokonaisturvallisuuden mallin mukaisesti mahdollisimman kattavaan yhteistyöhön viranomaisten paikallishallinnon, eri hallintoalojen ja ministeriöiden sekä elinkeinoelämän välillä ja muiden turvallisuustoimijoiden tukemiseen.

Seuraavassa kuvassa on tiivistetty edellä mainittujen periaatteiden mukaisesti esimerkki siitä, kuinka jatkuvuuden hallinta voidaan organisoida ja vastuuttaa, jotta koko henkilöstö voidaan osallistaa varautumiseen.



Kuvio 14: Organisaation jatkuvuuden hallinnan tekijät. (Muokattu lähteistä Turvallisuusstrategia 2017; VM 2016)

VAHTI ohjeen 2/2016 mukaan (VM 2016, 37) organisaation ydintoimintojen kriittiset erityisosaamiset on huomioitava henkilöstön osaamisvaatimuksissa, koulutuksessa, palvelujen hankinnassa ja resursoinnissa. Kriittisistä tehtävistä vastuulliset avainhenkilöt koulutetaan toimimaan häiriötilanteissa jatkuvuus- ja toipumissuunnitelmien mukaisesti. Jatkuvuuden hallinnan resurssointi tulee tarkistaa säännöllisesti sekä varmistaa henkilöresurssien ja osaamisen saatavuus häiriötilanteiden ja poikkeusolojen varalle. Oleellinen tehtävä on myös henkilövarausten (VAP) ylläpito omassa organisaatiossa sekä palveluja tuottavassa yritysverkostossa alihankintaketjuineen (Kumppanit).

Johdon rooli on kuvattu tarkemmin Vahti -ohjeen (VM 2017a, 14) riskienhallinnan johtamisen kontekstissa. Seuraavassa kuvassa on havainnollistettu organisaation toiminnan ja riskienhallinnan yhteys sekä johdon tehtävät ja rooleja. Tavoitteiden saavuttaminen ja toiminnan onnistuminen edellyttää kunnossa olevaa perustaa sekä toimivaa riskienhallintaa. Johto on näiden edistämisessä keskeisessä asemassa.

Kuvio 15: Johdon tehtävät ja roolit riskienhallinnassa. Käytettävissä olevat resurssit sekä niiden ohjaaminen ja kehittäminen vaikuttavat olennaisesti riskienhallinnassa onnistumiseen. (Muokattu lähteestä VM 2017a, 14)

Organisaation ydintehtävä muodostuu lakisääteisistä tehtävistä, strategisista tavoitteista, tulostavoitteista ja vuosisuunnittelusta. Se määrittelee viraston toiminnan puitteet ja reunaehdot, jolla se toteuttaa sille annettua tehtävä. Riskienhallinnan kokonaisuus on johdon vastuulla. Sen sitoutuminen, osallistuminen ja toimenpiteiden suunnittelu ja toteuttaminen sekä resurssien nimeäminen ja hyväksyminen muodostaa rungon organisaation riskienhallinnalle. Johto arvioi riskien negatiivisia ja positiivisia puolia päätöksentekonsa pohjaksi. Riskienhallinnassa johto laatii riskienhallintapolitiikan ja tukeutuu asiantuntijoihin, jotka käyttävät organisaation riskienhallinnan työkaluja sekä valtiohallinnon ohjeistusta ja riskienhallinnan standardeja laatiakseen organisaation riskikuvan johdon käyttöön. Organisaation perusta tulee olla kunnossa. Sen varmistaa sisäinen tarkastus ja se ilmenee lakien noudattamisen ja toiminnan turvallisuuden kautta. Organisaation johto varmistaa, että turvallisuuden osa-alueet ovat kunnossa, tietosuoja-asiat on otettu huomioon ja että toiminnan häiriötilanteisiin on varauduttu ja jatkuvuus varmistettu.

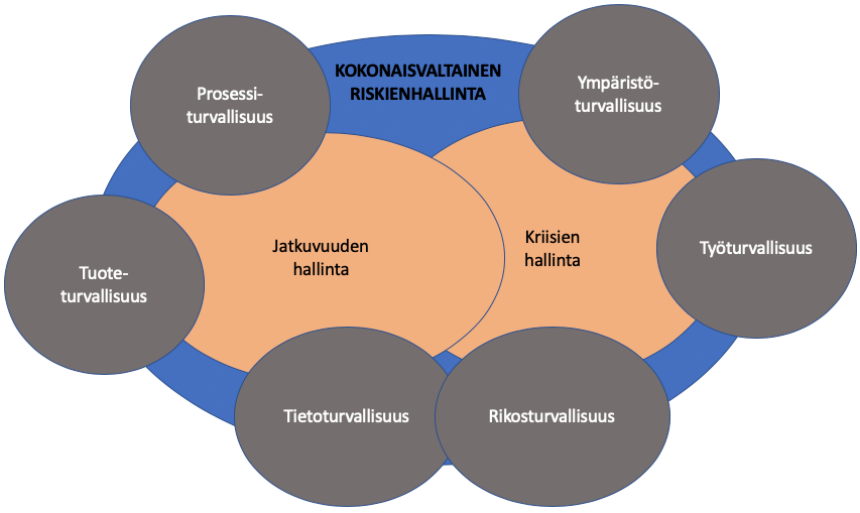
Laadunhallinnan standardi SFS-ISO 9000 (2015, 15) mukaan organisaation johtamisjärjestelmän eri osat, kuten sen laadunhallintajärjestelmä, voidaan liittää yhdeksi johtamisjärjestelmäksi. Laatuun, kasvuun, rahoitukseen, kannattavuuteen, ympäristöön, työterveyteen ja työturvallisuuteen, energiaan, turvallisuuteen ja muihin organisaation johtamisen osa-alueisiin liittyvät tavoitteet voidaan saavuttaa ja prosesseja ja resursseja käyttää vaikuttavammin ja tehokkaammin, kun laadunhallintajärjestelmä yhdistetään muihin hallintajärjestelmiin.

Turvallisuus ja riskienhallinta ovat organisaation keskeisiä johtamisen toimintoja ja ne lisäävät organisaation laatua. Yhdistämällä ne laadunhallintajärjestelmän kanssa muiden toimintojen lisäksi johtamisjärjestelmään, saadaan kattava kokonaisuus.

Vuonna 2019 voimaan tullut Laki julkisen hallinnon tiedonhallinnasta edellyttää, että tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on (4§, kohta 2) ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta ja (4§, kohta 5) järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta. (L906/2019)

Valtion virastona ja tietotalona Terveyden ja hyvinvoinnin laitoksen on huolehdittava siitä, että se, johto ja henkilöstö on riskienhallinnalla varautunut erilaisiin häiriö- ja kriisitilanteisiin ja poikkeusoloihin ja että se kykenee jatkaa toimintaansa näiden aikana ja niiden jälkeen, kun tilanne normalisoituu.

Kokonaisvaltainen riskienhallinta sitoo yhteen turvallisuuden osa-alueet ja jatkuvuuden hallinnan. Ilmonen ym. (2016, 41) kuvaa tätä kokonaisuutta seuraavalla kuviolla:



Kuvio 16: Kokonaisvaltainen riskienhallinta on moniulotteinen kokonaisuus, joka pitää johdon toimesta pitää tasapainossa turvallisuuden osa-alueiden kanssa. (Ilmonen 2016, 41)

Kokonaisvaltainen riskienhallinta muodostaa perusta turvallisuusjohtamiselle, jossa organisaation turvallisuuden osa-alueet sidotaan yhteen jatkuvuuden hallinnan ja erilaisten kriisien hallinnan kanssa. Organisaatio kohtaavista normaaliolojen poikkeusoloista huolimatta, tulee organisaation johdon varmistaa, että turvallisuuden eri osa-alueet on otettu huomioon poikkeusolojen aikana ja niistä toipumisessa. Ilmosen ym. mukaan (2016, 40-41) liian heikko riskienhallinta aiheuttaa organisaatiolle pahimmillaan suuria menetyksiä, ja vastaavasti riskeihin nähden ylimitoitettu riskienhallinta kuluttaa resursseja ilman riittävää tuottoa. Riskienhallintaa voidaankin kuvata prosessina tai kulttuurina eli pelisääntöinä siitä, kuinka riskejä hallitaan ja niistä raportoidaan.

3 Turvallisuuden johtamisen mallit

Turvallisuuden johtaminen on monisäikeinen tehtävä ja organisaation koosta (keskisuuret ja suuret) tai toimialasta riippumatta sisältää tiettyjä elementtejä, joita on edellä kuvattu. Turvallisuusjohtamisen mallin kuvaaminen on haastava tehtävä, mutta se kertoo siitä, miten kompleksinen turvallisuusjohtamisen kenttä on, ja millaista ammattitaitoa turvallisuuden johtaminen vaatii.

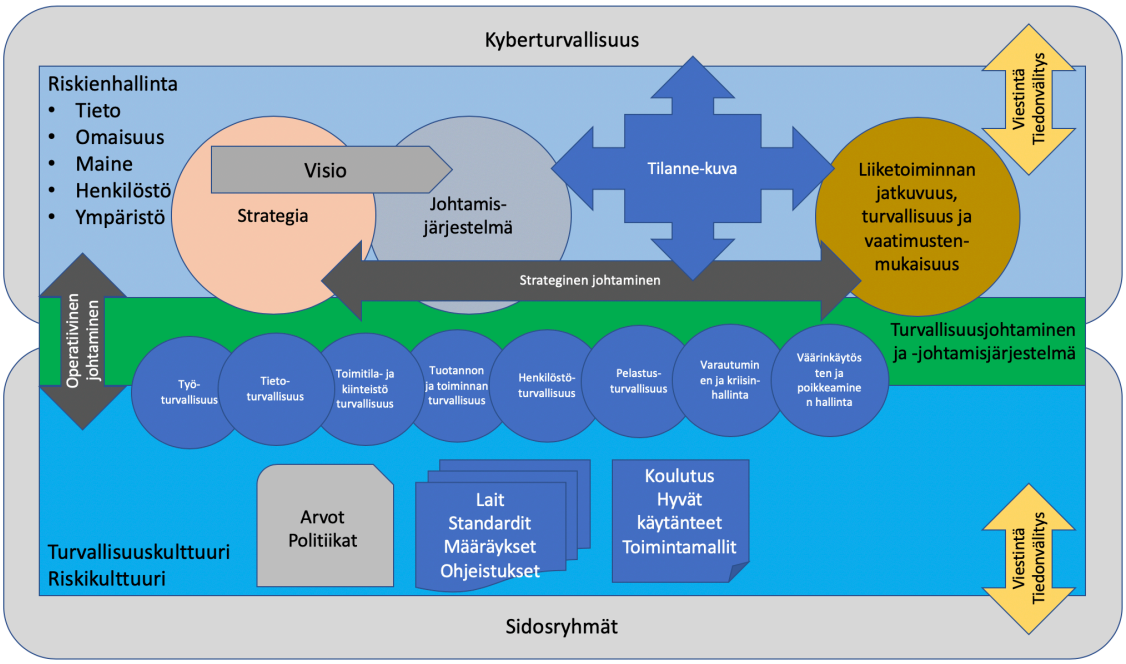
Tämä opinnäytetyö käsittelee turvallisuuden johtamisen kehittämistä Terveyden ja hyvinvoinnin laitoksella. Tässä kappaleessa olen luonut teoreettisen viitekehyksen pohjalta kolme eri mallia, joilla kuvataan turvallisuuden johtamista erityisesti valtiohallinnon näkökulmasta, mutta myös yleisesti. Mallit eivät ole toistensa vaihtoehtoja, vaan tukevat toisiaan ja muodostavat kokonaisuuden, josta kokonaisvaltainen turvallisuuden johtaminen kirjoittajan mielestä koostuu.

Ensimmäinen malli on ”iso kuva” turvallisuuden johtamisesta, jossa kirjoittaja on yhdistänyt eri periaatteita yhteen kuvaan. Toisessa mallissa kirjoittaja on aikaisemmin esitettyyn kuvioon liittänyt turvallisuusjohtamista, riskienhallintaa ja organisaation johtamisjärjestelmää tukevia elementtejä, jotta turvallisuusjohtamisen kokonaisvaltaisuus ja organisaation kahden keskeisen ryhmän kontribuutio siihen korostuisi. Huomautettakoon, että tässä erityisesti tulee esille valtiohallinnon organisaatiomalli, koska yksityisellä puolella voi olla ihan erilaisia ja eri kokoonpanolla olevia ryhmiä, joiden tehtävä koskevat kokonaisvaltaista turvallisuuden hallintaa ja organisaation valmiuden ylläpitoa. Turvallisuuden johtaminen perustuu erityisesti riskienhallintaan ja saa riskienhallinnan kautta toiminnan puitteet. Kirjoittaja on kolmannessa mallissa korostanut SFS-ISO 31000 standardin mukaisen riskienhallinnan puitteiden osa-alueiden merkitystä turvallisuuden johtamiseen. Kirjoittaja on nostanut kolme keskeisintä periaatetta, joiden pohjalta turvallisuuden johtaminen ja riskienhallinta yhdistyvät. Erityisesti nousee esille, että turvallisuuden johtaminen on tiedolla johtamista ja että tiedon tuottajana riskienhallinta on keskeinen.

Terveyden ja hyvinvoinnin laitos kuuluu sosiaali- ja terveysministeriön (STM) hallinnon alaan ja tästä syystä erillisessä kappaleessa tarkastelen vielä turvallisuuden johtamista sosiaali- ja terveysministeriön hallinnon alalla.

3.1 Kokonaisvaltaisen turvallisuuden johtamisen malli

Kirjoittaja on seuraavassa kuviossa kuvannut turvallisuuden johtamisen mallin yhdistäen Elinkeinoelämän keskusliiton, riskienhallinnan ja johtamisjärjestelmän yhteensopivaksi kokonaisuudeksi ja liittänyt siihen myös turvallisuuskulttuurin ja kyberturvallisuuden elementit. Malli on kirjoittajan oma ja pyrkii yhdellä kuvalla kuvaamaan turvallisuuden johtamisessa huomioon otettavat elementit.



Kuvio 17: Kokonaisvaltaisen turvallisuuden johtamisen malli

Turvallisuuden johtamisen perustana on riskienhallinta, organisaation visio ja arvot sekä strategia, jota tukee johtamisjärjestelmä ja hallintajärjestelmät (kuten VAHTI -julkaisut). Näiden lisäksi liiketoiminnan jatkuvuus, turvallisuus ja vaatimustenmukaisuus on turvallisuusjohtamisen ja turvallisuusjohtamisjärjestelmän perusta. Turvallisuuden johtaminen huomioi kaikki Elinkeinoelämän keskusliiton turvallisuuden osa-alueet (nämä vaihtelevat jonkin verran organisaatiosta riippuen) ja tavoitteena on turvallisuuskulttuurin kehittyminen. Sen perustana ovat organisaation arvot ja politiikat sekä lait standardit, (valtiohallinnon) määräykset, ohjeistukset että henkilöstön tarkoituksenmukainen koulutus. Viestintä ja tiedonvälitys sidosryhmien kanssa on olennainen osa turvallisuuskulttuurin muodostamisessa ja muodostumisessa.

Turvallisuuden johtaminen on sekä strategista, että operatiivista johtamista. Turvallisuuden johtaminen on jatkuvassa muutoksessa ja tulee muuttua ja kehittyä ympäristön muutosten mukaisesti. Organisaation johdolla on oltava ajantasainen tilannekuva, joka pohjautuu riskienhallintaan, kyberturvallisuus tilanteeseen, hallintajärjestelmien soveltamiseen sekä liiketoiminnan jatkuvuuden, turvallisuusvaatimusten ja vaatimustenmukaisuuden luomaan kokonaisuuteen. Viestinnällä ja tiedonvaihdolla on olennainen osa sidosryhmien ja organisaation lisäksi kyberturvallisuuteen liittyvällä tiedolla ja riskienhallinnan välillä. Kyberturvallisuuteen liittyvä tieto ovat esim. sähkönjakelun häiriöt, tietoverkon häiriöt ja siihen kohdistuvat hyökkäykset ja häirinnät, mobiiliverkon toiminnan häiriöt ja vikatilanteet ja kaikki sellainen tieto, joka yhdistää bittien maailman ja fyysisen maailman siten, että häiriöt toisessa on uhka toisen toiminnalle ja sitä kautta organisaation ja sidosryhmien toiminnalle.

3.2 Turvallisuuden johtaminen osana organisaation johtoa

Kappaleessa 2.3 ”Riskienhallinta turvallisuusjohtamisen kontekstissa” on kuviossa 3 esitetty turvallisuusjohtamisen ja riskienhallinnan suhdetta organisaation johtamisjärjestelmään (Virta 2014). Kirjoittaja on seuraavassa kuviossa lisännyt tähän näiden suhteet organisaation strategiseen johtamiseen, valmiusryhmään ja turvallisuusryhmän sekä nuolet siihen miten organisaatiokulttuuri vaikuttaa turvallisuusjohtamiseen riskienhallinnan kautta ja turvallisuuskulttuuri taas organisaatiokulttuuriin turvallisuusjohtamisen ja riskienhallinnan kautta.

Kuvio 18: Turvallisuuden johtamisen kokonaisuus ja kulttuurien vaikutus siihen (Muokattu lähteestä Virta 2014)

Turvallisuusryhmä vastaa organisaation kokonaisturvallisuudesta ja valmiusryhmä erityisesti organisaation valmiuteen keskittyvä ryhmä. Valmiusryhmä huolehtii siitä, että organisaation toiminnot säilyvät normaaliolojen häiriötilanteissa ja poikkeusoloissa. Turvallisuusryhmä on turvallisuusjohtamisen avaintekijä. Sen kautta saadaan turvallisuusjohtamiseen sekä eri alojen ammattilaisten osaamista (vrt. Elinkeinoelämän turvallisuuden osa-alueet) että tietoa organisaation tilannekuvaan. Turvallisuuden johtaminen on ennen kaikkea viestintää ja yhteistyötä ja turvallisuusryhmä sekä saa tietoa eri osastojen, yksiköiden ja toimintojen tilanteesta, että välittää tietoa organisaation eri osa-alueille. Valmiusryhmän toiminnan liittäminen turvallisuuden johtamiseen on ennakointia häiriötilanteiden hallinnassa. Valmiusryhmässä on erityisosaamista esim. laboratorioiden jatkuvuuden hallinnan suunnittelusta ja ryhmässä

käsitellään asioita, joita ei välttämättä niiden arkaluonteisuuden takia ole löydettävissä muissa foorumeissa, kuten intranetissä. Siksi on olennaista, että valmiusryhmä toimii turvallisuuden johtamisen ytimessä ja antaa näin tietoa sekä tilannekuvaan, että häiriötilanteiden hallintaan koko organisaation laajuisesti. Projektitoimisto (PMO) vastaa siitä, että projekteihin liittyvät riskit tulevat osaksi organisaation kokonaisvaltaista riskienhallintaan.

Organisaatiokulttuuri vaikuttaa turvallisuuteen johtamisjärjestelmän kautta. Turvallisuuskulttuuri luodaan turvallisuusjohtamisen avulla ja siihen tulee syötettä riskienhallinnasta. Kuviossa turvallisuuskulttuurin nuoli lähtee kokonaisvaltaisen turvallisuusjohtamisen alueelta ja läpäisee riskienhallinnan kokonaisuuden. Se vaikuttaa johtamisjärjestelmään ja leviää sitä kautta koko henkilöstöön ja tulee osaksi organisaatiokulttuuria.

3.3 Riskienhallinnan periaatteet turvallisuuden johtamisessa

SFS-ISO 31000 linjaa riskienhallinnan periaatteet, jotka on käsitelty kappaleessa 2.3.1. Riskienhallinnan periaatteiden mukaisesta kuviosta kirjoittaja on korostanut kolme tärkeintä kohtaa, jotka erityisesti nousevat esille turvallisuuden johtamisessa. Turvallisuuden johtamisessa riskienhallinnan periaatteista nousee esille tavoite, että riskienhallinta on organisaation johtamisjärjestelmään sisällytetty. Sen kautta varmistetaan, että organisaation johto on sitoutunut riskienhallintaa ja että riskienhallinnan näkökulma otetaan huomioon strategisessa johtamisessa ja jokapäiväisessä operatiivisessa johtamisessa. Toinen turvallisuuden johtamisen onnistumista edistävä tekijä on, että riskienhallinnassa sidosryhmät ovat mukana sekä riskien havaitsemisessa, että viestinnän ja tiedonvälityksen kumppaneina. Tällä varmistetaan se, että turvallisuuden johtamisessa käytössä riittävästi tietoa tilannekuvan muodostamiseen ja sen avulla johtamiseen. Kolmanneksi kohdaksi on kirjoittaja nostanut parhaan saatavilla olevan tiedon merkityksen turvallisuuden johtamisessa. Tiedolla johtaminen edellyttää, että käytössä oikea tieto oikeaan aikaan. Tietoa tulee valtavasti eri kanavista, mutta turvallisuuden johtamisessa pitää voida erottaa olennainen tieto kohinasta. Pitää myös olla keinot tiedon analysointiin, jotta paras saatavilla oleva tieto on käytettävissä oikeaan aikaan ja oikeassa muodossa. Edellä mainituista syistä riskienhallinnan periaatteista turvallisuuden johtamisen näkökulmasta nousee kolmeksi tärkeimmäksi tekijäksi, että riskienhallinta on sisällytetty organisaation johtamisjärjestelmään, se ottaa mukaan sidosryhmät ja että siinä käytetään parasta saatavilla olevaa tietoa.

Kuvio 19: Turvallisuuden johtaminen riskienhallinnan periaatteiden näkökulmasta. (Muokattu lähteestä SFS-ISO 31000, 8)

Keskiössä on organisaation arvon luominen ja säilyttäminen ja tämä päämäärän saavuttamiseksi on riskienhallinta oltava integroitu organisaation johtamisjärjestelmään. Organisaation johdon tulee jatkuvasti olla tietoinen riskienhallinnan tilanteesta ja tarvittaessa kyetä vaikuttamaan organisaation toimintaan niin, että tunnistetut riskit kyetään hallitsemaan.

Riskienhallinta on yhteistyötä ja nykypäivän verkottuneessa yhteiskunnassa jatkuva tiedonvaihto sidosryhmien kanssa on tärkeää näkemysten, tietämyksen sekä havaintojen huomioon ottamisen kannalta. Sillä varmistetaan, että organisaation tilannekuva perustuu parhaaseen sillä hetkellä saatavilla olevaan tietoon ja toimenpiteet ovat oikea-aikaisia ja oikean suuruisia.

Turvallisuuden johtaminen on erityisesti tiedolla johtamista. Paras saatavilla oleva tieto tulee monesta eri lähteestä. Sidosryhmien lisäksi organisaation tulee olla yhteydessä sekä kansallisiin, että kansainvälisiin oman alan toimijoihin, viranomaisiin, tutkimuslaitoksiin sekä turvallisuusalan yhdistyksiin ja muihin kolmannen sektorin toimijoihin. Näiden lisäksi tulee tietoa kerätä verkkosivuilta, sosiaalisesta mediasta, artikkeleista, alan lehdistä sekä myös turvallisuuden pimeältä puolelta, joka tänä päivänä tarkoittaa erilaisia internetin ”dark web” sivustoja, keskustelupalstoja ja sosiaalisen median lukuisia alustoja. Tiedon keräämisen pitää siis olla laajempaa kuin tilannekuvan kautta saatu tieto, joka tulee erilaisista raporteista, lokitiedoista, sidosryhmien ja osastojen turvallisuusvastaavien (jos sellaisia on) kautta sekä virallisia

kanavia pitkin. Turvallisuusjohtamisen onnistumiseksi ”anturit” pitää ulottaa syvälle erilaisiin ympäristöihin.

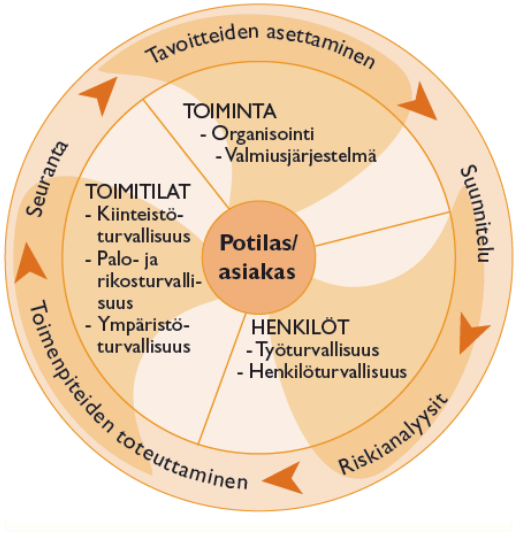
3.4 Turvallisuuden johtaminen Sosiaali- ja terveysministeriön hallinnon alalla

Sosiaali- ja terveysministeriön (STM) julkaisu Riskienhallinta ja turvallisuussuunnittelu (2011) ottaa kantaa kokonaisturvallisuuden johtamiseen toteamalla, että organisaatiossa tai toimintayksikössä tulee olla nimettynä turvallisuuden kokonaisuudesta perillä oleva henkilö, joka myös koordinoi turvallisuustoimintaa. Tämä henkilö voi hoitaa tehtäviä oman toimensa ohella, osa-aikaisesti tai päätoimisesti. Organisaation turvallisuudesta vastaavan henkilön tehtäväkenttään voi organisaation koosta riippuen kuulua mm. seuraavia tehtäviä:

- Valmiussuunnittelu, varautuminen, jatkuvuussuunnittelu
- Riskienhallinnan ja sisäisen valvonnan menetelmät
- Vakuutettavien riskien hallinta
- Henkilöturvallisuus, vartiointi, rikosasioiden selvittely
- Paloriskit, kiinteistö- ja tilaturvallisuus
- Tietoturvallisuus ja tietosuoja
- Työsuojelu

Pitkäjänteinen turvallisuuden kehittäminen sekä riskien ja vaarojen ennakointi ja hallinta edellyttävät laaja-alaista asiantuntemusta. Erityisesti suurissa sosiaali- ja terveydenhuollon organisaatiossa on suositeltavaa nimetä päätoiminen asiantuntija tai asiantuntijoita huolehtimaan turvallisuuskenttään kuuluvista vastuista. Näitä tehtäviä hoitavalla on oltava riittävä osaaminen ja koulutus sekä mahdollisuus vaikuttaa turvallisuuden ohjaamiseen ja tarvittavia resursseja koskevaan päätöksentekoon. (STM 2011, 13-14)

Sosiaali- ja terveydenhuollolla on edellä mainittua toimintamallia tukeva riskienhallintamalli, jossa kuvataan eri osa-alueiden suhdetta toisiinsa.



Kuvio 20: Sosiaali- ja terveydenhuollon riskienhallintamalli (STM 2011, 10)

Mallissa keskiössä on potilas tai asiakas ja turvallisuuden johtaminen on jaettu kolmeen pääluokkaan ja niiden alaluokkiin. Turvallisuusjohtamisen kokonaisuutta kehitetään jatkuvasti perustuen löysästi Demingin ympyrään (Plan-Do-Check-Act). Toimitiloja, toimintaa sekä henkilöitä koskevat riskit tulee tunnistaa, arvioida ja ryhtyä tarvittaviin toimenpiteisiin niiden hallitsemiseksi, jotta voidaan turvata (hoito)ympäristön häiriöttömyys ja toiminnan jatkuvuus.

4 Turvallisuus ja riskienhallinta Terveyden ja hyvinvoinnin laitoksella

Tässä kappaleessa kuvataan opinnäytetyön tutkimuksen ja kehittämisen kohteena oleva organisaatio. Kuvaus on synteesi, joka perustuu organisaation verkkosivuun (THL organisaatio; THL strategia; THL 2020) ja sisäisiin dokumentteihin (THL työjärjestetys) sekä opinnäytetyön tekijän omiin havaintoihin ja työkemukseen kohdeorganisaatiossa. Kirjoittaja itse työskentelee Terveyden ja hyvinvoinnin laitoksella, jonka johdosta hänellä on mahdollisuus nähdä lähtökohtaisesti kaikki intranetin aineisto ja saada näin laaja kuva laitoksen turvallisuuteen liittyvistä dokumenteista ja muistioista, joiden käyttöä ei ole rajattu vain tietylle ryhmälle. Kirjoittajan työtehtävät eivät kuitenkaan tällä hetkellä suoraan liity turvallisuuteen, joten lähteinä ovat olleet intranet sivustot, asiakirjat ja muistiot, joita täydennettiin turvallisuusasiantuntijoiden teemahaastatteluilla.

Tieto on Terveyden ja hyvinvoinnin laitoksen tärkein omaisuus, mutta voidaan kuitenkin todeta, että asiantuntijuus on tärkein ominaisuus, koska pelkkä tiedon tuottaminen ei riitä vaan sitä pitää tulkija ja soveltaa. Tietotalona riskienhallinnalla ja tiedon suojaamisella on luonnollisesti suuri merkitys.

Riskienhallinta on hajautettu eri osastoille, mutta koko virastossa noudatetaan yhteneväistä riskienhallintapolitiikkaa, joka on juuri uudistettu ja tullut käyttöön vuoden 2019 joulukuussa. THL:ssä on keskitetty riskienhallintafoorumi ja se kokoontuu harvoin, mutta säännöllisesti. Kokouksessa käydään läpi eri osastoiden määrittelemiä riskejä ja ne kirjataan sähköiseen Granite-nimiseen järjestelmään. Tällä hetkellä Graniteen kirjautuneet riskit ovat pääasiassa työsuojeluun liittyviä ja tarkoitus on laajentaa se koskemaan kaikkia riskejä.

Terveyden ja hyvinvoinnin laitoksen riskienhallintapolitiikan (Riskienhallintapolitiikka 2019) tehtävä on määritelty seuraavasti: ”Riskienhallintapolitiikassa määritellään Terveyden ja hyvinvoinnin laitoksen (THL) periaatteet, joiden avulla varmistetaan toimintaan ja tavoitteisiin kohdistuvien riskien hallinta ja mahdollisuuksien tunnistaminen toiminnan parantamiseksi.” Riskienhallintapolitiikka antaa ylätason suuntaviivat, jonka avulla on laadittu tarkempia ohjeita ja käytänteitä riskienhallinnan toteuttamiseen.

THL:n riskienhallinta perustuu kansainväliseen standardiin SFS-ISO 31000 Riskienhallinta - Periaatteet ja ohjeet. Politiikan toteuttamiseksi THL:llä ja sen alaisella hallinnolla on tarvittaessa omat riskienhallinnan toimintaohjeensa. Riskienhallintapolitiikan ja siihen liittyvien ohjeiden avulla varmistetaan, että riskienhallinnan toimintamalli on yhtenäinen läpi koko THL:n ja sen alaisen hallinnon, ja että johdolla on riittävästi tietoa toimintaan kohdistuvista riskeistä päätöksentekoaan varten. (THL intranet 2020)

Riskienhallintapolitiikassa (Riskienhallintapolittikka 2019) riski on määritelty SFS-ISO 31000 standardi mukaisesti tarkoittavan epävarmuuden vaikutusta tavoitteisiin ja poikkeamaa odotetusta. Riskejä ovat THL:lle koituvat vahingot, jotka haittaavat laitoksen toimintaa uhkien toteutuessa tai mahdollisuuksien jäädessä käyttämättä (positiivinen riski). Riskienhallinta perustuu yhtenäisiin menettelyihin eri uhkien tunnistamiseksi, arvioimiseksi, hallinnoimiseksi ja raportoimiseksi. Tehokas ja järjestelmällinen riskienhallinta tukee toiminnan suunnittelua ja seurantaa sekä oikea-aikaiseen tietoon perustuvaa päätöksentekoa. Lisäksi se parantaa tavoitteiden saavuttamista ja toiminnan turvallisuutta.

Johto huolehtii, että THL:ssä toteutetaan sen talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden asianmukaiset menettelyt. Ylin vastuu THL:n riskienhallinnasta on pääjohtajalla, valtion lastensuojeluyksiköissä ja vankiterveydenhuollossa päävastuussa ovat toiminnasta vastaavat johtajat ja mielisairaaloissa johtavat lääkärit. Työjärjestyksessä määrätyt toimintayksiköiden päälliköt vastaavat oman toimintayksikkönsä uhkien tunnistamisesta, riskienarvioinnista ja hallintatoimien toteuttamisesta. THL:n työjärjestyksessä henkilöille määrättyjen erityistehtävien riskienhallinnan koordinoinnista vastaavat kyseiset henkilöt. THL-tason riskienhallinnan koordinoinnista ja raportoinnista vastaa laatupäällikkö. Jokaisella työntekijällä on velvollisuus viipymättä raportoida havaitsemistaan vaaroista ja osallistua riskienarviointiin. (THL intranet 2020)

THL:ssä on työsuojeluriskien tunnistamiseen, arviointiin ja hallintaan keskittynyt bioturvaryhmä, jonka työ perustuu STM:n ohjeeseen ja HUS:n biologisten riskien arviointimalliin. Ryhmän on perustettu vuonna 2015 ja se keskittyy mm. seuraaviin riskilajeihin: fysikaaliset vaaratekijät, tapaturmat, ergonomia, kemialliset vaaratekijät ja biologiset vaaratekijät. Muita turvallisuuteen liittyviä ryhmiä ovat työsuojelutoimikunta, ennakoiva sisäilmatyöryhmä, valmiusryhmä, tietoturvaryhmä ja turvallisuusryhmä.

4.1 Granite riskienhallintajärjestelmä

Granite Riskienhallinta on Granite-yhtiön yksi ohjelmistotuote, joka on digitaalinen työkalu nykyaikaiseen riskienhallintaan. Sen avulla tunnistetaan ja arvioidaan riskejä sekä vastuutetaan korjaavia toimenpiteitä. Graniten avulla myös tuotetaan raportteja päätöksenteon tueksi. (Granite 2020)

Granite on STM:n hallinnon alan yhteinen riskienhallintajärjestelmä ja se jakaantuu kolmeen osaan:

1. Riskienhallinta, jossa arvioitavat riskialueet ovat strategia, operatiivinen, toiminta, talous ja resurssit, henkilöstö ja turvallisuus
2. Työn vaarat ja riskit, jossa tapahtuu työsuojeluhallinnon mallin mukainen työpaikan vaarojen tunnistus ja riskien arviointi
3. Tehtävät, jossa on avoimet tehtävät käyttäjäkohtaisesti

Riskienhallinta -paketti sisältää toiminnan sisältämien riskien tunnistamisen ja arvioinnin. Riskejä käsitellään lomakkeina.

Riskienhallintanäkymässä saadaan kokonaiskuva organisaation riskeistä matriisissa, jossa vaakatasolla on organisaatio osastoittain ja pystytasolla riskilomakkeiden lukumäärä, prosenttuaalinen osuus, joka on arvioimatta, prosentuaalinen osuus, joka on seurannassa ja prosentuaalinen osuus, joka on valmis. Näkymästä voidaan ottaa raportteja, joissa näkyy 5x5 todennäköisyyden ja vakavuuden matriisissa, miten riskit sijoittuvat asteikossa sekä graafisia esityksiä riskilukujen summasta, riskien lukumäärästä ja riskialueiden painostuksesta sekä todennäköisyyden ja vakavuuden kuvaavat mittarit.

Riskien arviointi on viisi portainen ja asteikot ovat todennäköisyyden ja vakavuuden osalta seuraavat:

Riskin todennäköisyys

1 = erittäin epätodennäköinen (ei ole tapahtunut)
2 = epätodennäköinen (on tapahtunut joskus)
3 = mahdollinen (on tapahtunut useammin kuin kerran)

4 = todennäköinen (tapahtuu usein)
5 = erittäin todennäköinen (tapahtuu jatkuvasti)

Riskin vakavuus

1 = erittäin pieniä häiriöitä tai taloudellisia menetyksiä
2 = pieniä häiriöitä tai taloudellisia menetyksiä
3 = toiminnan hidastuminen ja kohtuullisia taloudellisia menetyksiä
4 = toiminnan huomattava vaikeutuminen ja merkittäviä taloudellisia menetyksiä
5 = toiminnan lamaantuminen ja todella merkittäviä taloudellisia menetyksiä

Arviot tehdään erikseen strategia riskien, operatiivisen toiminnan, talouden ja resurssien, henkilöstön ja turvallisuuden osalta. Turvallisuus sisältää toiminnan jatkuvuuden, toimitilaturvallisuuden tietoturvallisuuden ja tietosuojan osalta.

Työn vaarat ja riskit -paketti sisältää työpaikan riskien tunnistamisen ja arvioinnin. Riskejä käsitellään tässäkin lomakkeina. Riskejä käsitellään edellisestä poiketen 3x3 todennäköisyyden ja vakavuuden matriisisssa ja asteikko on seuraavanlainen

- 0 = Ei koske meitä
- 1 = Ei aiheuta haittaa tai vaaraa
- 2 = Aiheuttaa haittaa tai vaaraa, joka avaa riskilomakkeen, johon tulee kirjata tarkemmin vaarasta aiheutuva riski ja määrittää toimenpiteet ja aikataulu riskin poistamiseksi tai pienentämiseksi.

Varsinainen riskienarviointi suoritetaan kolmiportaisella asteikolla

- Todennäköisyys
    - 1 = Epätodennäköinen: Tapahtunut kerran 30-100 vuoden sisällä
    - 2 = Mahdollinen: Tapahtunut kerran 5 vuoden sisällä
    - 3 = Todennäköinen: Tapahtunut vuoden sisällä
- Vakavuus
    - 1 = Vähäinen: Alle yksi poissaolopäivä
    - 2 = Haitallinen: 1-14 poissaolopäivää
    - 3 = Vakava: Pysyvä haitta tai yli 14 poissaolopäivää

Todennäköisyyden ja vakavuuden tulona saadaa riskiluku. Riskiin liittyy tilatieto, jota käytetään riskin tilanteen seuraamiseen:

1. Arvioimatta = Arviointi on kesken (toimenpiteitä ei ole aloitettu)
2. Seurannassa = Arviointi on valmis ja toimenpiteet on määritelty

3. Valmis = Kaikki riskiin liittyvät toimenpiteet on tehty

Granite on ollut käytössä vuodesta 2015.

4.2 Turvallisuusryhmä

Turvallisuusryhmän tehtävänä on kehittää ja hallinnoida Terveyden ja hyvinvoinnin laitoksen kokonaisturvallisuutta ja turvata laitoksen ihmiset, tieto, ympäristö, omaisuus ja maine sekä huolehtia työturvallisuuslain ja muiden lakien tuomista velvoitteista ja varmistaa, että organisaatioturvallisuuden eri osa-alueet on otettu huomioon laitoksen kokonaisvaltaisen turvallisuuden strategisessa ja operatiivisessa toiminnassa ja johtamisessa. Turvallisuusryhmän tehtävä on myös varmistaa yhteistyö laitoksen eri turvallisuusryhmien rajapinnassa. Ryhmä käsittelee vuosittain myös tietohallinnon ja tarvittaessa muiden osa-alueiden erityiskysymyksiä teemakokouksissa. Teemakokouksiin kutsutaan mukaan ryhmän ulkopuolisia edustajia tarpeen mukaan. (Jämsen 2017; Turvallisuusryhmä 2019)

Terveyden ja hyvinvoinnin laitoksen turvallisuuden yhteistyö organisoitiin uudella tavalla vuoden 2015 alusta perustamalla turvallisuusasiantuntijat kokoava turvallisuusryhmä. Yhteistä foorumia ei kokonaisturvallisuuden tarkastelulle aikaisemmin ole ollut. Kokonaisturvallisuutta korostavan ryhmän tavoitteena on luoda edellytykset paremmalla suunnittelulle, raportoinnille, tilannekuvalle ja koordinaatiolle kaikissa turvallisuuskysymyksissä organisaation sisällä. Asettamispäätöksen mukaisesti ryhmän tehtävä on kehittää ja hallinnoidan kokonaisturvallisuutta ja varmistaa yhteistyö organisaation eri turvallisuusrajapintojen välillä sekä varmistaa, että toiminnan suunnittelu on yhdenmukaista. (Jämsen 2017, 23)

Turvallisuusryhmän perustamisen jälkeen on turvallisuustoiminnan suunnittelu ja tavoitteet pyritty keskittämään yhteen turvallisuussuunnitelmaan koko organisaation tasoisesti. Toimintasuunnitelman tavoitteena on parempi koordinaatio turvallisuustyössä tarvittavien toimenpiteiden ja yhteisten resurssien osalta. Suunnitelmassa esitetään koko turvallisuusorganisaation yhteiset ja jokaisen osa-alueen erikseen määrittelemät tavoitteen vuositasolla, Ryhmällä on yhteisten tavoitteiden osalta vuosikello (kuvio 19), johon kirjataan vuosisuunnittelun kvartaalitason tapahtumat. Jämsenin mukaan (2017, 24-25) organisaatiolla tai turvallisuusryhmällä ei vielä ole vakiintunutta tapaa kerätä tietopohjaa ja raportoida turvallisuustoiminnan tuloksista organisaation johdolle. Tämä johtuu osin siitä, ettei yhteistä raportointikanavaa tai yhteisiä raportointikäytänteitä turvallisuustoiminnoissa vielä ole ollut ja että raportointivastuut on määritelty vaihtelevalla tavalla.

Turvallisuusryhmän toimikausi päättyi vuoden 2017 lopussa ja ryhmä on asetettu pääjohtajan päätöksellä uudelleen helmikuussa 2019. Ryhmä ei käytännössä ollut toiminnassa lainkaan vuoden 2018 aikana. Turvallisuusryhmä kokoontuu kuukausittain ja se käsittelee

toimeksiannon mukaisesti ”vuosittain myös tietohallinnon ja tarvittaessa muiden osa-alueiden erityiskysymyksiä teemakokouksessa”. Laitoksella on turvallisuusryhmän lisäksi turvallisuusjohto, joka kokoontuu tiiviimmin ryhmän ulkopuolella päivittäiskysymysten sopimiseksi ja ratkaisemiseksi. Toimeksiannossa turvallisuusryhmän tehtäväksi on annettu seuraavat kokonaisuudet (Turvallisuusryhmä 2019):

- Tukea turvallisuuden hallintajärjestelmän suunnittelua, toteuttamista ja kehittämistä
- Koordinoida turvallisuus- ja tietoturvariskien arviointia ja hallintaa
- Hyväksyy ja varmistaa, että turvallisuus- ja tietoturvaprosessit ovat normien mukaiset ja tukevat laitoksen toimintaa
- Turvallisuuden hallintajärjestelmän vuosikellon mukaiset tehtävät
- Varmistaa yhteistyö keskeisten toimintojen välillä

Turvallisuusryhmässä on edustettuna seuraavat toiminnallisuudet:

- Toimitilaturvallisuus
- Tietoturvallisuus
- Työsuojelu
- Pelastustoimi
- Laboratorioiden turvallisuus ja bioturvallisuus
- Henkilöstöturvallisuus
- Tukipalvelut
- Valmiustoiminto
- Riskienhallinta

Tärkeimmät sidosryhmät ovat valmiusryhmä, tekninen tietoturvaryhmä, työsuojelutoimikunta, laatutyöryhmä, Tietopalvelut-osasto (TIPO) erityisesti tietojärjestelmät -yksikkö (TIPE) sekä Hallinto- ja kehittäminen -osasto (HAKE) erityisesti Tukipalvelut -yksikkö (HATU).

Ryhmä raportoi THL:n johtoryhmälle vähintään vuosittain ja Hallinto- ja kehittäminen -osaston johtoryhmälle puolivuosittain.

Pääjohtajan tekemän päätöksen (19/2019) mukaan turvallisuusryhmän työskentelyn tavoitteet pohjautuvat laitoksen johdon priorisoimiin riskeihin, joiden kokonaiskuvaa hallinnoidaan riskienhallintajärjestelmässä (Virta 2014). Ryhmän tehtäväksi on asettamispäätöksessä annettu:

- Ylläpitää laitoksen riskienhallintapolitiikkaa
- Huolehtia riskienhallinnan ajantasaisuudesta ja ylläpitää organisaation riskitietoisuutta
- Turvallisuuden hallintajärjestelmän kokonaisuuden ylläpito
- Varmistaa yhteistyö keskeisten turvallisuustoimintojen välillä

Turvallisuusryhmän jäsenet rooleittain vuoden 2019 päätöksen mukaan (nimet on tästä jätetty pois)

- Palvelujohtaja (ryhmän puheenjohtaja)
- Turvallisuuspäällikkö
- Tietoturvapäällikkö
- Tietosuojavastaava
- Työsuojelupäällikkö
- Valmiuspäällikkö
- Laatupäällikkö/Riskienhallinta
- Bioturvapäällikkö

Turvallisuusryhmän tehtävänä on vuositasolla mm. arvioida toimintaansa ja raportoida siitä organisaation johdolle sekä suunnitella toimintaansa seuraavalle vuodelle, päivittää dokumentaatiota, laatia koulutussuunnitelmat ja järjestää yleiset turvallisuuskoulutukset sekä suunnitella turvallisuustoimen harjoitukset. Turvallisuusryhmän vuosisuunnittelu esitetään THL:n intranetissa (Turvallisuusryhmä 2019) vuosikellona, joka on esitetty seuraavassa kuviossa.

Kuvio 21: THL:n turvallisuusryhmän vuosikello. (Muokattu lähteestä THL intranet 2020)

Vuosikello on turvallisuusryhmän vuosisuunnittelun väline ja vuosisuunnitteluakin kehitetään jatkuvasti muuttuneiden turvallisuustilanteiden osalta.

4.3 Turvallisuusryhmän toiminnan tarkastelu

Edellisen turvallisuusryhmän toiminta on päättynyt vuoden 2017 lopussa ja uusi ryhmä on nimitetty vuoden 2019 syyskuussa uuden pääjohtajan toimesta, joka aloitti viisivuotisen

kautensa 1.1.2019. Ryhmän uudelleen nimittämiseen liittyy monia asioita, kuten tietosuojavastaavan viran alkaminen vuoden 2018 lopussa. Ryhmä on myös edellistä pienempi. Turvallisuusryhmän kick-off tilaisuus pidettiin 18.3.2019.

Terveyden ja hyvinvoinnin strategiassa (THL strategia 2020: STM tulossopimus 2020, 3) on kolme strategista tavoitetta: Tieto, Tulkinta ja Ratkaisut ja tuki. Tulkinta -kohdassa on tavoitteeksi asetettu ”ylläpidämme tilannekuvaa ja ennakoimme tulevaa.”. Turvallisuusryhmän toiminnassa tilannekuvan ylläpito tarkoittaa, että eri turvallisuuden osa-alueille tehdään vuosittaiset suunnitelmat, joiden pohjalta toimintaa suunnitellaan, mutta erityisesti sitä, että jokaisessa kokouksessa ja tarvittaessa muiden kanavien kautta koko turvallisuusryhmä on tietoinen turvallisuuden eri osa-alueiden tilanteesta. Tätä tietoa jaetaan turvallisuusryhmän agenda mukaan jokaisessa kokouksessa raportoimalla eri osa-aluiden sen hetkinen kuvaus turvallisuustilanteesta.

Seuraavassa on vuosittaiset suunnitelmat turvallisuuden eri osa-alueiden osalta. Suunnitelmat on kirjattu turvallisuusryhmän intranet sivulle ja tässä ne on referoitu.

Vuonna 2015 tavoiteltiin kokonaisuuden hallinnan saattamista kootuksi kokonaisuudeksi, jossa turvallisuuden eri osa-alueille saataisiin laadittua yhteiset tavoitteet ja prosessi, joiden mukaan toimitaan ja toimintaa suunnitellaan. Tavoitteena oli myös turvallisuusryhmän henkilöiden vastuiden selkeyttäminen sekä yhteisen dokumentaation avulla toteutettu jatkuvuuden varmistaminen ja hallinnointi. Tavoitteena oli myös yhteisen foorumin perustaminen ja toiminnan ohjaamiseen ja tavoitteiden saavuttamiseen luoda toimintaympäristö- ja tavat sekä saattaa suunnitelmallinen ja ennakoitava toiminta osaksi normaalia toimintaa tekemällä monipuolinen vuosisuunnitelma.

Vuonna 2015 tehtiin erilliset suunnitelmat seuraavilla turvallisuuden osa-alueille:

- Henkilöturvallisuus. Henkilökorttien käyttöön liittyviä uudistuksia
- Kiinteistö- ja toimitilaturvallisuus. Turvallisuustietoisuuden parantamista, uusia lukitusratkaisuja ja rakennushankkeiden turvallisuusvaatimusten määrittelyä.
- Pelastustoimi ja paloturvallisuus. Pelastussuunnitelmien laatiminen kiinteistökohtaisesti, suojelutoiminnan tehtävien kirkastaminen ja siihen liittyvää koulutusta.
- Tietoturvallisuus. Tietojen luokitteluun liittyviä päätöksiä ja korotetun tietoturvatason hanke, tietoturvakartoitusta ja -koulutusta, ICT-jatkuvuussuunnittelua, erilaista harjoitustoimintaa, keskitetyn lokienhallinnan hankintaa.
- Tuotannon ja toiminnan turvallisuus. Toimintojen priorisointia ja ohjeistusta.
- Matkustusturvallisuus. Matkustusohjeen päivittäminen turvallisuusnäkökulmien osalta.
- Valmiussuunnittelu. Valmiusryhmän uudistaminen ja organisointi.
- Ympäristöturvallisuus. Jäteohjeen uudistaminen.

Erillisenä oli vielä koulutussuunnitelma, jossa oli koulutustapahtumia tietoturvaan, työsuojeluun ja yleiseen turvallisuuskoulutukseen liittyen.

Vuonna 2016 kokonaisturvallisuuden hallinta oli vastuutettu turvallisuusryhmälle. Tavoitteet olivat samat kuin vuonna 2015, mutta niiden lisäksi oli tavoitteeksi asetettu yhteisen poikkeamatyökalun hankinnan selvittäminen, riskienhallinnan yhteisen toimintamallin kehittäminen ja yhteisen riskienhallintatyökalun (Granite) käyttöönotto, jatkuvuussuunnitelmien loppuunsaattaminen sekä turvallisuuden peruskurssin uudistaminen ja tarjoaminen uuden verkkokoulutustyökalun kautta. Erilliset suunnitelmat turvallisuuden eri osa-alueille sisälsi seuraavia asioita.

- Henkilöturvallisuus. Koordinaatiovastuu henkilöstöpäälliköllä ja turvallisuuspäälliköllä. tuloprosessin kokonaistarkistus, vaitiolositoutumisprosessin kehittäminen ja digitalisointi, henkilökortin käyttöönottoon ja käyttöön liittyviä varmistuksia ja kuvauksia.
- Kiinteistö- ja toimitilaturvallisuus. Koordinaatiovastuu turvallisuuspäälliköllä. Kulunvalvontajärjestelmän ja työajanseurantajärjestelmän erottaminen toisistaan. Kulunvalvontajärjestelmän uudistuksia, avainten hallinnan parantamista ja lukituksen uudistamista, toimitilojen turvallisuusmerkintöjen tarkastamista ja päivittämistä sekä turvallisuuskarttojen laatimista, turvallisuussopimukset tiloja hallinnoivan Senaatin kanssa.
- Tietoturvallisuus. Koordinaatiovastuu tietoturvapäälliköllä. Korotetun suojaustason ympäristön suunnittelua, STIII-verkon käyttöönotto, tietoturva-auditointisopimukset, sovelluskehittämisen prosessien tietoturvavastuiden määrittely ja implementointi, etäyhteyksien vahvan tunnistamisen pilotti.
- Tuotannon ja toiminnan turvallisuus. Koordinaatiovastuu bioturvapäälliköllä. Bioturvaohjeen implementointi ja bioturvan auditointi.
- Työturvallisuus ja työsuojelu. Koordinaatiovastuu työsuojelupäälliköllä. Riskiarvioiden tulosten korjausten jalkauttaminen, työturvallisuusriskien perehdyttäminen, palotarkastukset päätoimipaikassa, suojeluorganisaation toiminnan edellytysten tarkistaminen, poistumis- ja alkusammutus koulutus, pelastussuunnitelman täsmennykset.
- Matkustusturvallisuus. Koordinaatio vastuu matkatiimi. Valtion uuden matkustussuunnitelman implementointi, matkustusturvallisuuden koulutustapahtumat.
- Valmiussuunnittelu. Koordinaatiovastuu valmiuspäälliköllä. Valmiusohjelman päivityksen jatkaminen, osallistuminen TIETO2016 harjoitukseen.
- Ympäristöturvallisuus. Koordinaatiovastuu työympäristötiimillä. Jätteiden käsittelyn kehittäminen oikeuslääketieteen yksikössä.

Lisäksi oli erillinen koulutussuunnitelma, jossa koulutuksia työturvallisuudesta (12 kpl), tietoturvallisuudesta (1 kpl), tuotannon ja toiminnan turvallisuudesta (2 kpl) sekä yleisiä turvallisuuskoulutuksia (3 kpl).

Vuonna 2017 yhteisenä tavoitteena oli kokonaisuuden hallinnan saattamista kootuksi kokonaisuudeksi, jossa turvallisuuden eri osa-alueille saataisiin laadittua yhteiset tavoitteet ja prosessi, joiden mukaan toimitaan ja toimintaa suunnitellaan eli pitkälti sama kuin edellisinä vuosina. Lisäksi oli erikseen tavoitteeksi asetettu esitys riskienhallintatyökalun käyttöönotosta ja käyttöönoton laajentamisesta, ainakin yhden jatkuvuusharjoittelun järjestäminen, matkustusturvallisuuskäsikirjan laadinta, henkilöriskien vähentäminen, turvallisuuden opetusvideoiden tekeminen sekä poikkeamaraportoinnin kehittäminen. Erilliset suunnitelmat turvallisuuden eri osa-alueille sisälsi seuraavia asioita.

- Henkilöturvallisuus. Koordinaatiovastuu henkilöstöpäälliköllä ja turvallisuuspäälliköllä. Ei kirjauksia.
- Kiinteistö- ja toimitilaturvallisuus. Koordinaatiovastuu turvallisuuspäälliköllä. Kulunvalvontajärjestelmän ja työajanseurantajärjestelmän erottaminen toisistaan. Kulunvalvontajärjestelmän uudistuksia, avainten hallinnan parantamista ja lukituksen uudistamista, toimitilojen turvallisuusmerkintöjen tarkastamista ja päivittämistä sekä turvallisuuskarttojen laatimista.
- Tietoturvallisuus. Koordinaatiovastuu tietoturvapäälliköllä. Sovelluskehittämisen prosessien tietoturvavastuiden jatkokäsittelyt, järjestelmäympäristöjen haavoittuvuuksien selvittäminen ja korjaustoimenpiteet, käyttöoikeuksien hallinnan kehittäminen, tietoturvallisuuden sisäiset ohjeet, jatkuvuussuunnitelmien päivittäminen kriittisten järjestelmien osalta, tietoturvariskien arvioinnin ja raportoinnin jatkokehittäminen.
- Tuotannon ja toiminnan turvallisuus. Koordinaatiovastuu bioturvapäälliköllä. Laatujärjestelmän hyödyntäminen bioturvaohjeen laadinnassa, bioturva-auditointien jatkaminen, bioturvakoulutusten aloittaminen.
- Työturvallisuus ja työsuojelu. Koordinaatiovastuu työsuojelupäälliköllä. Esimiesten esimerkillisyyden kehittäminen, poistumisharjoitukset, pelastussuunnitelmien ylläpito, työpaikan riskienarvioinnit.
- Matkustusturvallisuus. Koordinaatio vastuu matkatiimi. Matkustusohjeen päivitys tietoturvallisuuden osalta, koulutustilaisuudet.
- Valmiussuunnittelu. Koordinaatiovastuu valmiuspäälliköllä. Valmiusohjelman päivityksen jatkaminen, TIETO2016 harjoituksen opit.
- Ympäristöturvallisuus. Koordinaatiovastuu työympäristötiimillä. Ei merkintöjä.

Lisäksi oli laadittu koulutussuunnitelma, jossa oli työturvallisuuden osalta poistumisharjoituksia kirjattu 11 kappaletta, joista viisi oli toteutunut, alkusammutusharjoituksia seitsemän kappaletta, joista neljä oli toteutunut, ensiapukoulutuksia kahdeksan kappaletta, joista kaikki

oli toteutunut. Matkustusturvallisuuteen liittyviä koulutuksia oli 1 kappale ja tietoturvallisuuteen liittyviä koulutuksia 13 kappaletta, joista kaikki oli toteutettu. Tuotannon ja toiminnan turvallisuuden koulutuksia oli suunnitelmassa yhdeksän kappaletta ja kaikki toteutunut sekä yleisiä turvallisuuskoulutuksia pidettiin kolme kappaletta vuonna 2017.

Tästä on selvästi havaittavissa toiminnan vakiintuminen ja turvallisuusryhmän aktiivisuus erityisesti koulutusten osalta.

Vuonna 2018 yhteisiä tavoitteita ei ollut erikseen kirjattu. Toimintasuunnitelmat oli viety organisaatioturvallisuuden osa-alueiden kohtaisiin taulukoihin ja niissä oli suunnitelmiin lisätty budjetointi, jokaisen osa-alueen yksittäisen tavoitteen kohdalle. Erilliset suunnitelmat turvallisuuden eri osa-alueille sisälsi seuraavia asioita. Uutena kohtana oli tullut tietosuoja ja riskiehallinta sekä työturvallisuudesta ja työsuojelusta oli pudotettu jälkimmäinen osa pois

- Henkilöturvallisuus. Koordinaatiovastuu henkilöstöpäälliköllä ja turvallisuuspäälliköllä. Ei kirjauksia.
- Kiinteistö- ja toimitilaturvallisuus. Koordinaatiovastuu turvallisuuspäälliköllä. Kulunvalvontajärjestelmän päivittäminen, kameravalvontajärjestelmän päivitys joidenkin tilojen osalta ja laajennus joidenkin tilojen osalta, olosuhdevalvonnan laajentaminen ja erikoisjätteiden kilpailutus.
- Tietoturvallisuus. Koordinaatiovastuu tietoturvapäälliköllä. Tehostetut tietoturvatarkastukset yksikössä, verkkouudistuksen ja aineistohallinnan toteuttaminen, tietoturvan hallintajärjestelmä ohjeistuksen tarkistukset, tietojärjestelmien- ja ympäristöjen käyttöoikeuksien tarkastus, sovelluskehittäjien tietoturvallisen kehittämiseprosessin jatkokehittäminen, tietoturvan pilvipalveluiden ohjeen laatiminen.
- Tietosuoja. Koordinaatiovastuu tietosuojavastaavalla. Ei merkintöjä.
- Riskienhallinta. Koordinaatiovastuu riskienhallintavastaava. Ei merkintöjä.
- Tuotannon ja toiminnan turvallisuus. Koordinaatiovastuu bioturvapäälliköllä. Bioturva-auditoinnit, bioturvaohjeistukset ja -perehdytykset ulkopuolisille työntekijöille.
- Työturvallisuus. Koordinaatiovastuu työsuojelupäälliköllä. Esimiesten työturvallisuustietoisuuden varmistaminen, pelastussuunnitelmajärjestelmän vaihtaminen, uusien työsuojeluvaltuutettujen ja varavaltuutettujen koulutus, sähköisen työturvallisuuspoikkeamaraportointityökalun käyttöönotto, vaarojen kirjaaminen Graniteen (riskienhallintajärjestelmä), ergokummikäytäntöjen vakiinnuttaminen, monitilatoimistojen pelisääntöjen luominen.
- Matkustusturvallisuus. Koordinaatio vastuu matkatiimi. Ei merkintöjä.
- Valmiussuunnittelu. Koordinaatiovastuu valmiuspäälliköllä. Valmiussuunnitelman päivitys.
- Ympäristöturvallisuus. Koordinaatiovastuu työympäristötiimillä. Ei merkintöjä.

Koulutussuunnitelmaan oli suunniteltu erityisesti työturvallisuuteen liittyviä koulutuksia. Työturvallisuuden osalta oli poistumisharjoituksia viisi kappaletta, alkusammutusharjoituksia kolme kappaletta, ensiapukoulutuksia yhdeksän kappaletta. Näiden lisäksi oli yleisiä turvallisuuskoulutuksia pidetty 3 kappaletta.

Vuoden 2019 turvallisuusryhmän toimintasuunnitelmassa ei enää ollut merkintää muista kuin suunniteluista koulutuksista. Vuoden 2019 aikana on ollut kaksi poistumisharjoitusta, kolme yleistä turvallisuuskoulutusta sekä viisi ensiapukoulutusta. Toimintasuunnitelmassa oli lisäksi kaksi alkusammutuskoulutusta, mutta kumpikaan ei niistä toteutunut.

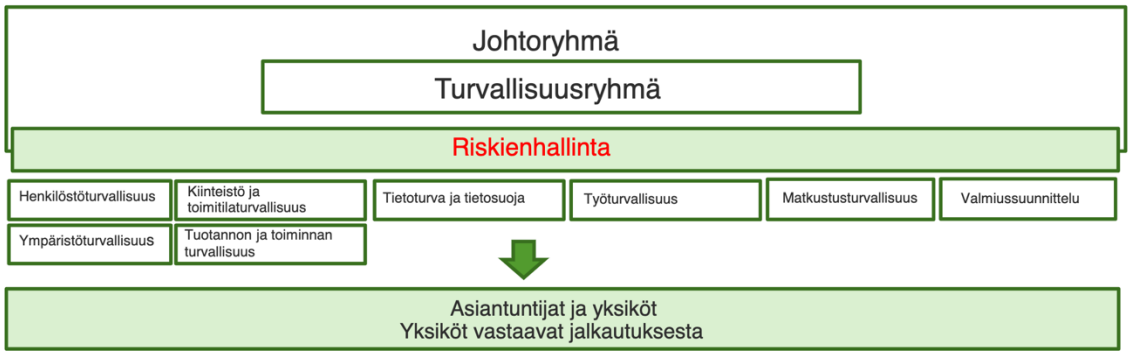
Vuoden 2020 toimintasuunnitelmaa ei ollut laadittu.

Turvallisuusryhmän toimintakertomus ja raportointi on viimeksi laadittu vuonna 2017. Turvallisuusryhmä on kuitenkin kokoontunut säännöllisesti vuodesta 2015 alkaen seuraavasti

2015	2016	2017	2018	2019	2020
7	7	6	6	4	5 (Q1-Q2)

Taulukko 6: Turvallisuusryhmän kokoukset 2015-2020.

Kokousten asialista noudattelee Elinkeinoelämän keskusliiton turvallisuuden osa-alueiden jakoa eli sitä samaa mitä on käytetty vuosisuunnittelussa. Lisäksi kokouksissa on käyty Granitessa tunnistettuja riskejä läpi vuoden 2019 alusta alkaen. Vuoden 2018 kokouksista oli vain asialistat saatavilla, joten on epävarmaa pidettiinkö kokouksia lainkaan. Turvallisuusryhmän toimikausi oli päättynyt vuoden 2017 lopussa ja uusi ryhmä nimettiin vasta vuoden 2019 tammikuussa. Vuoden 2019 ensimmäinen kokous oli järjestäytymiskokous, jossa todettiin ryhmän olevan pienempi kuin aikaisemmin ja että ryhmän toimintatapa on keskusteleva. Kokouksessa esiteltiin myös tulevaisuuden suunnitelmia turvallisuuden osalta, jossa selkeytettiin tietoturvapäällikön toimintakenttää, valmiusryhmän toimintaa ja suhdetta muihin ryhmiin sekä turvallisuusryhmän positiota.



Kuvio 22: Turvallisuusryhmän sijoittuminen organisaatiossa.

Turvallisuusryhmä raportoi laitoksen johtoryhmälle, mutta ei ole edustettuna johtoryhmässä. Turvallisuusryhmän perustaa päätöksensä ja toimenpide-ehdotuksensa riskienhallinnan kautta saatavaan tietoon ja sen perusteella tehtyyn tilannearviointiin. Turvallisuusryhmään kuuluu asiantuntijoita turvallisuuden eri osa-alueista ja kaikki Elinkeinoelämän keskusliiton turvallisuuden osa-alueet ovat edustettuna. Näiden kautta vaikutetaan yksiköiden asiantuntijoihin, jotka vievät turvallisuustietoutta henkilöstölle ja samalla kehittävät turvallisuuskulttuuria yksiköissä.

Jämsenin tutkielmassa (2017, 23) kävi ilmi, että turvallisuusryhmän olemassaolo kyllä tunnistettiin, mutta sen mandaattia osana johtamisjärjestelmää epäiltiin tai ei täysin hahmotettu. Turvallisuusryhmän muistioistakin ilmenee, että vuoden 2015 asettamisen jälkeen, se on hakenut paikkaansa ja tehtävänkuvaansa ja kun ryhmän toiminta päättyi vuoden 2017 lopussa, jäätiin tyhjäkäynnille. Turvallisuusryhmän toiminta on kuitenkin selkeytynyt ja vakiintunut vuoden 2019 uudelleenasettamisen myötä ja uuden ryhmän ensimmäisessä kokouksessa ryhmän toiminnalle asetetut tavoitteet tukevat niitä näkemyksiä, joita organisaation turvallisuusjohtamiselle on tietoperustassakin asetettu. Ryhmän odotuksiksi on kirjattu tilannekuvasta keskustelua, suurimpien riskien esille nostaminen ja toimenpiteet niiden ehkäisemiseen, viestinnän parantaminen eri (turvallisuus)ryhmien kesken, tekemisten ja tarkoitusten selkeyttäminen eri ryhmien osalta.

Uudistettu turvallisuusryhmä on toiminut nyt puolitoista vuotta ja pöytäkirjojen perusteella voidaan havaita, että toiminta on ollut aktiivista ja monipuolista. Turvallisuuden osa-alueita on käsitelty Elinkeinoelämän keskusliiton (EK yritysturvallisuus 2016) mukaisesti, mutta huomattavan suuren osan on vienyt työturvallisuuteen liittyvien asioiden käsittely, tietoturvallisuus ja tilaturvallisuus. Myös bioturvallisuus, THL:n erityisalueena, on ollut usein esillä. Keväällä 2020 on toki korona-asiat olleet suuressa roolissa ja korona mainitaankin vuoden 2020 kokousten (5 kpl) muistioissa kuusi kertaa. Turvallisuusryhmässä asioita käsitellään pitkälti riskienhallintapolitiikan periaatteilla ja riskilähtöisesti.

Koska turvallisuusryhmällä on neuvoa antava ja ohjaava rooli, se ei voi suoraan vaikuttaa turvallisuusasioiden käsittelyyn osastoittain, paitsi oman osastonsa kontekstissa. Seuraavassa taulukossa on katsottu henkilöiden sijoittumista osastoihin verraten sitä turvallisuustehtävään. Osastoja on seitsemän ja turvallisuusryhmän jäsenet sijoittuvat niihin seuraavasti (tilanne 7/2020).

Tutkimus- ja kehittämisosastot				Ohjaus- ja tukipalvelut		Valtion sote-palvelut
Hyvinvointi	Kansan terveys	Järjestelmät	Terveys-turvallisuus	Tieto-palvelut	Hallinto ja kehittäminen	Valtion erityispalvelut
			Bioturva-päällikkö		Palvelujohtaja (pj.)	

			Valmius-päällikkö		Turvallisuuspäällikkö Tietoturvapäällikkö Työsuojelupäällikkö Tietosuojavastaava Laatupäällikkö	

Taulukko 7: Turvallisuusryhmän jäsenten sijoittuminen osastoihin.

Hallinto- ja kehittäminen -osasto on lähes ainoan edustajana turvallisuusryhmässä, muiden osastojen jäädessä sen varjoon. Hallinto- ja kehittäminen -osasto tarkoitus määritellään THL intranetissa seuraavasti: Hallinto ja kehittäminen -osasto luo edellytyksiä johtamiselle ja organisaation toiminnalle. Sen vastuu alueeseen kuuluu talous, henkilöstö ja tukipalvelut sekä johdon esikuntapalvelut, joiden mukaisiin yksikköihin se jakaantuu. Turvallisuusryhmään kuuluvat ovat kaikki hallinto ja kehittäminen -osaston tukipalvelut -yksikössä ja sen tehtäväkuvaus kuuluu seuraavasti: ”Tukipalvelut -yksikkö valmistelee toimitilastrategian ja työympäristön kehittämissuunnitelmat sekä vastaa niiden toimeenpanosta, kehittää ja valvoo pelastusturvallisuutta, koordinoi näytehallinnan kehittämistä ja tuottaa näytehallinnan tukipalveluita, tuottaa laboratoriotyön tukipalveluja sekä vastaa kaasu- ja apex-turvallisuudesta, tukee hallinnon prosessien kehittämistä ja digitalisointia, vastaa tietoturvallisuuden hallintajärjestelmästä sekä koordinoi ja kehittää laitoksen tietoturvallisuutta.” Tukipalvelut -yksikön voidaan vahvoilla perusteilla sanoa olevan vastuussa Terveyden ja hyvinvoinnin laitoksen turvallisuudesta ja muiden yksiköiden osalle tietoisuus turvallisuusasioista tulevat johtoryhmän ja viestinnän kautta.

Ilmonen ym. (2016, 85) toteavat, että ”kokemus on osoittanut, että jos tietynlaisten riskien hallintaa hoitavat päätyönään tukitoiminnoissa työskentelevät asiantuntijat, liiketoiminnan edustajilla saattaa olla taipumus sulkea silmänsä tämän alueen riskeiltä ja luottaa siihen, että kyseisten riskien asiantuntijat hoitavat ne suvereenisti.” Lisäksi todetaan, että turvallisuudesta ja riskienhallinnasta vastaavan työryhmän kokoonpano tulee tukea riskienhallinnan kokonaistavoitetta, jolloin työskentely tähtää organisaation kannalta olennaisten riskien tunnistamiseen, analysoimiseen ja hallitsemiseen ja että edustettuna on syytä aina olla liiketoiminnan vetovastuussa olevat henkilöt joko organisaation vetäjä tai joku tämän lähipiiristä, joka hallitsee toiminnan liiketoiminnallisen kokonaisuuden. Ilmosen ym. näkemykseen perustuen Terveyden ja hyvinvoinnin laitoksessa se tarkoittaisi, että osastojen edustajien mukanaolo turvallisuusryhmässä toisi laajempaa näkyvyyttä osastojen riskeihin ja hallintakeinoihin.

4.4 Valmiusryhmä

Valmiusryhmä vastaa Terveyden ja hyvinvoinnin laitoksen jatkuvuussuunnittelusta ja valmiussuunnittelusta. Jatkuvuussuunnittelun tavoitteena on turvata laitoksen toiminnan nopea käynnistyminen häiriöiden ja poikkeavien tilanteiden jälkeen sekä vähentää niistä aiheutuvia haitallisia vaikutuksia. Jatkuvuussuunnittelun avulla varaudutaan jo ennalta mahdollisiin ongelmatilanteisiin. Hyvällä suunnitelulla pyritään varmistamaan laitoksen kyky jatkaa toimintaa mahdollisimman pienin menetyksin ja täyttämään velvollisuutensa, vaikka sen toiminta häiriintyisi jonkin sisäisen tai ulkopuolisen tapahtuman takia. Mahdollisina häiriötapahtumina on mainittu tietojärjestelmien häiriöt, inhimillinen virhe, jolla on laajat vaikutukset, väärinkäytös, tietoliikenteen häiriöt ja katkokset, sähkönjakelun häiriöt, tulipalo, vesivahinko, toimitilojen osittainen tai täydellinen tuhoutuminen tai avainhenkilöiden menetys. Valmiusryhmän tarkoituksen voidaan sanoa olevan toiminnan takaaminen niin, että Terveyden ja hyvinvoinnin laitos voi palvella yhteiskuntaa kriisitilanteissa ja että rekisteriaineistot ja muut elintärkeät tietokannat ovat yhteiskunnan käytössä myös normaaliolojen ulkopuolella.

Valmiusryhmä on toiminut vuodesta 2012 ja se kokoontuu 1-6 kertaa vuodessa tilanteista riippuen. Valmiusryhmään kuuluu turvallisuusryhmän jäsenten lisäksi yksiköiden päälliköt ja heidän varallaan varapäälliköt sekä asiantuntijalääkäreitä. Valmiusryhmän materiaalit ja kokousten muistiot ovat luokiteltuja ja vain jäsenten ja varajäsenten nähtävillä.

4.5 Turvallisuuden johtamisjärjestelmä

Terveyden ja hyvinvoinnin laitoksen turvallisuuden johtaminen perustuu STM:n tulossopimukseen (STM tulossopimus 2020), työjärjestykseen ja sen liitteisiin (THL työjärjestys), strategiaan (THL strategia), sisäisiin ohjeisiin, riskienhallintapolitiikkaan, tietoturvapolitiikkaan, turvallisuusryhmän kokouskäytäntöihin, sisäisten asiantuntijoiden muodostamiin ryhmiin sekä erilaisiin viraston suunnittelu, arviointi- ja raportointikäytänteisiin, joita osastoilla tehdään.

Turvallisuusvastuut ovat Terveyden ja hyvinvoinnin laitoksessa jakaantunut siten, että jokaisella yksikönpäälliköllä on omalta osaltaan vastuu yksikön turvallisuusasioiden hoidosta. Tämä vastuu on linjaorganisaation mukainen kehittämis- ja koordinointivastuu. Useimmissa yksiköissä turvallisuuteen liittyvät tehtävät ovat oman toimen ohella hoidettavia tehtäviä, kun taas joissakin turvallisuuskriittisissä yksiköissä, turvallisuustehtävät ovat vastuutettu henkilölle ja näkyy tämän nimikkeessä, esimerkiksi bioturvapäällikkö. Vastuiden jakautuminen noudattaa Terveyden ja hyvinvoinnin laitoksen työjärjestyksen mukaista vastuuta. Työjärjestys (viimeisin on tullut voimaan 1.1.2020) on Terveyden ja hyvinvoinnin laitoksesta sekä terveystietojen toissijaisesta käytöstä annettujen lakien ja asetusten (L668/2008 3§, L675/2008 2§, L70/2013, L552/2019) nojalla pääjohtajan antama. Työjärjestyksessä määrätään Terveyden ja hyvinvoinnin laitoksen organisaatiosta, johtamisesta ja ratkaisuvallasta. Turvallisuusorganisaatiosta ei työjärjestyksessä suoraan määrätä, mutta sisäinen tarkastus määritellään olevan

suoraan pääjohtajan alaisuudessa ja tietoturvallisuus määritellään olevan tietoylijohtajan alaisuudessa. Muilta osin turvallisuudesta vastaavat henkilöt nimetään erikseen työjärjestyksen liitteessä, jossa määritellään laitoksen henkilöstölle määrätyt erityistehtävät. Siinä nimetään suoraan turvallisuuteen liittyviin tehtäviin valmiusjohtaja, joka on sama kuin terveysturvallisuusosaston johtaja, valmiuspäällikkö, turvallisuuspäällikkö, tietoturvapäällikkö, tietosuojavastaava, bioturvapäällikkö sekä näille varahenkilöt. Turvallisuuspäällikön osalta määritellään, että hän nimeää erikseen laitoksen kulunvalvonta-, kameravalvonta- ja rikosilmoitusjärjestelmän pääkäyttäjät sekä laitoksen tunnistuspisteiden tunnistajina toimivat henkilöt. Muidenkin osalta pääasialliset tehtäväkuvaukset on annettu työjärjestyksessä. Turvallisuusjohtajaa ei Terveyden ja hyvinvoinnin laitoksella ole, vaan turvallisuus on kokonaisvastuutettu turvallisuusryhmälle, jonka jäseniä valmiusjohtajaa lukuun ottamatta edellä mainittuja tehtäviä hoitamaan nimetyt ovat ja jonka puheenjohtajana toimii palvelujohtaja. Palvelujohtaja on myös turvallisuuspäällikön ja tietoturvapäällikön esimies, kun taas tietosuojavastaava kuuluu laitoksen lakimiesryhmään. Laitoksella ei ole turvallisuuspolitiikka tai turvallisuusperiaatteet -nimistä dokumenttia, vaan laitoksen turvallisuus nojaa periaatteiltaan riskienhallintapolitiikkaan. Riskienhallintapolitiikka on laadittu vuonna 2015 organisaatiouudistuksen yhteydessä ja se on asetettu uudelleen voimaan vuoden 2019 joulukuussa. Sisällöltään molemmat ovat lähes yhteneväiset. Riskienhallintapolitiikan lisäksi laitoksella on jatkuvuuden hallinnan periaatteet.

Riskienhallintapolitiikan (2019) mukaan sen tavoitteena on turvata THL:n tavoitteiden saavuttaminen, toiminnan jatkuvuus ja henkilöstön hyvinvointi. Lisäksi todetaan, että riskienhallinta on olennainen osa johtamista, ohjausta ja toimintaa. Tavoitteeksi on asetettu, että kaikilla toiminnan tasoilla noudatetaan seuraavia periaatteita:

- Koko organisaatio sitoutuu riskienhallintaan
- Riskienhallinnan vastuunjako on kaikille selvä
- Kaikki ovat tietoisia toimintaansa kohdistuvista riskeistä ja niiden merkityksestä
- Riskienhallinta on järjestelmällistä, jäsenneltyä ja ajantasaista
- Riskeistä ja niiden hallintakeinoista välitetään tietoa avoimesti
- Riskienhallinta on osa päätöksentekoa
- Riskienhallinnan menettelytapoja kehitetään ja parannetaan jatkuvasti

Lisäksi todetaan, että riskienhallinnassa on olennaista, että havaitut riskit käsitellään avoimesti ja viestitään tarkoituksenmukaisella tavalla. Havaintona todetaan että, riskien tuominen yhteiseen keskusteluun parantaa riskienhallintaa ja edistää hallinnon läpinäkyvyyttä.

Jatkuvuudenhallinnan yleisten periaatteiden mukaan kaikki Terveyden ja hyvinvoinnin laitoksen palvelut pyritään tuottamaan mahdollisimman häiriöttömästi ja jatkuvuudenhallinnan lähtökohtana on, että laitoksen toimintaa arvioidaan, suunnitellaan, johdetaan ja toteutetaan

siten, että mahdolliset häiriötilanteet ja poikkeusolot voidaan riittävästi ennalta ehkäistä, ottaen huomioon kustannukset. Jatkuvuudenhallinnan periaatteiden mukaiset jatkuvuussuunnitelmat tulee laatia kaikille laitoksen priorisoitaville toiminnoille ja toiminnan kannalta merkittäville tukitoimille. Vastuista määritellään, että osastonjohtajat vastaa ja valvoo, että heidän vastuullaan olevien toimintayksiköiden jatkuvuudenhallinta toteutetaan näiden periaatteiden mukaisesti.

Turvallisuuden johtamisjärjestelmässä pitäisi Reimanin ja Oedewaldin (2008, 67-68) mukaan olla ainakin organisaation järjestelmälle asetetut tavoitteet, organisoitumisen, kommunikaatiotavat ja -välineet, keinot vaarojen hallintaan, toiminnan tarkastelun ja arvioinnin keinot, vastuualueet ja organisaatiorakenteen sekä vastuualueet, toimintatavat ja resurssit.

Jämsenin (2017, 23-24) tekemän tutkielman perusteella kävi ilmi, että turvallisuusjohtamisjärjestelmä sekä käsitteenä, että toimintaa ohjaavana tekijänä on huomattavan paljon epämääräisempi kuin johtamisjärjestelmä Terveyden ja hyvinvoinnin laitoksella. Vastausten perusteella haastateltavat (turvallisuusasiantuntijat) kyllä pääosin tunnistivat turvallisuusjohtamisjärjestelmän olemassaolon, mutta sitä ei mielletty kovin kehittyneeksi, näkyväksi tai vahvaksi suhteessa organisaation muuhun toimintaan. Pääosin järjestelmä miellettiin teknisen järjestelykysymysten (vastuut ja roolit on määritelty ym.) kokonaisuudeksi. Vastausten perusteella voidaan todeta, että turvallisuusjohtamisjärjestelmän formaalit perusrakenteet ovat hajautettuja ja pirstaloituneita eri toimintojen, tehtävien tai työroolien mukaan tai puuttuvat kokonaan. Toimintasuunnitelmia tehdään edelleen pääsääntöisesti toiminnoittain linjaorganisaation mukaisesti ja irrallisina toisistaan, vaikka turvallisuusryhmän perustaminen on hieman muuttanut suunnittelua ja toimintaa koordinoivampaan suuntaan. Todettiin myös, että kokonaisuuden hallinnassa, suunnittelussa, tavoitteiden asettamisessa ja resurssien varaamisessa ja käyttämisessä nähtiin puutteita. Turvallisuusjohtamisjärjestelmää ei tällä hetkellä faktisesti ole rakennettu kokonaisturvallisuuden näkökulmasta, vaan yksittäisten toimintojen tarpeesta.

Sosiaali- ja terveysministeriön julkaisun (2011) mukaan johdon tehtäviin kuuluvat riskienhallinnan ja turvallisuuden organisoiminen sekä tähän liittyvien vastuiden määrittäminen. Keskeisessä roolissa riskienhallintaa tukevien tehtävien toteuttamisessa on keskijohto ja operatiivisten yksiköiden esimiehet. Esimiehet, jotka vastaavat yksikkönsä toiminnan tuloksesta, vastaavat myös yksikkönsä riskienhallinnasta. Riskienhallinta- ja turvallisuusvastuut perustuvat toimintayksikön normaaliin toimintaan. Pääperiaate on, että vastuualueet ovat niin selkeitä, ettei päällekkäisyyksiä tai epäselvyyksiä ilmene. Vastuuhenkilöillä tulee olla varahenkilöt. (STM 2011, 13)

5 Tutkimuksen toteuttaminen

Tutkimus toteutettiin perehtymällä Terveyden ja hyvinvoinnin laitoksen turvallisuutta koskevaan materiaaliin intranetissa (nimeltään Terho) sekä teemahaastattelujen muodossa. Koska kirjoittaja itse työskentelee Terveyden ja hyvinvoinnin laitoksella, on hänellä mahdollisuus nähdä lähtökohtaisesti kaikki intranetin aineisto ja saada näin laaja kuva laitoksen turvallisuuteen liittyvistä dokumenteista ja muistioista, joiden käyttöä ei ole rajattu vain tietylle ryhmälle. Kirjoittajan työtehtävät eivät kuitenkaan tällä hetkellä liity turvallisuuteen, joten faktojen osalta lähteenä on ollut Terhoon viedyt sivustot, asiakirjat ja muistiot, joita täydennettiin turvallisuusasiantuntijoiden teemahaastatteluilla.

5.1 Johdanto

Terveyden ja hyvinvoinnin laitoksella on turvallisuuteen liittyviä tehtävä nimikkeitä seitsemän kappaletta. Näitä ovat turvallisuuspäällikkö, tietoturvapäällikkö, tietosuojavastaava, työsuojelupäällikkö, valmiuspäällikkö ja bioturvapäällikkö sekä laatupäällikkö. Lisäksi laitoksella on erikseen valmiusjohtaja. Turvallisuuden kokonaisvastuun kantaa työjärjestyksen (THL työjärjestys 2020) mukaan laitoksen johto. Turvallisuusryhmässä on edustettuna kaikki turvallisuuteen liittyvien toimintojen edustajat päällikkötasolla, mutta riskienhallintaan perustuvaa kokonaisturvallisuuden organisointia ja johtamista on syytä tarkastella laajemmassa mittakaavassa. Terveyden ja hyvinvoinnin laitoksen nykytilanteeseen perehdytään kolmella tavalla

- Tutustumalla viraston omiin turvallisuutta koskeviin materiaaleihin intranetissa
- Hyödyntämällä aikaisemmin tehtyjä riskienhallinnan tutkimuksia samaan kohdeorganisaatioon (Virta 2014; Jämsen 2017)
- Teemahaastattelujen avulla

Terveyden ja hyvinvoinnin laitoksen intranet on wiki-pohjainen alusta, jonne kuka tahansa THL:n tunnukset omaava voi tuottaa materiaalia. Intranet on nimeltään Terho ja se on ollut käytössä vuosia. Koska sinne voi kuka tahansa tuottaa materiaalia on selvää, että vuosien saatossa materiaalia on kertynyt runsaasti. Terhon heikkous onkin sen hakuominaisuudet, jonka vuoksi sekä tätä tutkimusta ajatellen, että yleensä käyttöä ajatellen, ei ole varmaa, että turvallisuutta koskeva tieto saavuttaa sen kohderyhmän eli käyttäjät. Turvallisuuden johtamisen yksi keskeinen tekijä on, että materiaali on henkilöstön saavutettavissa aina tarvittaessa sekä viestintä, joka edellyttää, että viesti saavuttaa vastaanottajan oikeaan aikaan ja oikean muotoisena. Terho on tätä tarkoitusta varten huonosti ylläpidetty ja vastuutettu ja turvallisuudesta ja riskienhallinnasta viestiminen sekä materiaalin saatavuus olisikin yksi sen kehittämisen kohteista.

Teemahaastatteluissa selvitellään turvallisuusjohtamista erilaisten teemojen avulla. Teemahaastattelu on puolistrukturoitu haastattelu ja siksi teemoista voidaan poiketa tai jotkin

voidaan kokonaan ohittaa, kun taas toisiin voidaan syventyä laajemmin. Tarkoitus oli saada kokonaiskuvaa eri näkökulmista Terveyden ja hyvinvoinnin laitoksen turvallisuusjohtamiseen. Haastattelukutsu lähetettiin kuudelle, joista kolme vastasi kutsuun ja oli mukana haastatteluissa.

Opinnäytetyön yhtenä lähtökohtana on ollut Matias Virran vuonna 2014 tekemä opinnäytetyö ”Riskienhallintajärjestelmän luominen Terveyden ja hyvinvoinnin laitokselle”. Työssä on pohdittu myös turvallisuuden johtamista ja tehty alustava turvallisuusjohtamisen kehittämissuunnitelma. Sen mukaan Terveyden ja hyvinvoinnin laitoksen turvallisuusjohtamista voidaan ryhtyä rakentamaan luomalla vahva ja yhtenäinen riskienhallintajärjestelmään perustuva hallinnointijärjestelmä. Turvallisuusjohtamisen hallinnointijärjestelmän kehittäminen aloitetaan organisaation turvallisuuden vastuiden ja tavoitteiden määrittelyllä. Turvallisuusjohtamisesta kehitetään toiminto, joka kattaa niin lakisääteisen kuin omaehtoisenkin turvallisuuden hallinnan. Turvallisuusjohtamisessa yhdistyy toimintatapojen, prosessien ja organisaation henkilöstön johtaminen. Turvallisuusjohtamisen tärkeimpänä päämääränä on varmistaa organisaation häiriötön toiminta sekä työnteon ja työympäristön turvallisuus ja terveellisyys. Turvallisuusjohtamista tulee myös kehittää jatkuvasti Demingin -ympyrän (tai -kehän) mukaisesti. Tässä työssä yritetään haastattelujen kautta selvittää myös, miten tuo kuusi vuotta sitten tunnistettu kehittämisen tavoite on saavutettu.

Toisena lähtökohtana on ollut Christian Jämsenin vuonna 2017 tekemä AaltoPron turvallisuusjohdon koulutusohjelman tutkielma ”Turvallisuusjohtamisjärjestelmä osana organisaation johtamisjärjestelmää”. Se keskittyy erityisesti strategisen johtamisen ja turvallisuuden johtamisen yhteensovittamisen dilemmaan ja kohdeorganisaationa oli Terveyden ja hyvinvoinnin laitos. Työssä etsittiin keinoja, joilla turvallisuuden johtaminen voidaan ottaa osaksi organisaation tavoitteiden suunnittelua seurantaa ja jokapäiväistä toimintaa. Jämsenin työ on antanut hyvät lähtökohdat myös tälle opinnäytetyölle, koska se on verrattain tuore ja koska siinä esille nostettuja kehittämiskohteita on otettu huomioon mm. turvallisuusryhmän uudelleenasettamisessa vuoden 2019 alusta.

Sekä Virran (2014), että Jämsenin (2017) työssä turvallisuuden johtaminen riskiperusteisesti ja riskienhallinnan keskeinen rooli turvallisuusjohtamisessa on tuotu vahvasti esiin ja samaa periaatetta on käytetty myös tässä työssä.

5.2 Teemahaastattelut

Haastatteluja on erityyppisiä ja kullekin on oma käyttötarkoituksensa. Strukturoitu haastattelu on tarkoitukseltaan ja toteutukseltaan lähellä kyselyä. Siinä haastattelija on etukäteen suunnittelut haastattelurungon, jota käytetään kaikissa haastatteluissa. Puolistukturoitu haastattelu eli teemahaastattelu sopii sellaisiin tilanteisiin, joissa ei täysin tunneta tutkimuksen kohdetta etukäteen, eikä haluta liikaa ohjata vastaajia. Teemahaastattelussa

haastatteluteemat on suunniteltu huolellisesti etukäteen, mutta sanamuodot sekä kysymysten järjestys ja painotukset saattavat vaihdella haastattelun kesken. Teemahaastattelussa myöhempiä haastatteluja voidaan muokata edellisten haastattelujen mukaan, jos niistä ilmenee jotain mielenkiintoisia asioita, joita ei etukäteen olla osattu ottaa huomioon. (Ojasalo, Moilanen & Ritalahti 2014, 41)

Teemahaastattelu on lomake- ja avoimen haastattelun välimuoto ja puolistrukturoituna haastatteluna lähellä syvähaastattelua. Teemahaastattelussa on tyypillistä, että haastattelun aihepiirit eli teema-alueet ovat tiedossa, mutta kysymysten tarkka muoto ja järjestys puuttuu. (Hirsjärvi ym. 2018, 208)

Mäntynevan ym. (2013, 71) mukaan henkilökohtaisia teemahaastatteluja voidaan toteuttaa kasvokkain tai esimerkiksi puhelimitse. Puhelinhaastatteluja käytetään laajasti kvantitatiivisessa tutkimuksessa, mutta kvalitativiisessa tutkimuksessa se mahdollistaa syvällisen tutkimustiedon keräämisen. Lisäksi he toteavat, että mitä väljempi runko haastattelussa on, sitä enemmän osaamista ja kokemusta haastattelijalta vaaditaan.

Kananen (2012, 99) toteaa, että teemahaastattelua käytetään ymmärryksen hakemiseen ja, että kyselemällä urkitaan asian ydin, mikä tarkoittaa totuuden paljastamista.

Teemahaastattelussakaan ei voi kysellä ihan mitä tahansa, vaan siinä pyritään löytämään merkityksellisiä vastauksia tutkimuksen tarkoituksen ja ongelmanasettelun tai tutkimustehtävän mukaisesti. Periaatteessa etukäteen valitut teemat perustuvat tutkimuksen viitekehykseen eli asioista, joita jo tiedetään tutkittavasta ilmiöstä. Teemahaastattelun avoimuudesta riippuen teemojen sisältämien kysymysten suhde tutkimuksen viitekehyksessä esitettyyn kuitenkin vaihtelee intuitiivisten ja kokemusperäisten havaintojen sallimisesta varsin tiukasti vain etukäteen tiedetyissä kysymyksissä pitäytymiseen. (Tuomi & Sarajärvi 2018, 88)

Tässä tutkimuksessa haastattelumuotona käytetään teemahaastattelua ja teemahaastattelun teemat on toimitettu haastateltaville etukäteen haastattelukutsun mukana, jotta heillä on ollut mahdollisuus valmistautua teemojen pohdintaan. Teemahaastattelun mukaisesti teemojen sisällä on liikuttu ja haastateltavan alueen mukaisesti toisia teemoja on painotettu, kun taas toisia on voitu jättää kokonaan pois tai käsitellä vain ohuesti.

5.3 Haastattelujen toteuttaminen

Teemahaastattelut toteutettiin kesä-elokuussa 2020 keskellä koronan aiheuttamaa poikkeustilaa. Terveyden ja hyvinvoinnin laitoksella on keskeinen rooli koronan torjunnassa, tilastoinnissa ja viestinnässä.

Teemahaastattelut olivat yksilöhaastatteluja ja haastateltavina oli kolme henkilöä Terveyden ja hyvinvoinnin laitoksella. Heidän tehtävänsä sijoittuvat organisaatiossa sekä hallinto- ja

kehittäminen, että terveysturvallisuusosastolle ja työtehtävät käsittävät työturvallisuuteen, valmiuteen ja jatkuvuuden hallintaan sekä bioturvallisuuteen liittyviä johtotehtäviä ja kansallista ja kansainvälistä yhteistyötä. Kaikki haastateltavat kuuluvat sekä turvallisuusryhmään, että valmiusryhmään. Kysymysten tarkoitus oli saada ymmärrys siitä mistä Terveyden ja hyvinvoinnin laitoksen riskienhallinnassa ja turvallisuuden johtamista toteutetaan ja mikä on riskienhallinnan, turvallisuuden organisoinnin ja kansallisen ja kansainvälisen yhteistyö tilanne ja miten niitä pitäisi kehittää?

Haastattelut toteutettiin Skype -kokouksina ja niissä ei käytetty kameraa. Haastattelu aloitettiin esittelyllä ja johdannolla ja jokaisen teeman kohdalla annettiin lyhyt johdanto teemaan. Teemahaastattelun mukaisesti teemasta voidaan poiketa, sitä voidaan syventää tai joitakin teemoja voidaan kokonaan ohittaa.

Haastattelut keskittyvät yhdeksän (9) teeman ja vapaan sanan ympärille. Teemat ovat seuraavat

1. Riskienhallinnan yleiskuva
2. Turvallisuuden organisointi ja vastuuttaminen
3. Riskienhallinnan kattavuus
4. Globaalien riskien seuranta
5. Kyberuhat ja jatkuvuuden hallinta
6. Kansallinen vaikuttavuus ja yhteistyö
7. Kansainvälinen yhteistyö
8. Hyviä riskienhallinnan esimerkkejä
9. Turvallisuuskulttuuri
- Vapaa sana

Tarkemmat kuvaukset haastattelun kysymyksistä ja johdannosta on liitteessä 2.

Haastatteluun oli varattu kaksi tuntia aikaa ja haastattelu nauhoitettiin, jotta joihinkin kohtiin voitiin palata jälkeenpäin. Haastattelija kirjasi ylös haastattelun aikana nousseita asioita eli haastattelusta on sekä nauhoite, että tekstimuotoinen muistio. Haastatteluja ei tässä työssä julkaista sellaisenaan, eikä haastateltavien nimiä tule esille. Haastatteluista on tehty yhteenvedot, jotka ovat otsikoita teemoittain, joitakin yhdistellen ja joista on tehty tutkimuksen johtopäätökset.

5.4 Löydökset ja yhteenveto haastatteluista

Tässä kappaleessa tehdään yhteenveto teemahaastattelussa esille nousseista asioista. Teemahaastattelun luonteen mukaisesti joihinkin teemoihin pureuduttiin syvällisesti ja jotkin jäivät kevyemmälle käsittelylle asiantuntijan oman kokemuksen ja tietämyksen mukaisesti. Tärkeää

oli saada kokonaiskuva Terveyden ja hyvinvoinnin laitoksen turvallisuuden johtamisen tilanteesta ja aikaisempien tutkimusten (Virta 2014; Jämsen 2017) esille nostamien kehittämiskohteiden nykytilasta ja uusista kehittämiskohteista. Kappaleen alaotsikointi ei ole teemahaastattelun teemojen kanssa täysin yhtenevä, vaan yhteenvedossa on jossain määrin yhdistelty eri teemojen kautta nousseita asioita niin, että kokonaiskuva olisi sellainen, josta näkee keskeiset esille nousseet kehittämiskohteet.

5.4.1 Yleistä

Turvallisuuden johtaminen ja koordinointi keskittyy turvallisuusryhmälle ja normaaliolojen häiriötilanteissa ja poikkeusoloissa lisäksi valmiusryhmälle, mutta mukana on myös viestintä, valtion erityispalvelut ja mielenterveyden asiantuntijat. Molemmissa on melko kapea-alaisesti edustettuna yksiköt koko THL:n näkökulmasta ja edustus on painottunut hallinnon tukipalveluiden ja terveysturvallisuuden yksiköihin. Henkilökunnan osallistaminen turvallisuustyöhön ja oman työnsä merkitys kokonaisturvallisuudessa on osittain epäselvää ja vaihtelee osastoittain. Joissakin yksiköissä turvallisuuden merkitys ja turvallisuuskulttuuri ymmärretään hyvin, kun taas toisessa yksikössä se on täysin vieras asia.

Riskienhallinta käsittää kaikki riskienhallinnan osa-alueet, mutta painostusta on työturvallisuuteen ja bioturvallisuuteen, joissa molemmissa turvallisuuden merkitys työn tekemiseen on sisäistetty. Työturvallisuus koskee koko henkilökuntaa ja bioturvallisuus erityisosaajien asiantuntijaryhmää, jossa työtä tehdään turvallisuusorientoituneessa ympäristössä. Riskienhallintajärjestelmä Granite toimii hyvin niissä kategorioissa missä sitä käytetään, mutta sen käyttöä pitäisi edelleen laajentaa ja helpottaa tuomalla se osaksi jokaisen osaston riskienhallintaa. Granitessa esiin nousseita riskejä käsitellään sekä esimiesten kanssa osastoittain, että yhteisessä johtamisfoorumissa, jossa on edustettuna kaikkia laitoksen esimiehet ja ylin johto. Turvallisuushavaintoja tehdään pääasiassa Intranettiin, joka on matalan kynnyksen foorumi kirjata havaintoja, kun taas Graniten käyttö vaatii korkeamman kynnyksen ja useimmissa yksiköissä on nimetyt henkilöt, jotka tekevät kirjauksia Graniteen. Riskienhallinnan ja turvallisuushavaintojen yhdistäminen toisi etuja kokonaisuuden hallintaan, mutta Graniten käytön kynnystä pitäisi alentaa, ettei menetetä sitä helppoutta, joka nyt on turvallisuushavaintojen kirjaamisessa.

Vuonna 2015 aloitettu ja vuonna 2019 uudistettu turvallisuusryhmän toiminta koettiin pääosin positiivisena ja turvallisuutta edistävänä asiana. Jossain määrin herätti keskustelua turvallisuusryhmän asiantuntijoiden sijoittuminen vain kahteen osastoon. Siinä on vaarana, että turvallisuutta ei muissa osastoissa mielletä omaksi asiaksi ja jätetään se muiden hoidettavaksi, kun samaan aikaan nousi esille tarve vahvemmin osallistaa koko henkilöstö turvallisuustyöhön ja saada heidän ymmärtämään oman työnsä merkitys kokonaisturvallisuudelle. Myös vastakkaisia mielipiteitä oli ja turvallisuusasioiden kattavuutta pidettiin hyvänä ja nykyistä

toimintatapaa onnistuneena turvallisuusryhmän toimiessa operatiivisen turvallisuuden johtamisen foorumina. Haastatteluissa kävi ilmi, että turvallisuusryhmän kokouksia voisi nykyisen viiden tai kuuden sijasta olla useammin esim. kuukausittain, jotta kaikkiin turvallisuuden osa-alueisiin liittyvät asiat ehdittäisiin käsitellä. Nyt usein näin ei ole ja haastatteluissa tuli ilmi epäilys, että osa asioista käsitellään turvallisuusryhmän ulkopuolella, mikä hämärtää kokonaisturvallisuuden tilannekuvaa ja riskikuvaa. Turvallisuusryhmän puheenjohtaja raportoi organisaation johdolle ainakin kerran tai pari kertaa vuodessa turvallisuusasioista, mutta johdon ymmärryksen lisäämistä riskeistä ja turvallisuusasioista yleensä ajateltiin kaivattavan lisää eli turvallisuuden johtamisen integroimista organisaation johtamiseen pitäisi parantaa. Havaittiin, että ylimmän johdon edustaja ei ole vielä vieraillut turvallisuusryhmässä ja turvallisuusasioiden virallinen tie johdon tietoisuuteen kulkee turvallisuusryhmän puheenjohtajan raporttina. Lisäksi nähtiin, että turvallisuusryhmässä tulisi käsitellä enemmän matkustusturvallisuuteen liittyviä asioita, vaikkakin ne ovat nyt otettu yleisen turvallisuuskoulutuksen listalle. Yleisesti ottaen havaittiin, että turvallisuusryhmä on tuonut turvallisuuden johtamiseen ja hallinnointiin kaivattua jämäkkyyttä, jatkuvuutta ja rakennetta, mutta asioiden käsittelyä ja laajuutta pitäisi syventää, organisaation johdon tuki turvallisuustyölle pitäisi tuoda selkeämmin esille ja henkilöstön saamista mukaan turvallisuustyöhön pitäisi edistää. Toisaalta nähtiin, että turvallisuusryhmän toiminta on jatkuvasti parantunut ja ryhmä on hyvin ryhmäytynyt ja organisoitunut.

Turvallisuusryhmän ja valmiusryhmän keskinäiset roolit nähtiin selkeinä. Turvallisuusryhmä vastaa jokapäiväisesti operatiivisesti turvallisuuden johtamisesta ja takaa laitoksen normaalin toiminnan turvallisuuden, kun taas valmiusryhmä on valmiudessa oleva toimija, joka nousee esille, kun normaalioloista siirrytään normaaliolojen häiriötilanteisiin tai poikkeusoloihin. Haasteena valmiusryhmässä nähtiin, että siinä toimitaan oman toimen ohella ja esim. harjoitteluun jää huonosti aikaa ja ryhmän toiminnan tehokkuutta voidaan mitata vain todellisissa tilanteissa.

Yleinen turvallisuuskoulutus nostettiin esiin onnistuneena muutoksena. Sitä on saatavilla ympäri vuoden ja mukaan otettu matkustusturvallisuuden osuus on ollut tervetullut. Siihen kuitenkin kaivattaisiin lisää koulutusta ja erityisesti maakohtaisia riskianalyyseja ja tarkkojakin ohjeita mm. tietoteknisten laitteiden mukaan ottamisesta ja käytöstä.

Työturvallisuus koskettaa kaikkia Terveyden ja hyvinvoinnin laitoksella työskenteleviä ja vierailijoita. Työturvallisuusasiat nähtiin olevan hyvässä kunnossa koko laitoksessa ja turvallisuushavainnoista saadaan jatkuvasti uutta tietoa, jolla sitä kehitetään entisestään. Terveyden ja hyvinvoinnin laitoksella työskentelee THL:n henkilökunnan lisäksi monia muita toimijoita ja työlainsäädännöstä tuleva yhteisen työpaikan (Työturvallisuuskeskus 2020b) käsite nostaa esiin tarpeen miettiä yhteisiä turvallisuuden pelisääntöjä, joka Terveyden ja hyvinvoinnin laitoksella se tarkoittaa, että pitäisi luoda yhteiset työturvallisuuden, perehdyttämisen,

turvallisuushavaintojen ja harjoittelun pelisäännöt kaikkien niiden toimijoiden kanssa, jotka toimivat Terveyden ja hyvinvoinnin laitoksen tiloissa.

Turvallisuuden organisointi ja hyvien turvallisuuskäytänteiden laajentamista yli siilomaisen osastorakenteen niin, että koko henkilöstö kokee turvallisuustyön omakseen ja ymmärtää sen merkityksen omassa työssään sekä tunnistaa siihen liittyvät riskit ja osaa ja haluaa raportoida niistä matalalla kynnyksellä turvallisuusorganisaatiolle, vaatii uutta kokonaisvaltaisen turvallisuuden merkityksen pohdintaa. Osastojen roolia riskien tunnistamisessa ja hallinnassa ja yleistä vastuuta laitoksen kokonaisturvallisuudesta pitäisi konkretisoida. Samalla nousi esille tarve miettiä, onko nykyinen turvallisuusryhmä riittävän monipuolinen ja osastojen tarpeet, mutta myös vastuuttamisen huomioon ottava turvallisuuden johtamisen foorumi ja onko dialogi organisaation johdon kanssa riittävää niin, että turvallisuusasiat tulevat kokonaisvaltaisesti huomioiduksi laitoksen johtamisessa. Osastoilla, joilla ei ole edustusta turvallisuusryhmässä, voi olla haasteellista ymmärtää turvallisuusryhmän asioita ja niiden merkitystä omalle toiminnalle. Turvallisuusryhmän vaikuttamismahdollisuuksia myös pohdittiin. Nyt käytetään pehmeitä keinoja ohjeistuksen ja neuvojen muodossa, mutta jos osastojen rooli turvallisuudessa ja riskienhallinnassa olisi suurempi, voisi olla mahdollista antaa suoria määräyksiä ja käskyjä organisaatiotasolla ja näin harmonisoida viraston kokonaisturvallisuuden johtamista. Haastatelluissa todettiin, että esimiesten velvollisuus on toteuttaa turvallisuusryhmän ehdotukset ja juuri esimiesten kautta onkin onnistuttu viemään toisaalta turvallisuusryhmän sanomaa osastoille ja toisaalta saamaan informaatiota osastojen turvallisuuden ja riskienhallinnan tilanteesta turvallisuusryhmälle. Haasteeksi nähtiin, että turvallisuusasiat saattavat työpaineessa jäädä huomiotta osastoilla ja turvallisuusryhmän ehdotusten toteuttamista siirretään ajanpuutteen vuoksi. Esimiesten roolin lisäksi osastojen johtajan roolia korostettiin turvallisuusasioissa esimerkkinä toimimisena ja turvallisuuskulttuurin edistäjänä. Myöskin auditointien tekeminen osastoille on todettu auttavan turvallisuusasioiden ymmärryksen lisäämisessä ja niitä suositeltiin tehtäväksi enemmän.

Yhteistyö kansallisella ja kansainvälisellä tasolla sekä viranomaisten ja muiden turvallisuusorganisaatioiden kanssa nousi esille kehittämistarpeena. Turvallisuuden kokonaisuus on jatkuvasti monimutkaistuva maailma, jossa tiedon saanti ja sen perusteella tehty tilannekuva toimintaympäristöstä on entistä tärkeämpää tuottaa nopeasti eri lähteistä kokoamalla. Organisaation johtaminen pitää perustua tietoon ja tiedon kerääminen eri lähteistä ja sen yhteismitallistaminen on keskeistä, jotta ymmärretään tiedon arvo ja sen merkitys organisaatiolle ja organisaatiota koskevien riskien priorisoinnille. Relevantin tiedon suodattaminen tiedolla johtamisen perustaksi asettaa suuria vaatimuksia sekä tiedon lähteelle, että sen käsittelylle. Toisaalta todettiin, että joillakin aloilla kansallista ja kansainvälistä yhteistyö on ollut avainasemassa ja sitä tehdään hyvin laajasti ja sitä kautta saadaan arvostusta ja vaikuttavuutta. Monella alalla Terveyden ja hyvinvoinnin laitoksen henkilö istuu kansainvälisissä työryhmissä ja EU:n päätöksenteon foorumeissa EU:n lainsäädännön asioissa.

5.4.2 Turvallisuuden organisointi ja vastuuttaminen

Turvallisuusryhmän aloittaminen vuonna 2015 on osoittautunut hyväksi päätökseksi. Substanssiosastoilta on vain kaksi edustajaa kahdeksasta ja substanssipuolen edustus pitäisi näkyä vahvemmin, jotta dialogi osastojen kanssa olisi vahvempaa. Turvallisuusorganisaatiosta puuttuu ainakin kaasuturvallisuudesta vastaava henkilö, joka kyllä työskentelee laitoksessa, mutta ei kuulu turvallisuusryhmään. Maineriskien hallinnasta ei yleensä ole ollut puhetta, eikä niitä ole huomioitu. Turvallisuusryhmän ja valmiusryhmän välinen roolijako on selvä ja nykyinen toimintatapa koettiin hyväksi. Turvallisuusryhmän operatiivisen toiminnan roolia ja esimiesten vastuuta turvallisuusasioiden edistämisessä turvallisuusryhmän antamien suositusten ja ohjeiden pohjalta korostettiin useassa haastattelussa. Myös viestintä haluttiin mukaan turvallisuusryhmän toimintaan, vaikkakin se on nyt valmiusryhmässä edustettuna.

Yleisesti ottaen todettiin, että Terveyden ja hyvinvoinnin laitoksessa on laajasti turvallisuuden eri osa-alueita. Tarvitaan paljon erilaista osaamista ja on hyvä, että THL:ssä on kaiken kattava lähestymistapa ja omasta alueesta vastaavat tekevät yhteistyötä. Toimivaltaa turvallisuusryhmällä ei ole vaan päällikkövirastona implementointi tapahtuu yksikönpäälliköiden toimesta. Turvallisuusryhmä voi antaa suosituksia ja ohjeita, mutta ei voi määrätä osastoja. Siiloutumisen ongelma ja turvallisuusryhmässä osastojen kapea edustavuus tiedostettiin, mutta samalla korostettiin johtamisfoorumin roolia turvallisuustietoisuuden leviämisessä ja sen kautta esimiesten ja osastojen johdon merkitystä turvallisuusasioiden edistäjänä omilla osastoillaan ja yksiköissään. Haastattelussa tuli ilmi, että osastojen johtajien osallistumista turvallisuusryhmän toimintaan ei pidetty tarpeellisena, vaan pidettiin riittävänä sitä, että johtamisfoorumilla käsitellään turvallisuusasioita ja sitä kautta tieto relevanteista asioista menee osastoille esimiesten ja osastojohtajien kautta. Toisaalta todettiin, että turvallisuusasioiden merkityksen ymmärtäminen substanssissa saattaisi edellyttää laajempaa ymmärrystä kokonaisvaltaisesta turvallisuudesta, johon ei kuitenkaan ole mahdollisuutta perehtyä pelkästään johtamisfoorumin puitteissa, jossa turvallisuusasioille on rajoitettu aika käytettävissä.

Turvallisuuden johtamisessa yleensä epäselväksi on jäänyt mitä oikeastaan tarkoitetaan kokonaisvaltaisella turvallisuusjohtamisella. Sen pohjalla pitäisi olla näkyvillä ja helposti saatavilla erilaiset standardit, mutta tällä hetkellä on vaikea löytää dokumentteja mihin tämän hetken turvallisuuden johtaminen perustuu. Standardit pitäisi helposti olla löydettävissä ja näkyvillä, kuten kaikki muukin toimitilojen ja henkilöstön turvallisuuteen liittyvä materiaali. Myös mahdolliset auditoinnit ja niiden tulokset pitäisi olla nähtävillä esimerkiksi aulassa ja kannustamassa turvallisuuden positiiviseen huomioimiseen ja turvallisuuskulttuurin luomiseen. Turvallisuusasioita on kyllä nostettu esille, mutta katvealueita on havaittavissa parannettavaa on paljon.

Valmiusasiat on haastateltavien mielestä hyvin huomioitu ja ne myös löytyvät helposti. Valmiusryhmän toimintaan oltiin lähtökohtaisesti tyytyväisiä, mutta senkin toiminnasta löytyi keskusteluissa kehitettävää. Valmiusryhmän toiminnan lähempi tarkastelu ja kehittäminen voisikin olla yksi jatkotutkimuksen kohde.

Haastatteluissa johtamisen heikkona lenkkinä pidettiin sitä, että turvallisuusjohtamisjärjestelmää ei vieläkään nähtävästi ole integroitu johtamisjärjestelmään tai se on epäselvä. Riskienhallintajärjestelmän osalta työturvallisuus ja strategiset riskit ovat selvimmin esillä Granitessa, mutta Granite vaatisi vielä kehittämistä, jotta se vastaisi kaikkeen riskienhallinnan tarpeisiin. Oli myös epäselvää, miten Granitea hyödynnetään johtamisjärjestelmässä.

Vastuuttamisesta kävi ilmi, että työturvallisuusasioissa esimies vastaa oman alueensa riskienarvioinnista ja esimies on valinnut turvallisuuden arvioijat (OTO rooli). Keskustelut esimiesten kanssa ovat lisänneet tätä ymmärrystä. Ylimmän johdon tukea tarvittaisiin siihen, että eri osastot arvioivat omat riskinsä ja todettiin, että keskitetty johtaminen turvallisuudesta ja riskienhallinnasta puuttuu. Turvallisuusryhmä kyllä raportoi johdolle, mutta sitä pitäisi tehdä useammin ja laajemmin. Nyt vain pieni osa asioista menee ylimmän johdon tietoon.

5.4.3 Riskienhallinnan kattavuus

Haastatteluissa todettiin, että riskien arviointi on parantunut Graniten käyttöönoton (2015) myötä ja nyt riskejä seurataan aktiivisesti, mutta järjestelmällisyyttä voitaisiin parantaa. Riskeistä todettiin, että työsuojeluriskit nousevat parhaiten esille ja niitä kirjataan ahkerimmin ja valmiuteen ja jatkuvuuteen liittyvät riskien käsittely on parantunut, mutta se ei ole vieläkään hyvällä tasolla. Joidenkin erityisriskien, kuten bioturvariskien arviointiin, ei Granite sovellu, eikä Granitessa yleensäkään voi kaikkia riskejä käsitellä, jonka vuoksi joillakin osastoilla on oma riskienhallintajärjestelmänsä.

Riskien tunnistamiseen ja luokitteluun sekä priorisointiin kaivattiin selkeyttä. Granitessa on kahden tasoista matriisi todennäköisyyden ja vaikutuksen arviointiin ja tätä ei ihan ymmärretty miksi tarvitaan kaksi erilaista mittaustapaa. Todettiin myös, että työturvallisuuteen liittyvät riskit tunnistetaan ja käsitellään osastotasolla, kun taas strategisia riskejä käsitellään laitostasoisina. Raportoinnissa johdolle tämä pitää huomioida. Granitesta todettiin, että sen käyttöönotto on jäänyt kesken ja muitakin riskikategorioita kuin nyt käytössä olevat työturvallisuus ja strategiset riskit pitäisi ottaa käyttöön. Operatiiviset riskit, tietoriskit ja ympäristöriskit mainittiin erillisinä kategorioina. Granitessa on myös omat moduulit auditoinneille ja turvallisuushavainnoille ja näiden käyttöönoton tarpeellisuutta pitäisi selvittää. Toisaalta todettiin, että on hyvä, kun turvallisuushavainnot kirjataan Terhoon, koska sen käyttökynnys on matalampi kuin Graniten. Graniten raportointimahdollisuuksia pidettiin erittäin onnistuneina. Graniten heikkoudeksi nähtiin myös, että siellä ei arvioida taloudellisia riskejä osastoilla ja

osastojen toiminnallisuus saattaa vaarantua taloudellisten riskien realisoituessa. Granitea ollaan kuitenkin kehittämässä ja sille on tekeillä kehittämissuunnitelma ja se on tarkoitus uudistaa vielä vuoden 2020 aikana.

Yhteisen työpaikan käsite tuli myös riskienhallinnan kohdalla esille haastatteluissa. Terveyden ja hyvinvoinnin laitos on työturvallisuuslain mukainen yhteinen työpaikka, jossa käytetään yhteisiä valtion palveluita ja yhteisen työpaikan mukaisesti pitäisi työturvallisuusriskejä arvioida ja käsitellä yhteisissä foorumeissa muiden tiloissa toimivien kanssa.

Hyvänä asiana pidettiin sitä, että Granitessa on mahdollista tehdä vertailua (benchmarking) joidenkin muiden valtiohallinnon organisaatioiden kanssa. Tämä tukee myös edellä mainittua yhteisen työpaikan turvallisuuskäsitteen periaatteita.

Riskien arviointia on tehty ja tehdään edelleen myös laatujärjestelmän kautta. Erityisesti laboratorioissa käytetään laatujärjestelmän avulla tehtävää riskien arvointia, eikä näitä riskejä viedä Graniteen.

5.4.4 Kyberuhat ja jatkuvuuden hallinta

Haastattelussa todettiin, että jatkuvuuden näkökulmasta turvallisuuden eri osa-alueilla tehdään jonkin verran auditointeja ja tarkastuksia, mutta tietoturvallisuuteen liittyen näitä ei tehdä samalla tavalla ja siihen kaivattiin tehostusta, että tietotalona Terveyden ja hyvinvoinnin laitoksen tiedon turvaamiseen ja siihen liittyviin menetelmiin olisi enemmän osasto- ja yksikkökohtaisia ohjeita. Se edellyttää, että tietoturvallisuuden asiantuntijat jalkautuisivat osastoille ja tekisivät siellä tarkastuksia ja auditointeja. Toisaalta todettiin, että näitä tietoturvapäällikön tekemiä auditointeja on jo tapahtunut.

Kyberuhkiin liittyviä kysymyksiä pidettiin lähinnä tietoturvapäällikön vastuualueen asioina ja niihin liittyviä ilmoituksia käsitellään tietoturvapäällikön ja tietosuojavastaavan toimesta ja niistä tiedotetaan tarvittaessa Terhossa ja käsitellään turvallisuusryhmässä tai tietoturvaryhmässä. Kyberturvallisuudesta todettiin, että termi on aika vieras ja ainakaan tällä termillä asioista ei juuri ole keskusteltu, mutta varmaankin niihin liittyviä uhkia on käsitelty eri nimikkeillä. Haastattelussa tuli kuitenkin ilmi, että riski sille, että tietoverkkojen kautta voidaan manipuloida vaikkapa laboratorioiden olosuhteita ja aiheuttaa näin vääristyneistä mittaustuloksia tai suorainaista vahinkoa ja tuhoa laboratorioympäristössä tunnistettiin uhaksi jatkuvuudelle, mutta asioista on keskusteltu vähän ja riskikartoituksia on tehty marginaalisesti. Tässä nousi esille myös vastuukysymys, siitä kenen vastuulla on miettiä näitä asioita osastolla. Jatkuvuussuunnittelusta todettiin, että se ei saa olla staattinen paperi vaan sitä pitää tehdä dynaamisesti ja päivittää jatkuvasti tarpeen mukaan.

5.4.5 Globaalit riskit ja kansallinen ja kansainvälinen yhteistyö

Globaaleista riskeistä todettiin, että niitä seurataan eri lähteistä. Työturvallisuuden osalta esimiehet saavat tiedon globaaleista riskeistä työturvallisuusorganisaation kautta ja bioturvallisuuden osalta esimerkkeinä todettiin olevan WHO:n International Health Regulations, josta tietoa saadaan päivittäin ja riskien seuranta on aktiivista sekä lisäksi käytössä on Early Warning Risk System (CREWS), joka toimii eurooppalaisena riskien havainnointi ja varoitus järjestelmänä bioturvallisuuden alueella. Vuosittainen Global Risk Report (GRR 2019) pitäisi vuosittain jossakin tilaisuudessa avata henkilöstölle ja miettiä miten siinä esille nousevat riskit vaikuttavat ja uhkaavat Terveyden ja hyvinvoinnin laitoksen toimintaa. Matkustusturvallisuuden osalta erityisesti kaivattiin lisää globaalia yhteistyötä ja kansainvälistä tiedonvaihtoa. Kansainvälistä yhteistyötä kaivattiin myös laajemmin, koska maailma kutistuu ja tietoa pitäisi voida vaihtaa nopeasti etenevistä uhkista lähes reaaliajassa.

Terveyden ja hyvinvoinnin roolista kansallisena ja kansainvälisenä toimijana todettiin, että yhteistyö on avainasemassa ja, että vaikuttavuus on koronan myötä kasvanut huomattavasti. THL toimii asiantuntijana sekä kansallisissa, että kansainvälisissä foorumeissa mm. EU:ssa WHO:ssa. Todettiin kuitenkin, että Terveyden ja hyvinvoinnin laitoksen rooli on enemmän tutkimuksellinen ja vaikuttavuus riippuu siitä, miten hyvin osataan viestiä ulospäin. THL saa äänensä kuuluvilla, kun kerrottavaa on.

Kansallinen ja kansainvälinen yhteistyö liittyy Terveyden ja hyvinvoinnin laitoksen rooliin osana yhteiskunnan kokonaisturvallisuutta, mikä vaikuttaa kaikkiin kansalaisiin. Valmiusryhmällä on oma erityinen tehtävä normaaliolojen häiriötilanteissa ja poikkeusoloissa ja yhteiskunnan kriisitilanteissa varmistaa rekisteriaineistojen ja muiden elintärkeiden tietokantojen turvallisuus ja tämä asettaa laitoksen turvallisuuden strategiselle ja operatiiviselle ja toiminnalle aivan erityisen vastuun, joka tulee osaksi turvallisuuden johtamista eri osa-alueiden kautta. Kokonaisvaltaisen turvallisuuden operatiivisen toiminnan ja johtamisen tulee muodostaa vahva ketju, jossa ei ole heikkoja lenkkejä.

5.4.6 Turvallisuuskulttuuri

Haastatteluissa todettiin, että turvallisuuskulttuuri on parantunut viime vuosina. Vaatimukset turvallista ympäristöä kohtaan ovat tiukentuneet ja lainsäädäntö sekä valtiohallinnon ohjeistus ohjaa entistä tiukemmin virastoja kiinnittämään huomiota kokonaisvaltaisen turvallisuuden toteuttamiseen. Laatujärjestelmää (SFS-ISO 9000) on vuosien ajan noudatettu ja sen kautta on tullut käyttöön myös turvallisuuteen liittyviä toimintamalleja, kuten ”puhtaan pöydän periaate” eli että työpäivän jälkeen tai taukojen aikana työpöydälle ei jätetä arkaluonteisia papereita. Turvallisuuskulttuurin kehittämiseen ja esimiesten sitoutumiseen liittyen hankittiin vuonna 2018 kaikille esimiehille verkkokoulutuslisenssit, joiden avulla esimiehet voivat suorittaa työturvallisuuden verkkokoulutuksen. Lopulta vain 12/44 henkilöä suoritti

kurssin. Vuoden 2020 aikana tarjolla on ollut verkkovalmennuksena ”Esimies työturvallisuuden ja työhyvinvoinnin johtajana”, joka saatavilla esimiesten lisäksi uusille tiimipäälliköille.

Turvallisuuskulttuuri ei ole sillä tasolla, että turvallisuushavaintoja tehtäisiin aktiivisesti. Vuosittain on nyt vain noin 90 havaintoa. Turvallisuusasiat pitäisi saada johtoryhmän agendalle, jossa ne ei tällä hetkellä ole. Tästä puhuttu, mutta ei ole tapahtunut. Johtajien esimerkki on todella tärkeää, että noudatetaan omia ohjeita ja olla esimerkkinä. Turvallisuusasioita ei pidä vähätellä ja hiljaisen hyväksymisen kulttuurista pitäisi päästä eroon. Tarkoittaa, että esimiehet ei katso sormien välistä turvallisuusrikkomuksia. Toisaalta todettiin, että turvallisuushavaintojen julkisuus on lisännyt tietoisuutta niistä ja osaltaan ollut parantamassa turvallisuuskulttuuria, kun ei tehdä samoja virheitä uudestaan.

Esimerkkinä turvallisuuskulttuurin kehittämisen tarpeesta nousi esille mobiililaitteiden käyttö julkisissa tiloissa. Kännykkään saatetaan puhua arkaluonteisiakin asioita ja sähköposteja ja muita viestejä selataan välittämättä ympärillä olevista ihmisistä. Arveltiin, että älypuhelimesta on tullut niin kiinteä osa jokapäiväistä elämää, että sen käyttöä työasioiden hoitoon julkisessa tilassa, ei mielletä turvallisuusriskiksi. Myös kannettavien osalta todettiin, että ne jäävät helposti pöydälle tai sellaiseen paikkaan, josta niitä on helppo vakoilla tai laite varastaa. Tiedostojen osalta todettiin kuitenkin, että ne ovat useimmiten turvassa pilvessä tai verkkolevyllä eikä tiedostojen lopullinen katoaminen tai joutuminen vääriin käsiin ole enää merkittävä riski. Tietoturvan kiristymisen todettiin myös olevan yhteistyötä vaikeuttava asia, kun tiedostojen jakaminen yhteistyökumppanille voi olla mahdotonta ilman fyysistä tapaamista. Yleisesti havaittiin, että tietoturva on kiristynyt ja tietoturvatietoisuus on parantunut. Sen sijaan fyysisen turvallisuuden riskiä todettiin lisäävän ihmisten hyväntahtoisuus ja ovia helposti avataan tuntemattomille, vaikka ei saisi ja henkilökortin puuttumisesta on suuri kynnys huomauttaa, vaikka ohjeissa näin kehotetaan toimimaan. Ihmisten ymmärrys omaan työhönsä liittyvistä riskeistä todettiin olevan kaksinainen. Toisaalta arkaluonteisia tietoja käsittelevät ymmärtävät työnsä riskit ja osaavat ne huomioida ja toisaalta jotkin ajattelevat, että turvallisuus on organisaation vastuulla ja sen hoitamiseen on nimetty henkilöt, eikä asiaa tarvitse yksittäisen työntekijän ajatella sen enempää. Tätä ajatteluvääristymää on yritetty poistaa yleisillä turvallisuuskoulutuksilla, joihin kaikkien tulee osallistua. Vuosittain useasti järjestettävä yleinen turvallisuuskoulutus on yksi merkittävät turvallisuuskulttuurin luoja Terveyden ja hyvinvoinnin laitoksella, johdon ja esimiesten esimerkkiä unohtamatta.

Haastatteluissa todettiin lisäksi, että Terveyden ja hyvinvoinnin laitoksessa ei välttämättä ymmärretä, miten keskeinen toimija se on osana Suomen turvallisuusympäristöä ja THL:n turvallisuuden johtamisen onnistunut toteuttaminen on periaatteessa osa koko valtiohallinnon turvallisuuden korkeampaa tasoa. Tämän ymmärryksen lisäämiseksi laitoksen turvallisuuskulttuurin kehittymisellä on aivan keskeinen rooli.

5.4.7 Vapaa sana

Haastatteluissa nousi vapaa sana -osiossa neljä asiakokonaisuutta, joita ei teemakohtaisissa kappaleissa oltu käsitelty.

- Riskienhallintajärjestelmän olemassa oloa pitää painottaa ja tuoda sen kautta esille konkreettisia asioita, joilla on vaikutusta turvallisuuteen ja sen ymmärtämiseen työntekijätasolla omassa työssä.
- Viestinnällä on suuri rooli asioiden eteenpäin viemisessä ja sen merkitystä pitää korostaa. Asioista pitää puhua ymmärrettävästi ja kattavasti ja viestintäkanavia pitää kehittää.
- Valmiusryhmässä työskentelyn haasteena koettiin, että turvallisuustyön tekemisellä OTO:na on vaikutusta ryhmän toimintaan ja että työasioita joudutaan priorisoimaan valmiusryhmän toiminnan kustannuksella. Valmiusryhmän toimintaa pitäisi arvioida omana tutkimuksenaan.
- Terveyden ja hyvinvoinnin laitoksella vierailevat tutkijat ja muut toimijat, jotka saavat käyttöoikeuden tietojärjestelmiin ja resursseihin, mutta eivät ole THL:n työntekijöitä, saattavat muodostaa odottamattoman uhkan, joka pitäisi arvioida.

5.5 Tutkimuksen reliabiliteetin ja validiteetin tarkastelu

Hirsjärven mukaan (2018, 231) tutkimuksessa pyritään välttämään virheiden syntymistä, mutta silti tulosten luotettavuus ja pätevyys vaihtelevat, jonka vuoksi kaikissa tutkimuksissa pyritään arvioimaan tehdyn tutkimuksen kautta luotettavuutta. Tutkimuksen reliabiliteetti (luotettavuus) tarkoittaa mittaustulosten toistettavuutta ja validiteetti (pätevyys) tarkoittaa mittarin tai tutkimusmenetelmän kykyä mitata juuri sitä, mitä on tarkoituskin mitata.

Tässä tutkimuksessa on muutamia tekijöitä, jotka vaikeuttavat tutkimuksen luotettavuuden ja pätevyyden arviointia.

Ensinnäkin kvalitatiivinen tutkimus itsessään on aina ainutkertainen ja sen muotoutuminen kirjalliseksi tuotokseksi poikkeaa Hirsjärvenkin (2018, 266) mukaan melkoisesti teoriapohjaisen tutkimusselosteen yleisestä kaavasta (Eskola & Suoranta 1996). Laadullisen tutkimuksen kirjallista kuvausta on sanottu ”juoneltaan eteneväksi kertomukseksi” (Alasuutari 2007) ja kuvastaa sellaisena laadullisen tutkimusprosessin todellista kulkua tarkemmin kuin perinteinen tutkimusseloste. Kirjoittajan mielestä on vaikea reliabiliteetti -periaatteen mukaisesti toistaa tutkimusta organisaatiossa, joka on jatkuvasti muuttuva ja kehittää toimintaansa esille nousseiden havaintojen (kuten tämä tutkimus tai strategiset ja operatiiviset muutokset organisaatiossa) mukaan.

Toiseksi tutkimusmenetelmien valinnat on tehty siten, että kirjoittaja on harkinnut, mitkä olisivat mahdollisimman monipuoliset lähteet turvallisuuden johtamisen kehittämisen arviointiin. Turvallisuuteen liittyvää kirjallista aineistoa on yleisesti ottaen paljon ja jopa runsauden pulasta kärsien. Tietoperusta perustuu turvallisuutta ja riskienhallintaa käsittelevään kirjalliseen aineistoon ja erityisesti valtiohallinnon ohjeisiin ja määräyksiin, joten kokonaisuutena katsoen tietoperusta on luotettavuuden kannalta riittävä ja kattava, mutta kirjoittaja on joutunut tekemään valintoja kirjallisuuden suhteen ja joutunut jättämään pois paljon mielenkiintoista lähdekirjallisuutta. Kirjoittaja on pyrkinyt valitsemaan parhaita ja perustanut teoriansa standardeihin, jotka ovat pitkän kehitystyön tuloksia ja maailmanlaajuisesti hyväksyttyjä, luotettavia lähteitä.

Kolmanneksi kohdeorganisaation materiaali on hajallaan intranetissa (Terho) ja Terhon hakuominaisuudet ovat heikohkot. Organisaation siilomaisuudesta johtuen myös turvallisuuteen liittyvä materiaali on hajallaan eri paikoissa Terhoa, eikä kirjoittajalla ole täyttä varmuutta siitä, että kaikki materiaali mitä olisi tarvittu kohdeorganisaation kehittämisen perustaksi, on saavutettu ja käytetty. Kirjoittaja on kuitenkin keskittynyt uusimpaan materiaaliin ja siten, mahdollisimman ajantasaiseen ja myös haastateltavia saatujen vinkkien perusteella vahva usko on, että kaikki olennainen materiaali on saatu käyttöön, jotta tutkimuksen tuloksien luotettavuus on saavutettu.

Neljänneksi haastattelut osuivat poikkeukselliseen aikaan. Koronakevät ja -kesä 2020 on erityisesti Terveyden ja hyvinvoinnin laitoksella ollut ja on edelleen ajanjakso, jolloin turvallisuudesta vastaavat ihmiset ovat vaikeasti tavoitettavia ja haastattelujen saaminen ei ole ollut yksinkertaista. Haastattelukutsu lähetettiin kuudelle henkilölle, joista kolmea pääsin haastattelemaan. Teemahaastattelujen myötä on kuitenkin selvinnyt keskeiset tekijät, joilla on vaikutusta turvallisuusjohtamisen kehittämiseen ja kun teemahaastattelun luonteeseen kuuluu, että teemoja voidaan syventää ja suuntaakin muuttaa haastattelun kuluessa tai haastateltavan osaamisalueen mukaan, on kirjoittaja kokenut, että haastateltavista on saatu esille juuri oikeita asioita. Siihen on auttanut se, että kirjoittaja työskentelee kohdeorganisaatiossa ja tuntee ennalta haastateltavien osaamisalueen ja kykenee sitä kautta säätämään teemahaastattelun kulkua niin, että kyseisen haastateltavan kanssa käydään läpi kaikki teemat, mutta keskitytään haastateltavan omaan erityisosaamiseen. Tämä on teemahaastattelun rikkaus ja yksi valintaperusta juuri tälle menetelmälle. Hirsjärvikin toteaa (2018, 181), että aineiston suuruuden päättäminen on yhtä ongelmallista sekä kvantitatiivisessa että kvalitatiivisessa tutkimuksessa. Aineistona voi olla vaikkapa vai yksi tapaus tai yhden henkilön haastattelu. Toisaalta aineisto voi käsittää joukon yksilöhaastatteluja. Koska tarkoituksena ei ole etsiä keskimääräisiä yhteyksiä eikä tilastollisia säännönmukaisuuksia, aineiston koko ei määräydy näiden perusteella.

Tutkimuksen luotettavuudesta ja pätevyydestä voidaan todeta, että tutkimuksen motiivina olleet aikaisemmat tutkimukset (Virta 2014; Jämsen 2017) ovat huolellisesti laadittuja ja niiden tekijät ovat myös olleet kohdeorganisaatiossa työntekijöinä ja antavat siten luotettavan kuvan sen hetkisestä riskienhallinnan käytännön toteutuksesta ja pohjaa turvallisuusjohtamisen kehittämiselle. Aikaisemmat tutkimukset yhdistettynä tässä tutkimuksessa käytettyihin menetelmiin ja tietoperustaan yhdessä sisäisen materiaalin ja turvallisuusasiantuntijoiden haastattelujen kanssa antaa pohjan luotettavalle kvalitatiiviselle tutkimukselle ja vahvan uskon siitä, että kirjoittaja on onnistunut nostamaan esiin oikeita asioita, jotta Terveyden ja hyvinvoinnin laitoksen turvallisuusjohtamista voidaan kehittää siten, että se saavuttaa strategiset ja operatiiviset tavoitteet.

6 Pohdinta

Hirsjärven ym. mukaan (2018, 221, 229) kerätyn aineiston analyysi, tulkinta ja johtopäätösten teko on tutkimuksen ydinasia. Se on tärkeä vaihe, johon tähdättiin tutkimuksen aloittamisesta lähtien. Tutkimus ei ole valmis vielä silloin, kun tulokset on analysoitu, eikä tuloksia pidä jättää lukijan eteen jakaumina ja korrelaatioina vaan niitä on selitettävä ja tulkittava.

Tästä näkökulmasta katsoen kirjoittaja perustaa johtopäätökset neljään eri tekijään:

1. Tietoperustan kautta esille tulleisiin riskienhallinnan, valmiussuunnittelun ja turvallisuusjohtamisen periaatteisiin, joita noudattamalla organisaatio käsittelee riskejä ja ottaa ne huomioon turvallisuuden johtamisessa.
2. Turvallisuuteen ja riskienhallintaan liittyviin tutkimuksiin, jotka ovat aikaisemmin tehty Terveyden ja hyvinvoinnin laitoksella (Virta 2014, Jämsen 2017) ja jotka tukevat tämän tutkimuksen johtoajatusta siitä, että turvallisuuden tehokas ja tarkoituksenmukainen johtaminen vaatii selkeä turvallisuusjohtamismallin, joka perustuu riskienhallintaan, on sidottu johtamisjärjestelmään ja saa tarkoituksensa strategiasta
3. Terveyden ja hyvinvoinnin laitoksessa noudatettavaan lainsäädäntöön, sopimuksiin, ohjeisiin, toimintamalleihin, työryhmien muistiohin, käytänteisiin ja turvallisuuteen liittyvään dokumentaatioon, joka pääosin on saatavilla intranetissa.
4. Teemahaastatteluihin, joissa on haastateltu kolmea turvallisuusasiantuntijaa kymmenen eri teeman ympärillä.

Terveyden ja hyvinvoinnin laitoksen turvallisuuden johtaminen perustuu työjärjestykseen ja sen liitteisiin, strategiaan, sisäisiin ohjeisiin, riskienhallintapolitiikkaan, tietoturvapolitiikkaan, turvallisuusryhmän kokouskäytäntöihin, sisäisten asiantuntijoiden muodostamiin ryhmiin sekä STM:n tulossopimukseen. Näiden lisäksi osastoilla tehdään turvallisuuteen liittyvää suunnittelua, arviointia ja raportointia.

Turvallisuuden strateginen ja operatiivinen johtaminen on käytännössä turvallisuusryhmän vastuulla ja ryhmä pitääkin yllä turvallisuuden tilannekuvaa kokoontumalla 5-6 kertaa vuodessa ja raportoimalla riskienhallinnan tilanteesta ja turvallisuuden eri osa-alueiden tilanteesta koko ryhmälle. Turvallisuusryhmän kokousmuistiot ovat avoimesti saatavilla koko Terveyden ja hyvinvoinnin henkilökunnalle intranetissa. Turvallisuusryhmää johtaa palvelujohtaja, jonka alaisuudessa toimivat turvallisuuspäällikkö ja tietoturvapäällikkö. Työsuojelupäällikkö, tietosuojavastaava, valmiuspäällikkö ja laatupäällikkö toimivat muiden alaisuudessa. Terveyden ja hyvinvoinnin laitos on päällikkövirasto, mikä tarkoittaa, että päätöksenteko tapahtuu linjaorganisaation mukaisesti työjärjestyksessä ja sen liitteissä määritellyllä tavalla. Turvallisuusryhmällä on määräysvaltaa linjaorganisaation mukaisesti niissä osastoissa, joissa turvallisuusryhmän jäsen organisaatiossa toimii. Turvallisuusryhmä voi antaa suosituksia ja ohjeita turvallisuuteen liittyvissä asioissa, mutta suoranaiset käskyt tai toimintamallit tulevat osastojen johdon kautta. Asioista tehdään ratkaisut pääasiassa esittelyjen kautta. Turvallisuudesta vastuussa olevat henkilöt, joiden nimikkeessä on ”turvallisuus” kuten turvallisuuspäällikkö tai tietoturva(llisuus)päällikkö toimivat organisaatiossa neuvoa antavassa roolissa ja osittain toimintaa valvovassa roolissa. Direktio-oikeutta heillä ei ole, mutta he voivat jossain määrin määrätä työskentelystä turvallisuusvelvoitteisiin vedoten ja pääjohtajan päätöksellä työjärjestyksen liitteen neljä (THL työjärjestys 2020 erityistehtävät) mukaisesti. Vastuu toimenpiteiden toteuttamisesta jää linjaorganisaatiolle.

Terveyden ja hyvinvoinnin laitoksen siilomainen organisaatiorakenne tuo haasteita turvallisuuden johtamiselle. Turvallisuusryhmä on kokonaisturvallisuuden kannalta haastava kokonaisuus ja siihen valitut henkilöt edustavat turvallisuuden eri osaamisen alueita, joten lähtökohtaisesti se mahdollistaa informaation välittämisen sekä turvallisuusryhmästä osastoille, että päinvastoin. Taulukosta 7 nähdään kuitenkin, että hallinto- ja kehittäminen -osasto on vahvasti edustettuna (5/8 turvallisuusasiantuntijaa) turvallisuusryhmässä ja muiden osastojen edustus on vähäisempää tai sitä ei ole. Terveyden ja hyvinvoinnin laitoksen valmiusryhmässä on edustettuna turvallisuusasiantuntijan roolissa valmiuspäällikkö, turvallisuuspäällikkö, tietoturvapäällikkö ja palvelujohtaja sekä yksiköiden päälliköt ja Terveysturvallisuusosaston johtaja ja asiantuntijalääkäri. Tässäkin ryhmässä vahva edustus on hallinto ja kehittäminen osaston tukipalvelut -yksikössä, josta tulevat kaikki turvallisuuden asiantuntijat. Tukipalvelut -yksikkö käytännössä vastaa yksin Terveyden ja hyvinvoinnin laitoksen operatiivisesta turvallisuudesta ja muiden yksiköiden osalle tietoisuus turvallisuusasioista tulevat johtoryhmän ja viestinnän kautta. Jämsen (2017, 27) on todennut tutkielmassaan, että turvallisuusryhmän jäsenille pitäisi selkeämmin määritellä toimintatavat, resurssit, roolit sekä raportointikäytännöt suhteessa muuhun organisaatioon ja johtamisjärjestelmään. Erityisesti raportointikäytäntöjen kehittäminen mahdollistaisi asiantuntemuksen viemisen yhden osaston yhdestä yksiköstä koko Terveyden ja hyvinvoinnin laitoksen henkilöstölle.

Terveyden ja hyvinvoinnin laitoksella on johtoryhmä, johon työjärjestyksen (THL työjärjestys 2020 organisaatio) mukaan kuuluu pääjohtaja, tietoylijohtaja, tiedonhallintajohtaja, hallinto- ja talousjohtaja, viestintäjohtaja ja osastojen johtajat. Johtoryhmä huolehtii laitoksen kokonaisvaltaisesta kehittämisestä sekä toiminnan, talouden ja henkilöstöjohtamisen yhteensovittamisesta. Johtoryhmä luo myös edellytykset strategian toteuttamiselle ja seuraa järjestelmällisesti tavoitteiden toteuttamista. Hallinto- ja talousjohtaja johtaa hallinto ja kehittäminen -osastoa ja on siten linkki hallinto- ja kehittämisosaston ja johtoryhmän välillä. Jämsenin tutkielmassa (2017, 26) haastatellut kokivat, ettei turvallisuusjohtamisjärjestelmä ole kovin hyvin yhteydessä organisaation yleiseen johtamisjärjestelmään ja nytkin voidaan todeta, että turvallisuusjohtamisen kytkeytyminen organisaation johtamisjärjestelmään on ehkä liian ohut ja vaarana on, että se ei nouse riittävästi esille silloinkaan, kun se tarve on ilmeinen. Turvallisuusasiat saattavat jäädä muiden asioiden taakse johtoryhmässä.

Turvallisuuteen ja riskienhallintaan liittyvän materiaalien saatavuudella helposti ja nopeasti (esim. Ilmonen ym. 2016, 88) on turvallisuustietoisuuden ja sitä kautta turvallisuuskulttuurin syntymisen kannalta olennainen rooli. Lisäksi tarvitaan tilannekohtaista turvallisuusviestintää, jolla välitetään oikea-aikaista ja oikeantasoista informaatiota sellaisessa muodossa, että organisaation jäsenten ymmärrys turvallisuusasioissa ja niihin liittyvissä vastuissa tulee kaikille selväksi. Viestinnän haasteet Terveyden ja hyvinvoinnin laitoksessa kiteytyvät viestintäkanavaan. Terho-intranet on sekava ja sillä hakujen tekeminen tuottaa heikosti oikeita tuloksia. Siilomaisesta organisaatiosta johtuen turvallisuusasioiden keskittäminen yhteen paikkaan on haasteellista. Osa turvallisuuden osa-alueista kuten tietoturvallisuus, tilaturvallisuus ja työturvallisuus on siinä onnistunut ja näiden osalta turvallisuuteen liittyvät asiat löytyvät yhdeltä sivustolta, mutta ajankohtaisten asioiden viestinnässä tämä onnistuminen rapautuu. Ajankohtaiset asiat nousevat Terhon etusivulle, mutta nopeasti hukkuvat muiden asioiden joukkoon, koska viestintää on paljon ja viestien priorisointiin on vain vähän keinoja. Viesti voidaan nostaa joksikin aikaa muiden yläpuolelle, mutta tämän priorisoinnin voi kuka tahansa poistaa. Terhon viestintäongelmat ovat tiedossa ja niihin toivottavasti puututaan. Turvallisuusviestinnän osuus turvallisuuden johtamisessa on kiistaton ja turvallisuusviestintä vaatii ehdottomasti kehittämistä.

Turvallisuus pitäisi nähdä myös positiivisena asiana. Se mahdollistaa strategiaan perustuvat toiminnot ilman, että organisaation ihmiset, maine, tieto, ympäristö tai omaisuus on vaarassa. Turvallisuudesta pitäisi myös kertoa positiivisesti ja tuoda esille hyviä esimerkkejä ja käytänteitä niin valtiohallinnosta yleensä kuin erityisesti Terveyden ja hyvinvoinnin laitoksesta.

Riskienhallintaa tehdään Granite -riskienhallintajärjestelmän kautta (esitelty kappaleessa 4.1). Haastatteluissa kävi ilmi, että Graniten käyttöönottoa ei ole viety loppuun saakka.

Granitea ollaan kuitenkin kehittämässä ja sille on tehty kehittämissuunnitelma, jonka avulla Granite on tarkoitus uudistaa vielä vuoden 2020 aikana.

Granitessa on kaksi riskikategoriaa: työturvallisuusriskit ja strategiset riskit. Granitessa käsitellään riskejä, mutta turvallisuushavainnot kirjataan Terhoon, vaikka Granitessa on turvallisuushavainnoille oma moduuli, samoin kuin auditoinneille, jotka myös tehdään Graniten ulkopuolella. Graniten käyttö ja tunnettuus on myös jäänyt hieman hämäräksi. Työturvallisuus puolella on kuitenkin saatu hyviä kokemuksia, kun riskienhallinnasta Graniten avulla on kerrottu esimiehille. Työturvallisuuteen liittyvät riskit luokitellaan 3x3 matriisilla, kun taas strategiset riskit 5x5 matriisilla. Muitakin riskilajeja olisi hyvä Granitessa ottaa käyttöön kuten tieto(turvallisuus)riskit, ympäristöriskit, operatiiviset riskit. Eräs haastateltava toi esille, että henkilöstön osaamiseen liittyviä riskejä mietitään koko Terveyden ja hyvinvoinnin laitoksen tasolla, mutta työturvallisuusriskejä osastokohtaisesti. Kaivattiin jonkinlaista harmonisointia riskien käsittelyyn ja Graniten kehittämistä siten, että se vastaisi paremmin Terveyden ja hyvinvoinnin laitoksen tarpeeseen johtamisen välineenä.
Riskienhallinnan kypsyystasosta Ilmonen ym. (2016, 59-61) toteaa, että kypsyystasoja on viisi, joista alin on, että huolehditaan vakuutuksista ja riskeistä keskustellaan lähinnä vakuutusyhtiön tuotteiden kautta. Toisella tasolla (tai vaiheessa) yrityksen johto tiedostaa tarpeen koordinoida kattavasti riskienhallintaa ja laaditaan riskienhallintapolitiikat ja -ohjeistukset ja tunnistetaan asiantuntijoiden ja yksiköiden johtajien tarve periaatteiden mukaisten tehtävien hoitamiseen. Kolmannella tasolla riskienhallinnalla alkaa olla liiketoimintaa neuvova rooli. Riskienhallinta on osa päätöksen tekoa ja se saatetaan sijoittaa suoraan toimitusjohtajan tai pääjohtajan alaisuuteen. Tällä tasolla myös yleensä perustetaan muita turvallisuusjohtamiseen liittyviä osastoja kuten tietoturvaosasto tai työturvallisuusosasta. Myös prosessityöhön kyetään liittämään riskien tunnistamista ja kontrollien laatimista. Neljännellä tasolla riskienhallinta integroidaan vahvasti toiminnan suunnitteluun ja riskienhallintatyöstä on tullut ennaltaehkäisevää. Riskiarviointeja liitetään osaksi strategiaprosesseja ja toiminnan suunnittelua, mutta niillä ei ehkä vielä ole toimintaa ohjaavaa vaikutusta. Kontrollien toteuttaminen ja sisäisen valvonnan tarkastukset ovat organisaation operatiivisesta toiminnasta riippumattomia. Viidennellä tasolla riskienhallinta on integroitu johtamiseen ja riskienhallinta tukee tavoitteiden saavuttamista. Riskienhallinnan negatiivinen sävy on muuttunut positiivisten mahdollisuuksien havaitsemiseksi ja riskienhallintaa kehitetään jatkuvasti toiminnan muutosten mukana. Tätä tukee parhaiten jatkuvasti kehittyvä ja ajantasainen riskienhallintajärjestelmä, joka on integroitu johtamisjärjestelmään. Todettakoon, että Terveyden ja hyvinvoinnin laitoksen riskienhallinnan kypsyystasoa ei ole määritelty ja kehittämiskohteena voisikin olla sen tekeminen ja kehittämispolun määritteleminen nykytilanteesta ylimmälle tasolle.

Haastatteluissa tuli ilmi myös yhteisen työpaikan (Työturvallisuuskeskus 2020b) käsite, joka liittyy tässä tapauksessa valtiohallinnon yhteiseen käsitykseen työturvallisuudesta. Yhteisen työpaikan määritelmä kuvataan työturvallisuuslaissa. Asiaa on käsitelty yhdessä

turvallisuusryhmän kokouksessa vuoden 2020 aikana ja Terveyden ja hyvinvoinnin laitoksella se tarkoittaa, että pitäisi luoda yhteiset työturvallisuuden, perehdyttämisen, turvallisuushavaintojen ja harjoittelun pelisäännöt kaikkien niiden toimijoiden kanssa, jotka toimivat Terveyden ja hyvinvoinnin tiloissa, joita ovat Valtori, Lassila&Tikanoja, ISS ja Leijona Catering. Osittain yhteisiä tiloja on myös lääkealan turvallisuus- ja kehittämiskeskus Fimean kanssa. Työterveyslaitoksen mukaan (TTL 2020) yhteisten työpaikkojen ongelmien perimmäinen syy on tutkimuksen mukaan se, että sen toimintalogiikkaan ei ole täysin ymmärretty. Ihmiset ovat tottuneet ylhäältä alas ohjautuvaan hierarkkiseen toiminta- ja johtamisen malliin ja tämä malli ei yhteisillä työpaikoilla päde. Uuden logiikan mukainen toiminta haastaa ja jopa pakottaa ylittämään ja rikkomaan perinteisiä toiminnan rajoja ja johtamisen tapoja. Turvallisuusjohtamisella on yhteisen työpaikan pelisääntöjen luomisella olennainen rooli ja yhteisellä työpaikalla pitää kiinnittää enemmän huomiota kommunikointiin, perehdyttämiseen ja eri osapuolten vastuiden ja velvollisuuksien selkeyttämiseen.

Terveyden ja hyvinvoinnin laitoksen riskienhallinta ja turvallisuuden näkyminen organisaation jäsenille näyttää haastattelujen ja olemassa olevan materiaalin perusteella painottuvan vahvasti negatiivisiin asioihin. Turvallisuudella on kuitenkin myös se positiivisempi puoli ja turvallisuus pitäisi nähdä positiivisena ja tekemistä mahdollistavana asiana, kuten kypsyystaso arviossakin (Ilmonen ym. 2016, 61) tasolla viisi havaitaan. Turvallisuuden johtaminen ja johtamiseen integroitu riskienhallinta mahdollistavat strategiaan perustuvat toiminnot ilman, että organisaation ihmiset, maine, tieto, ympäristö tai omaisuus on vaarassa. Turvallisuudesta pitäisi myös kertoa positiivisesti ja tuoda esille hyviä esimerkkejä ja käytänteitä niin valtiohallinnosta yleensä kuin erityisesti Terveyden ja hyvinvoinnin laitoksesta.

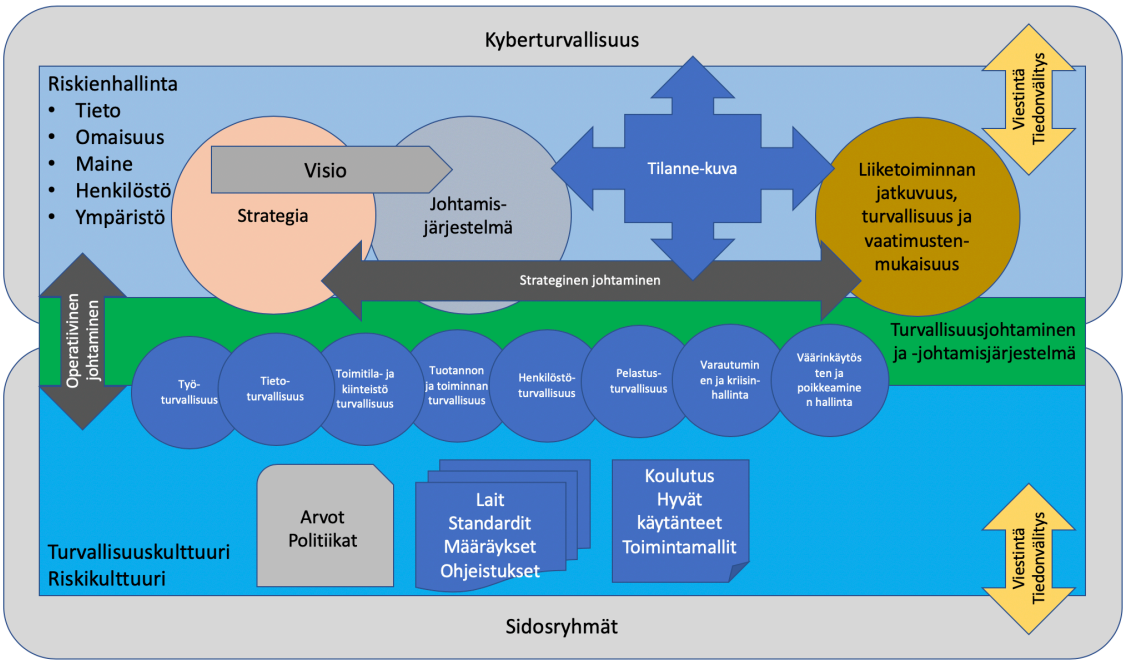
Johtopäätöksenä turvallisuuden johtamisjärjestelmästä Terveyden ja hyvinvoinnin laitoksella voidaan todeta, että riskienhallintaa perustuva turvallisuuden johtaminen on hyvin viestitty ja omaksuttu ohjeistuksessa ja riskienhallintapolitiikkaa laadittaessa. Riskienhallintapolitiikassa on selkeät ja kattavat tavoitteet ja ne on ymmärrettävästi kirjattu, samoin kun viestinnän merkitystä on korostettu. Haastatteluissa on kuitenkin tullut ilmi, että ohjeiden sisäistäminen ja politiikan jalkauttaminen ei ole aivan yhtä selkeää ja että riskienhallinnan näkyvyys, riskeistä viestintä ja henkilöstön osallistaminen ei ole mennyt läpi organisaation. Tämä vaatisi erillisen kvantitatiivisen tutkimuksen siitä, kuinka laajasti nämä periaatteet ja käytännöt on omaksuttu koko laitoksessa ja voisi olla yksi jatkokehityskohde.

7 Turvallisuuden johtamisen kehittämisen mallit Terveyden ja hyvinvoinnin laitoksella

Kehittämisehdotukset perustuvat sekä tämän tutkimuksen ja haastattelujen kautta esille tulleisiin seikkoihin, että Jämsenin (2017) tutkielmassa nostamiin kehittämisehdotuksiin, koskien erityisesti turvallisuuden johtamisen kehittämistä. Jämsenin tutkimus on melko tuore ja siinä

esitettyjä kehittämisehdotuksia ei ole ainakaan kaikilta osin otettu käyttöön ja siksi ne on hyvä tuoda esille siltä osin, kun ne tukevat tässä tutkimuksessa esille nousseita havaintoja, joissa kehittämiskohteet tukevat tämän hetken Terveyden ja hyvinvoinnin laitoksen strategisen ja operatiivisen turvallisuusjohtamisen tarvetta. Haastatteluissa kävi ilmi, että Virran (2014) tekemän tutkielman esiin nostamat kehittämiskohteet ovat suurelta osin otettu käyttöön riskienhallintajärjestelmän (Granite) käyttöönoton myötä, mutta senkin kohdalla on edelleen kehitettävää.

Yhteenvetona voidaan todeta, että turvallisuuden johtamisen tulee olla kokonaisvaltaista, arvioida positiivisia ja negatiivisia epävarmuuden vaikutuksia tavoitteisiin riskienhallinnan periaatteilla, olla johdon tukemaa, perustua strategiaan, olla osa johtamisjärjestelmää ja toteuttaa tietoon perustuvana operatiivisena johtamisena toiminnan kaikilla tasoilla ja tähdätä koko henkilöstöön ja sidosryhmiin vaikuttavaan turvallisuuskulttuuriin, jossa huomioidaan sekä fyysisen, että digitaalisen maailman uhat ja näiden yhteisvaikutukset organisaation päätöksentekoon ja johtamiseen turvallisuuden kaikilla osa-alueilla.



Kuvio 23: Kokonaisvaltaisen turvallisuuden johtamisen malli.

Edellä esitetty kuvio (kuvio 23), joka on esitelty kohdassa 3.1 Kokonaisvaltaisen turvallisuuden johtamisen malli, sisältää kokonaisuuden, johon Terveyden ja hyvinvoinnin laitoksen turvallisuuden johtamisen tulisi perustua. Tätä kuviota (kuvio 23) yhdessä kuvion 24 kanssa voidaan pitää tämän tutkimuksen kokoavina päätuloksina, joiden perusteella Terveyden ja hyvinvoinnin laitoksen turvallisuuden ja riskienhallinnan johtamista voidaan toteuttaa ja edelleen kehittää.

Riskienhallinnan kehittäminen sekä toimenpiteiden, että riskienhallintajärjestelmän osalta vahvistaisi perustaa turvallisuuden johtamiselle. Keskellä on vihreä palkki, joka kuvastaa turvallisuusjohtamista ja turvallisuusjohtamisjärjestelmää ja jolla on yhtymäkohta operatiiviseen johtamiseen turvallisuuden osa-alueiden (EK yritysturvallisuus 2016) kautta. Operatiivinen johtaminen on yhtymäkohta johtamisen (vaalean sininen alue) ja henkilöstön toimintaympäristön (tumman sininen alue) välillä. Turvallisuuden osa-alueiden vastuut, henkilöstö, resurssit, toimintasuunnitelmat ja budjetti on määritelty ja dokumentoitu. Turvallisuuden johtaminen perustuu organisaation strategiaan, jakaa yhteisen vision ja on integroitu johtamisjärjestelmään. Johtamisjärjestelmä saa jatkuvasti tilannekuvan päivitystä eri suunnista, kuten kyberturvallisuuden kokonaisuudesta, teknisistä lähteistä, sidosryhmiltä ja kansalliselta ja kansainvälisiltä yhteistyökumppaneilta. Johtamisen kokonaisuuden takana on riskienhallinta, jolla suojataan organisaation tietoa, omaisuutta, mainetta, henkilöstöä ja ympäristöä. Strateginen johtaminen kokoaa yhteen kokonaisvaltaisen johtamisen tekijät normaalioloissa ja hyödyntää jatkuvuuden hallinnan suunnitelmia normaaliolojen häiriötilanteessa ja poikkeusoloissa niin, että Terveyden ja hyvinvoinnin laitoksen toiminnan jatkuvuus, turvallisuus ja vaatimustenmukaisuus on taattu. Johdon esimerkillä ja henkilöstön ohjeistuksella, koulutuksella, hyvillä käytänteillä ja toimintamalleilla kehitetään Terveyden ja hyvinvoinnin laitoksen turvallisuuskulttuuria ja riskikulttuuria, joka vastaa organisaation arvoja ja perustuu politiikkoihin. Viestinnällä ja tiedonvaihdolla ollaan yhteydessä sidosryhmiin sekä annetaan ja saadaan informaatiota bittien ja atomien yhdistämästä maailmasta eli kyberturvallisuusympäristöstä.

Turvallisuuden ja riskienhallinnan ohjausryhmä säästäisi toimivan johdon aikaa. Käytännössä harvoin on riittävästi aikaa ja tilaa organisaation johtoryhmän agendalla käsitellä riskienhallintaan ja kokonaisturvallisuuden johtamiseen liittyviä asioita. Ratkaisuna olisi turvallisuuden ja riskienhallinnan ohjausryhmä, jossa on mahdollisuus keskittyä tehokkaasti juuri näihin asioihin. Ohjausryhmässä tulisi olla edustettuna organisaation ylimmästä johdosta edustaja (esimerkiksi talous- ja hallintojohtaja), osastojen edustajat sekä turvallisuudesta vastaavat tahot, sitten että ohjausryhmän koko olisi kohtuullinen. Tämä olisi asiantuntija foorumi, joka käsittelisi koko viraston tasoisia riskejä sekä antaisi ohjeita, määräyksiä ja suosituksia turvallisuuden parantamiseksi virastossa. Ohjausryhmä myös asettaisi tavoitteet riskienhallinnalle ja turvallisuustyölle. Ohjausryhmän agendalla olisi esimerkiksi riskikarttojen ja -raporttien käsittely sekä niihin liittyviä riskienhallinta- ja turvallisuustoimia.

Ilmonen ym. (2016, 50-51) esittelee riskienhallinnan kolmen puolustuslinjan mallin, jonka avulla organisaation on helpompi ymmärtää vastuut ja velvoitteet riskienhallinnan toteuttamisessa ja valvonnassa. Malli on suoraan sovellettavissa turvallisuuden johtamiseen, koska riskienhallinta muodostaa sille perustan. Ensimmäinen puolustuslinja muodostuu Terveyden ja hyvinvoinnin laitoksen osastojen riskienhallinnasta operatiivisessa toiminnassa. Jokaisella osastolla tulisi olla nimetty riskivastaava, jonka tehtävänä on sekä kerätä osastoilla ilmenneitä riskejä ja koostaa niistä raportti turvallisuusjohdolle, että toimia viestin viejänä

osastoille turvallisuusjohdolta saamiensa tehtävien mukaisesti. Samat asiat viestitettäisiin sisäisissä kanavissa, mutta varmistettaisiin viestin perillemeno myös osastokohtaisen riskivastaavan tai turvallisuusvastaavan kautta. Osastolla ja näiden johtajilla on oikeus riskinottoon ja se omistaa riskin ja vastaa sen hallinnasta, silloin kun muutenkin vastaa riskiin liittyvästä tuloksesta, tavoitteesta, prosessista, tuotteesta tai muusta organisaation vastuulla olevasta toiminnasta. Kuitenkin toisen puolustuslinjan tehtävä on antaa neuvoja, miten riskienhallinta käytännössä toteutetaan. Ensimmäinen puolustuslinja raportoi riskeistään turvallisuusjohdolle tai tarvittaessa linjaorganisaatiossa ylöspäin.

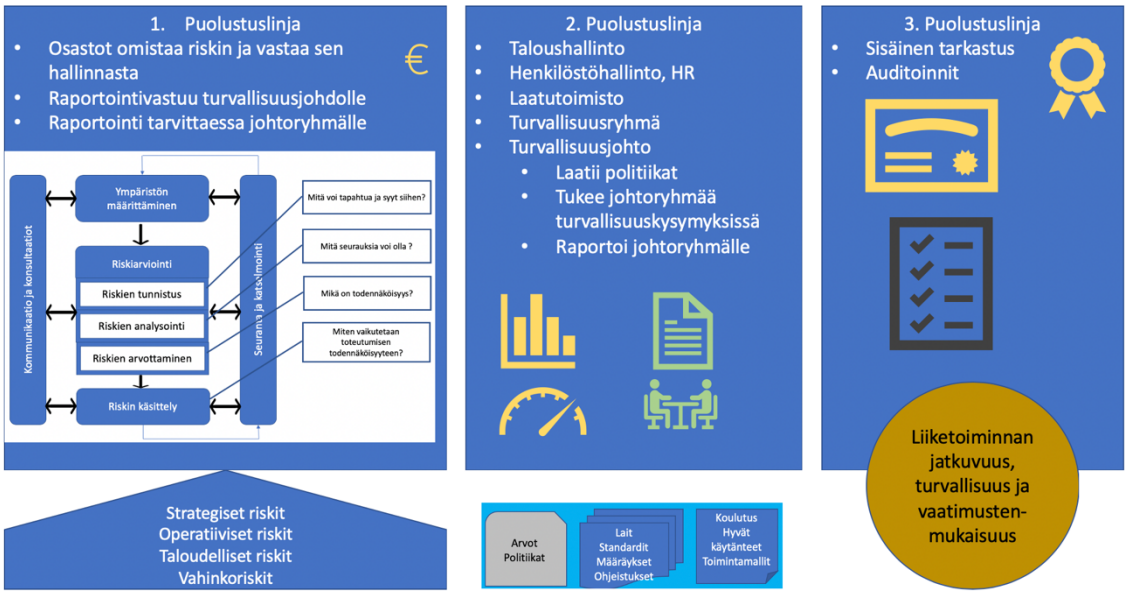
Toisessa puolustuslinjassa toimii esim. taloushallinto, turvallisuusorganisaatio ja laatutoimisto. Linjan tehtävä on tukea toimivaa johtoa koko organisaation laajuudessa ja kaikissa toiminnoissa omalla ammatillisella vastuualueellaan. Toisen linjan toiminnot ovat riippumattomia ensimmäisen linjan toiminnoista ja toisen linjan keskeinen tehtävä on riskiraportointi johdolle. Mikäli ensimmäisen linjan raportointi on laadukasta ja riittävää, voi toinen linja keskittyä valvonnan ja laadunhallinnan näkökulmaan.

Ensimmäisen ja toisen linjan työnjakoa voidaan havainnollistaa seuraavasti:

- Toinen linja valmistelee periaateasiakirjat, kuten riskienhallintapolitiikka, turvallisuuspolitiikka, tietoturvapolitiikka, laatupolitiikka, joiden mukaan ensimmäinen linja toimii
- Toinen linja määrittelee, miten riskejä tunnistetaan
- Ensimmäinen linja vastaa, että riskejä tunnistetaan ja kuvaa mitä riskejä on tunnistettu
- Ensimmäinen linja vastaa taloudellisen tuloksen raportoinnista
- Toinen linja raportoi ensimmäisen linjan kumulatiivisesti ottamat taloudelliset riskit.

Kolmas linja on sisäinen tarkastus, joka arvioi riskienhallinnan tehokkuutta ja toimivuutta ja huolehtii toiminnan auditoinneista. Suoritetut auditoinnit nostetaan esiin hyvinä esimerkkeinä onnistuneesta turvallisuustyöstä. Sisäisellä tarkastuksella on tärkeä rooli organisaation toiminnan jatkuvuuden, turvallisuuden ja vaatimustenmukaisuuden tarkastajana.

Seuraavassa kuvassa (Kuvio 24) tätä mallia on sovellettu Terveyden ja hyvinvoinnin laitokseen. Tätä kuviota voidaan kuvion 23 lisäksi pitää tämän tutkimuksen kokoavana päätuloksen, johon Terveyden ja hyvinvoinnin laitoksen riskienhallinnan tulisi perustua. Yhdessä nämä kuviot muodostavat kokonaisuuden, jonka varaan voidaan Terveyden ja hyvinvoinnin laitoksen turvallisuuden ja riskienhallinnan johtaminen ja kehittäminen perustaa.



Kuvio 24: Kolmen puolustuslinjan järjestelmä riskienhallinnassa ja turvallisuuden johtamisessa Terveyden ja hyvinvoinnin laitoksella. (Riskienhallinta kuvion lähteenä Nylander 2017, 144)

Kolmen puolustuslinjan järjestelmässä osastot ja niiden johto muodostaa ensimmäisen ja vastaa itse osastokohtaisesta riskinotosta (strategiset, taloudelliset, operatiiviset ja vahinkoriskit) ja riskienhallinnasta sekä raportoi niistä eteenpäin. Osastolla voi olla oma riskienhallintavastaava, mutta osaston johto vastaa kokonaisuudesta.
Toisen puolustuslinjan muodostaa Terveyden ja hyvinvoinnin laitoksen yhteiset palvelut eli taloushallinto, henkilöstöhallinto ja laadunhallinta sekä turvallisuusryhmä ja turvallisuusjohto. Näiden tehtävä on punnita ensimmäisen puolustuslinjan raporttien perusteella, minkälainen on riskikuva ja turvallisuuden tilannekuva ja raportoida siitä johdolle. Ilmosen ym. (2018, 202) mukaan johdon riskiraportointi voidaan jakaa esimerkiksi niin, että neljännesvuosittain raportoidaan merkittävämmät riskit ja mahdollisuudet ja kuukausiraportissa muutokset riskitasossa ja riskienhallintatoimissa. Lisäksi kannattaa raportointi jakaa ulkoiseen ja sisäiseen raportointiin, jossa ulkoisella tarkoitetaan sidosryhmille raportointia.
Kolmannessa linjassa sisäinen tarkastus tekee tarkastuksia ja arvioi riskienhallinnan tilannetta sekä mahdollisesti suorittaa auditointeja osastoille tarkastaakseen riskienhallinnan prosessin toimivuuden. Hyvät esimerkit turvallisuuden parantamiseksi nostetaan näkyviin esimerkiksi diplomien muodossa toimipisteen aulassa.

Oikein mitoitetulla ja oikea-aikaisella viestinnällä on turvallisuuden johtamisessa merkittävä osuus. Sisäisiä viestintäkanavia tulisi kehittää ja luoda viestinnälliset toimintamallit turvallisuusasioista viestimiseen ja kannustamiseen. Turvallisuusviestintä pitäisi olla kahdentasoista, toisaalta viestitään vaaroista ja uhkista ja toisaalta viestitään positiivisista turvallisuutta lisäävistä asioista ja teoista. Jokavuotiseen viestintäpalkintojen jakoon voisi lisätä kategorian, jossa palkitaan henkilöstön edustaja, joka on oman alansa asiantuntija turvallisuusasiantuntijoiden ulkopuolelta, turvallisuusasioiden edistämisestä viestinnällä ja näin kannustaa turvallisuuden positiiviseen viestintään.

Terveyden ja hyvinvoinnin laitos on tietotalo, mutta myös asiantuntijalaitos, jossa pelkkä tiedon tuottaminen ei riitä, vaan sitä pitää tulkita ja soveltaa. Tiedonhallinnan riskien havaitsemiseen ja tunnistamiseen pitäisi luoda omat teknologiset ja toiminnalliset periaatteet ja niiden priorisointi tulee nostaa korkealle tasolle. Havainnointikyvyn lisääminen tietoteknisessä ympäristössä yhdessä Valtorin toimijoiden kanssa toisi näkyvyyttä riskienhallinnan tueksi, samoin kuin teknisten raportointimenetelmien kehittäminen. Teknologian hyödyntäminen on tärkeää, mutta havainnointien tulkitseminen tulee viime kädessä olla ihmisten tekemään. Tämä taas vaatii sekä resursseja, että osaamista.

Turvallisuuden kokonaisvaltainen hallinta ja turvallisuuden osa-alueiden vastuiden määrittely pitäisi tarkentaa. Pitäisi lisätä ymmärrystä ja tehdä selkeitä suunnitelmia siitä mitä Terveyden ja hyvinvoinnin laitoksella tarkoitetaan esimerkiksi toimitilaturvallisuudella, ympäristöturvallisuudella tai väärinkäytösten ja poikkeamien hallinnalla ja millaisia organisaatio- ja osastokohtaisia toimenpideohjeita näille on luotu ja ketä niistä on vastuussa. Tähän voidaan soveltaa edellä esiteltyä kolmen puolustuslinjan menetelmää.

Terveyden ja hyvinvoinnin laitos on monimutkainen, perinteitä omaava ja haastava toimintaympäristö, jonka ihmiset, maine, ympäristö, omaisuus ja tieto tarvitsevat turvallisuuden johtamisen menetelmiä, käytänteitä, osaamista ja kyvykkyyksiä, joita parhaiten voidaan toteuttaa ammattimaisen turvallisuuden johtamisen avulla. Johdon tulisi miettiä päätoimisen turvallisuusjohtajan viran perustamista ja ottamista osaksi johtoryhmää. Se selkeyttäisi johtovastuita ja antaisi mahdollisuuden kehittää sekä Virran (2014, että Jämsenin (2017), kuten tämänkin työn esille nostamia turvallisuuden johtamisen osa-alueita niin turvallisuusasioiden laajentamiseksi osastoille, ihmisten turvallisuustietoisuuden lisäämistä kuin myös vastuiden määrittelyä ja valvontaa organisaation johdon tukena, joka antaisi pohjan vahvan turvallisuuskulttuurin kehittymiselle ja turvallisuusasioiden jatkuvalle parantamiselle.

8 Johtopäätökset

Tässä kappaleessa on kuvattu tutkimuksen tulosten suositukset, hyödyt ja jatkotutkimuksen mahdollisuudet.

8.1 Tiivistelmä suosituksista

Turvallisuuden johtamisen kehittäminen Terveyden ja hyvinvoinnin laitoksella on haasteellinen ja vaativa tehtävä monimuotoisen ja pitkän historian omaavan toimintaympäristön vuoksi. Vaativuutta lisää se, että osastot toimivat melko itsenäisesti ja niillä on omia toimintatapoja ja sääntöjä kehittynyt vuosien mittaan. Turvallisuuden johtaminen vaatii laajaa yhteistyötä niin Terveyden ja hyvinvoinnin laitoksen sisällä, kuin valtiohallinnossa kokonaisuutena. Se vaatii myös oikea-aikaista ja oikein mitoitettua viestintää käyttäen sellaisia kanavia, että kaikilla on mahdollisuus saada tietoa, ymmärtää oma yksilöllinen, yksikkökohtainen ja osastokohtainen vastuu ja kehittää omaa turvallisuusosaamistaan omassa työssään ja havaita oman työympäristön riskit ja tietää miten niistä raportoidaan. Esimiehillä on tässä tärkeä tehtävä mm. palautteen antajana ja tarvittaessa palkitsijana hyvästä turvallisuustyöstä, jotta organisaation turvallisuus nähdään positiivisen asiana ja turvallisuuskulttuurin kehittämiselle luodaan puitteet ja mahdollisuudet. Turvallisuus pitää tuoda esille positiivisena ja mahdollisuuksia tuovana asiana ja siitä kertominen tulisi kuulua jokaiseen henkilökuntatilaisuuteen. Riskienhallinnan ulottuvuutta pitää laajentaa ja ottaa hyviä malleja ja onnistumisia esimerkiksi työturvallisuuden puolelta, jossa riskienhallinnan kypsyystaso on hyvällä tasolla.

Tärkeintä turvallisuuden johtamiselle ja sen kehittämiselle on kuitenkin johdon sitoutuminen ja tuki. Johto seisoo turvallisuusjohtamisen päätösten ja menetelmien ja turvallisuusjohtajan takana ja antaa itse hyvän esimerkin turvallisuuden noudattamisesta kehittäen sitä kautta koko organisaation turvallisuuskulttuuria. Turvallisuudesta vastuussa olevien ei pitäisi olla yhden yksikön sisällä, vaan turvallisuuden vastuita pitäisi laajentaa koskemaan jokaista osastoa. Kaikkien osastojen edustajat käsittävä turvallisuuden johtoryhmä tai organisaation johtoryhmän tueksi perustettu turvallisuusjohdon tai riskienhallinnan ohjausryhmä tukisi johdon tarvetta kokonaisvaltaisen tilannekuvan muodostamiseen tiedolla johtamisen perustaksi ja turvallisuusviestinnän tarpeiden arvioimiseksi. Turvallisuus tulisi nostaa kirkkaammin esille ja miettiä myös palkitsemiskeinoja hyvästä turvallisuustyöstä.

Turvallisuuden johtamisen tulee perustua riskienhallinnan kautta saatuun ajantasaiseen tilannetietoon, kehittämiskohteiden tunnistamiseen, yhteistyöhön, hyvien käytänteiden ja esimerkkien hyödyntämiseen, viestintään ja osaaviin henkilöihin, joilla on kykyä ja taitoa viedä Terveyden ja hyvinvoinnin laitosta kohti turvallisempaa, hallittavampaa ja toimivampaa organisaatiota valtiohallinnon pelisäännöillä, mutta uusimpaan tietoon perustuvaan kokonaisvaltaisen turvallisuusjohtamisen opeilla. Turvallisuuden johtamiselle ja sen kehittämiselle on keskeistä johdon tuki, jonka pohjalta tulevaisuuden Terveyden ja hyvinvoinnin laitosta

rakennetaan ja kuten pääjohtaja virtuaalisessa aamukahvitilaisuudessa 12.8.2020 totesi, on muutoksen THL2021 tavoitteena uudistuva, ketterä ja monimuotoinen THL. Tätä muutosta ei voi tapahtua ilman, että kokonaisvaltainen riskienhallinta ja turvallisuuden johtaminen on integroitu johtamisjärjestelmään, on systemaattista, kaikki mukaanottavaa ja jatkuvasti kehittyvää.

8.2 Opinnäytetyön hyödyt

Tutkimuksen hyödyt konkretisoituvat laajan tietoperustan kautta saatuun käsitykseen turvallisuuden johtamisen perustasta. Riskienhallinnan ja turvallisuuden johtamisen yhteys on kiistaton. Organisaation täytyy ymmärtää toimintaansa kohdistuvat riskit ja kyetä hallinnoimaan niitä koko organisaation laajuisesti

Tutkimuksen kautta saatuja tuloksia ja tutkimuksessa kehitettyjä turvallisuuden ja riskienhallinnan johtamisen malleja voidaan soveltaa sekä yksityiseen, että julkishallinnon organisaatioon. Kuviot 23 ja 24 muodostavat yhdessä kattavan mallin riskienhallinnalle ja turvallisuuden johtamiselle. Niitä voidaan soveltaa kaikenkokoisiin organisaatioihin keskisuurista suuriin. Pienissäkin organisaatioissa voidaan näitä malleja pitää ohjeellisina ja ymmärtää mitkä kohdat kuvioista ovat toteutettavissa omassa organisaatiossa ja hyväksyä, että malleja ei ehkä voida kokonaisuutena implementoida, mutta niistä voidaan ottaa parhaiten omaan organisaatioon soveltuvat kohdat.

Mallit kattavat organisaation sekä vertikaalisesti, että horisontaalisesti. Elinkeinoelämän keskusliiton organisaatioturvallisuuden mallin kautta tulevat turvallisuuden osa-alueet muodostavat keskeisen elementin sille, että turvallisuuden johtaminen tulee kattaa koko organisaatio horisontaalisesti eli huomioida niin fyysinen turvallisuus, tietoturvallisuus tai väärinkäytösten ja poikkeamien hallinta kuin työturvallisuus ja henkilöstöturvallisuuskin sekä strategisessa johtamisessa, että operatiivisessa johtamisessa. Vertikaalinen kattavuus tulee johdon sitoutumisesta ja käyttäytymisestä niin, että turvallisuuden ja riskienhallinnan asia koetaan omaksi kaikella organisaation tasoilla ja niin että se luo pohjan turvallisuuskulttuurin syntymiselle ja kehittämiselle. Sidosryhmien mukaan ottaminen ja jatkuvuuden hallinnan periaatteiden ymmärtäminen kaikilla turvallisuuden osa-alueilla sekä atomien ja bittien rajapinnassa kyberturvallisuudessa, mahdollistaa kokonaisvaltaisen turvallisuuden johtamisen ottamisen osaksi organisaation johtamisjärjestelmää.

Tässä tutkimuksessa kehitetty kokonaisvaltaisen turvallisuuden johtamisen malli korostaa viestintää ja yhteistyötä. Sidosryhmien ja toisaalta kyberturvallisuuden kautta tulevan jatkuvuuden hallinnan välinen viestintä ja tiedonvaihto on jokaisen organisaation turvallisuuden johtamisen onnistumisen keskiössä. Verkottuneessa maailmassa ei kannata yrittää pärjätä yksin. Uhkatkin ovat useimmiten yhteisiä. Sidosryhmäyhteistyö, viestintä ja tiedonvaihto muodostaa osan, joka mahdollistaa parhaan saatavilla olevan tiedon perusteella tiedolla

johtamisen, jossa oikean tiedon saanti ja sen soveltaminen omaan organisaatioon säästää aikaa ja kustannuksia, mutta myös mahdollistaa oikea-aikaisen ja oikein mitoitetut toimenpiteet organisaation arvojen säilyttämiseksi.

Tutkimuksen hyödyt näkyvät myös turvallisuuskulttuurin ja riskikulttuurin muodostumisen elementteinä. Tässä tutkimuksessa on tuotu esille niitä tekijöitä, joiden avulla organisaation turvallisuuskulttuuri ja riskikulttuuri muodostuu. Monessa kohdassa korostuu johdon tuki ja esimerkki turvallisuustyölle. Sen lisäksi tarvitaan arvot ja visiot, joissa mukana tulee olla turvallisuus selkeästi ilmaistuna ja sitouttavana tekijänä. Turvallisuuskulttuurin perustan luodaan lakien, määräysten ja standardien implementoinnilla organisaation jokaiselle tasolle. Näiden yhdessä sovittujen arvojen ja visioiden sekä ”pakottavien” säädösten lisäksi tarvitaan pehmeitä keinoja, kuten koulutusta, hyviä käytänteitä ja toimintamalleja. Kun nämä elementit ovat organisaatiossa sisäistetty, saadaan koko henkilöstö ymmärtämään mistä tekijöistä turvallisuus muodostuu ja mikä on henkilökohtainen, yksikkökohtainen ja osastokohtainen tekijä sen muodostamisessa. Tästä kokonaisuudesta muodostuu organisaation turvallisuuskulttuuri ja riskikulttuuri.

Tutkimuksen tuloksena syntynyt kolmen puolustuslinjan järjestelmän soveltaminen Terveyden ja hyvinvoinnin laitokseen, mahdollistaa sen soveltamisen muihinkin organisaatioihin. Ensimmäisen puolustuslinjan riskienhallinta muodostaa rungon, jonka avulla riskit käsitellään siellä missä parhaiten tunnetaan substanssi. Osastoilla on oikeus ottaa riskejä ja velvollisuus hallinnoida niitä sekä raportoida niistä eteenpäin turvallisuusorganisaatiolle ja tarvittaessa organisaation johdolle. Jokaisessa organisaatiossa tulee esittää mallissa (kuvio 24) oleva riskienhallinnan kysymykset: mitä voi tapahtua ja miksi? mitä seurauksia tapahtumasta voi olla? mikä on todennäköisyys tälle tapahtumalle? miten vaikutetaan tapahtuman toteutumisen todennäköisyyteen? Tämä johdattaa riskienhallinnan ytimeen ja kun tämä tehdään kaikille riskilajeille, niin ollaan varmistettu riskienhallinnan ensimmäinen puolustuslinja. Jos organisaatio on sisäitänyt mallin, joka esitettiin kuviossa 23, on tämän kuvion 24 ensimmäisen puolustuslinjan avulla saavutettu organisaation turvallisuuden johtamisen hyvä kypsyystaso.

Viimeisenä voidaan todeta, että teknologiasta on suuri apu ja sitä tulee mahdollisimman paljon hyödyntää kaikissa vaiheissa turvallisuuden johtamisessa, mutta ihmisten mukaan saaminen, kaikilla organisaation tasoilla, on aivan välttämätöntä. Turvallisuuden johtaminen on suurelta osalta viestintää. Organisaatiossa työskentelevien ihmisten ja organisaatioon vaikuttavien ihmisten tulee tietää, miksi jotain tehdään, miten se tehdään ja mitkä ovat sen seuraukset. Käytännössä tämä on hyvin lähellä muutosjohtamista. Ilman selkeää, asianmukaista, oikea-aikaista ja oikean tasoista viestintää, ei ole mahdollista tehdä muutosta, kuten ei ole mahdollista rakentaa ympäristöä, jossa henkilöt tuntevat olonsa turvalliseksi ja tietävät mistä elementeistä se muodostuu ja mikä on oma rooli siinä. Jos tässä onnistuu, on onnistunut turvallisuuden johtamisessa.

8.3 Jatkotutkimusmahdollisuudet

Jatkotutkimuksen kohteita voisi olla ihmisten osallistamiseen liittyvät käytänteet ja konkreettiset toimenpiteet Terveyden ja hyvinvoinnin laitoksella. Näitä olisivat sellaiset kokonaisvaltaisen turvallisuuden jalkauttamiseen liittyvät projektit tai projektin omaiset toimenpiteet, joilla saadaan koko henkilöstölle tietoa heitä koskevista turvallisuusasioista, saadaan heiltä tietoa kaikkia koskevista turvallisuuteen vaikuttavista tapahtumista ja tekijöistä sekä saadaan heidät ymmärtämään miten voisi omassa työssään parantaa oman työnsä turvallisuutta sekä organisaation turvallisuutta ja sen kautta valtiohallinnon ja edelleen yhteiskunnan turvallisuutta. Kaikesta teknologiasta huolimatta, ihminen on edelleen turvallisuusketjussa se heikoin, mutta myös vahvin lenkki. Organisaation johdon tehtävä on mahdollistaa sellaiset olosuhteet, että jokainen kohta ketjussa on vahva, eikä heikkoja lenkkejä ole, eikä niiden syntymiseen ole kasvualustaa organisaation operatiivisessa toiminnassa.

Valmiusryhmän toiminnan kehittämiseen nousi tässä tutkimuksessa myös paineita, vaikka sen toimintaan oltiinkin lähtökohtaisesti tyytyväisiä. Erityisesti valmiustoimintaan liittyvä harjoittelu ja sitä kautta ryhmän toiminnan yhteensitominen koettiin kehittämiskohteiksi. Toisaalta olisi hyvä, että tarkastelu tehtäisiin toiminnan kehittämisen lisäksi tietoperustan kautta laajasti ja alan julkaisuihin, käytänteisiin ja toimintamalleihin perustuen, jotta ryhmän toimintaa voitaisiin uudistaa sekä sisäisen tarpeen, että ulkoisten vaatimusten ja esimerkkien kautta.

Kolmanneksi jatkokehittämisen kohteeksi nousi turvallisuusviestintä kaikissa eri muodoissa. Viestintäkanavien, viestintäkäytänteiden, viestintävälineiden, viestintätasojen, viestintävastuiden jne. muodostama kokonaisuus kaipaisi tutkimuksellista otetta ja kehittämistä. Voidaan kysyä voiko turvallisuusviestinnässä edes onnistua, kun muistetaan Wiion (esim. Wiio 1994) viestinnän lait, joista tunnetuin on, että ”viestintä yleensä epäonnistuu, paitsi sattumalta” ja toinen laki, jossa sanotaan, että ”joukkoviestinnässä ei ole tärkeintä se, miten asiat ovat, vaan miten asiat näyttävät olevan”. Turvallisuusviestintää siis kannattaa tutkia ja kehittää. Sen onnistuminen tai epäonnistuminen vaikuttaa niin käytökseen kuin asenteisiinkin.

Lähteet

Andersson, P. & Tikka, H. 1997. Mittaus- ja laatutekniikat. Porvoo: WSOY.

Beckford, J.1998. Quality, A critical introduction. London: Routledge.

BS 2011. British Standard BS 31100:2011.

Alasuutari, P. 2007. Laadullinen tutkimus. 6.painos (3. uud. p.). Vaajakoski: Vastapaino.

COSO-ERM 2017. Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management, Integrating with Strategy and Performance, Executive Summary.

EK yritysturvallisuus 2016. Elinkeinoelämän yritysturvallisuusmalli. Elinkeinoelämän keskusliitto. Helsinki: YTNK.

EK 2020. Työelämä, Yritysturvallisuus, Elinkeinoelämän keskusliitto, viitattu 24.5.2020. https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.

Granite 2020. Granite Riskienhallinta. Viitattu 21.8.2020. http://granite.fi/riskienhallinta

GRR 2019. Global Risk Report 2019, World Economic Forum 14th Edition, Insight Report. Viitattu 22.2.2020, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Haaparanta, L. & Niiniluoto, I. 2016. Johdatus tieteelliseen ajatteluun. Helsinki: Gaudeamus.

Heinonen, J., Keinänen, A., Paasonen, J. 2013. Turvallisuustutkimuksen tekeminen. Helsinki: Tietosanoma.

Hillson, D. 2013. The A-B-C of risk culture: how to be risk-mature. Paper presented at PMI® Global Congress 2013—North America, New Orleans, LA. Newtown Square, PA: Project Management Institute.

Hirsjärvi, S. & Hurme, H. 2007, Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2018. Tutki ja kirjoita. 22.painos. Helsinki: Tammi.

Hopkin, P. 2018. Fundamentals of Risk Management, Understanding, evaluating and implementing effective risk management, 5th edition. London, New York, New Delhi: Kogan Page.

HSE 1997. Successful Health and Safety Management. London: Health and Safety Executive, HMSO.

Ilmonen, I., Kallio, J., Koskinen, J., Rajamäki, M. 2016. Johda riskejä, Käytännön opas yrityksen riskienhallintaan, 2.painos. Helsinki: Finva.

IRM 2002. A Risk Management Standard. London: The Institute of Risk Management.

JAMK 2020. Opinnäytetyön raportointi, viitattu 24.5.2020, https://oppimateriaalit.jamk.fi/raportointiohje/4-opinnaytetyon-rakenne/4-2-opinnaytetyon-runko-osa/4-2-3-tietoperusta/

Janesick, V. J. 2000. The choreography of qualitative research design. Teoksessa N. K. Dnezin & Y. S. Lincoln (toim.) 379-399.

Jämsen, C. 2017. Turvallisuusjohtamisjärjestelmä osana organisaation johtamisjärjestelmää, Integraation edellytykset ja mahdollisuudet. Turvallisuusjohdon koulutusohjelma – TJK 14. Aalto University Professional Development – AaltoPro. Tutkielma.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä, Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu (JAMK).

Katakri 2015. Katakri 2015. Tietoturvallisuuden auditointityökalu viranomaisille. Puolustusministeriö. Helsinki: Puolustusministeriö.

Keski-Uudenmaan pelastuslaitos 2012. Pelastusviranomaisen valvontasuunnitelman mukainen TUTOR-arviointi. Max versio. Vantaa: Keski-Uudenmaan pelastuslaitos.

Kerko, P. 2001. Turvallisuusjohtaminen. Jyväskylä: PS-kustannus.

Kiviharju, V. 2015. Onko turvallisuusjohdon sijoittumisella organisaatiorakenteessa vaikutusta turvallisuuden toteuttamiseen ja toteutumiseen?. Kohteena valtiohallinnon organisaatiot. Turvallisuusjohtamisen koulutusohjelma TJK-13. Aalto University Professional Development – AaltoPro. Tutkielma.

Laakkonen, K. 2017. Jatkuva parantaminen. Jatkuvan parantamisen elementit. Oulun ammattikorkeakoulu. Pro Gradu -tutkielma.

Lanne, M. 2007. Yhteistyö yritysturvallisuuden hallinnassa. Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa. Espoo: VTT Publications 632. Väitöskirja.

L423/1988. Laki valtion talousarviosta.

L1243/1992. Asetus valtion talousarviosta.

L668/2008. Laki Terveyden ja hyvinvoinnin laitoksesta.

L675/2008. Asetus Terveyden ja hyvinvoinnin laitoksesta.

L379/2011. Pelastuslaki.

L1552/2011. Valmiuslaki.

L70/2013. Asetus Terveyden ja hyvinvoinnin laitoksesta annetun asetuksen 2 ja 3 §:n muuttamisesta.

L552/2019. Laki sosiaali- ja terveystietojen toissijaisesta käytöstä.

L906/2019. Laki julkisen hallinnon tiedonhallinnasta.

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J., Salminen, M., 2018. Kyberturvallisuuden strateginen johtaminen Suomessa, Valtioneuvoston selvitys- ja tutkimustoiminta, julkaisusarja 28/2018. Helsinki: Valtiovarainministeriö.

Limnéll, J., Majewski, K., Salminen, M. 2014. Kyberturvallisuus. Helsinki: Docendo.

Martikainen, S. 2016 (toim.). Varautuva, turvallinen koulu. Laurea Julkaisut 70. Helsinki: Laurea-ammattikorkeakoulu.

Martikainen, S. & Ranta, T. 2020. Varautuva, ennakoiva oppilaitos ja korkeakoulu – jatkuvuuden turvaaminen arjen normaalioloista poikkeusoloihin. Laurea-julkaisut 141. Helsinki: Laurea-ammattikorkeakoulu.

Maxwell, J. 2016. The 5 levels of Leadership. Viitattu 13.7.2020. https://www.johnmaxwell.com/blog/the-5-levels-of-leadership1/

Mielenihmeet 2018. Psykologia, Maslowin tarvehierarkia. Viitattu 10.7.2020. https://mielenihmeet.fi/maslown-tarvehierarkia/

Mäntyneva, M, Heinonen, J., Wrange, K. 2003. Markkinointitutkimus. Helsinki: WSOY Oppimateriaalit.

Nylander, O. 2017. Tietojohtaminen ja tapaus sote. Norderstadt (Saksa): BoD Books.

Oedewald,P., Reiman,T. 2006. Turvallisuuskriittisten organisaatioiden toiminnan erityispiirteet. VTT Publications 593. Espoo: Otamedia Oy

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2018. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. 3.-5.painos. Helsinki: Sanoma Pro Oy.

Pelkonen, A., Ahlqvist, T., Nieminen, M., Salonen, J., Savola, R., Savolainen, P., Suominen, A., Toivanen, H., Kyheröinen, J. & Remes, J. 2016. Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen. Valtioneuvoston selvitys- ja tutkimustoiminta, julkaisusarja 9/2016. Helsinki: Valtiovarainministeriö.

Peltomäki, J. & Noppa, K. 2015. Rikos meni verkkoon, Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum.

Pwc 2017. Uudistunut COSO ERM uudistaa riskienhallinnan ajattelua, viitattu 21.5.2020, https://uutishuone.pwc.fi/uudistunut-coso-erm-uudistaa-riskienhallinnan-ajattelua/

Reiman, T., Oedewald, P. 2008. Turvallisuuskriittiset organisaatiot, Onnettomuudet, kulttuuri ja johtaminen. Helsinki: Edita.

Reiman, T., Pietikäinen E., Oedewald, P. 2008. Turvallisuuskulttuuri, Teoria ja arviointi. Helsinki: VTT Publications.

Riskikompassi 2018. Riskikompassi – uutta suuntaa riskienhallintaan, viitattu 22.5.2020, https://riskikompassi.fi/

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasa: Vaasan yliopiston julkaisuja.

Seppälä, T. 2017. Organisaation turvallisuusjohtamisjärjestelmän luominen. Laurea-ammattikorkeakoulu. Opinnäytetyö.

SFS-ISO 9000. 2015. Laadunhallintajärjestelmät. Perusteet ja sanasto. Quality Management Systems. Fundamentals and vocabulary. Helsinki: Suomen Standardoimisliitto SFS ry.

SFS-ISO 31000. 2018. Riskienhallinta. Ohjeet, Risk Management. Guidelines. Helsinki: Suomen Standardoimisliitto SFS ry.

SFS 2018. SFS Standardien verkkokauppa, Riskit hallintaan: SFS-ISO 31000, viitattu 21.5.2020, https://sales.sfs.fi/fi/

STM 2011. Riskienhallinta ja turvallisuussuunnittelu, Opas sosiaali- ja terveydenhuollon johdolle ja turvallisuusasiantuntijoille. Sosiaali- ja terveysministeriön julkaisuja 2011:15. Helsinki: Sosiaali- ja terveysministeriö.

STM tulossopimus 2020. Sosiaali- ja terveysministeriön ja Terveyden ja hyvinvoinnin laitoksen tulossopimus vuosille 2020-2023, tulostavoitteet 2020. Helsinki: Sosiaali- ja terveysministeriö. Viitattu 2.7.2020. https://stm.fi/documents/1271139/20710136/Terveyden+ja+hyvinvoinnin+laitos

Suomen kyberturvallisuusstrategia 2013. Valtioneuvoston periaatepäätös 24.1.2013. tulostettu 12.4.2020.

Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös 3.10.2019. tulostettu 3.7.2020.

Sutela, I. 2014. Organisaatioturvallisuuden arvo tietointensiivisessä palveluliiketoiminnassa asiakasnäkökulmasta. Vantaa: Laurea. Opinnäytetyö.

Talous ja koti 2019. Jarno Limnéll: Näin digitaalisuus valtasi Suomen, haastattelu Talous ja koti -lehdessä 6.12.2019. Viitattu 14.7.2020 https://www.talousjakoti.fi/turvallisuus/jarno-limnell-nain-digitaalisuus-valtasi-suomen/#

THL 2020. Terveyden ja hyvinvoinnin laitos. Viitattu 22.2.2020, https://thl.fi/fi/thl/mika-on-thl

THL organisaatio. Terveyden ja hyvinvoinnin laitos. Organisaatio. Viitattu 23.2.2020, https://thl.fi/fi/thl/organisaatio

THL strategia. Terveyden ja hyvinvoinnin laitos. Strategia. Viitattu 23.2.2020, https://thl.fi/fi/thl/strategia

TSK 2017. Kokonaisturvallisuuden sanasto. Helsinki: Sanastokeskus TSK.

TTL 2020. Työterveyslaitos. Johtajuuden sakkaaminen yhteisillä työpaikoilla voi johtaa tapaturmiin tai jopa kuolemiin. Viitattu 28.7.2020. https://www.ttl.fi/johtajuus-sakkaa-yhteisilla-tyopaikoilla/

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi, uudistettu laitos (2.painos). Helsinki: Tammi.

Turpeinen, I. 2017. Organisaatioturvallisuuden nykytila ja sen kehittämismahdollisuuksia Rajavartiolaitoksessa. 14. Turvallisuusjohtamisen koulutusohjelma. Helsinki: Aalto Pro. Tutkielma.

Turvallisuusjohtaminen 2010. Turvallisuusjohtaminen. Työsuojeluhallinto. Aluehallintovirasto, työsuojeluoppaita- ja ohjeita 35. Tampere: Työsuojeluhallinto.

Työturvallisuuskeskus 2020. Johtaminen ja esimiestyö. Viitattu 5.7.2020. https://ttk.fi/tyoturvallisuus_ja_tyosuojelu/tyoturvallisuuden_perusteet/johtaminen_ja_esimiestyo

Työturvallisuuskeskus 2020b. Yhteinen työpaikka ja yhteisten vaarojen paikka. Viitattu 8.7.2020. https://ttk.fi/tyoturvallisuus_ja_tyosuojelu/toimialakohtaista_tietoa/yksityiset_palvelualat/yhteinen_tyopaikka_ja_yhteisten_vaarojen_tyopaikka

VM 2016. Toiminnan jatkuvuuden hallinta, Valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmä – VAHTI 2/2016, Julkisen hallinnon ICT. Helsinki: Valtiovarainministeriö.

VM 2017a. Ohje riskienhallintaan, Valtiovarainministeriön julkaisuja 22/2017, Julkisen hallinnon ICT. Helsinki: Valtiovarainministeriö.

VM 2017b. Ohje riskienhallintaan, liitteet 1-6, Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI). Helsinki: Valtiovarainministeriö.

VM 2017c. Suositus, Diaari VM/532/00.01.00/2015. Valtiovarainministeriö, Valtiovarain contoller -toiminnon suositus valtiohallinnon riskienhallinnasta, Valtiovarain controller -toiminto. Helsinki: Valtiovarainministeriö.

VNK 2020. Turvallisuus ja tilannekuva, Valtioneuvoston kanslia. Viitattu 26.4.2020. https://vnk.fi/turvallisuus-ja-tilannekuva

Virta, M. 2014. Riskienhallintajärjestelmän luominen Terveyden ja hyvinvoinnin laitokselle. Vantaa: Laurea. Opinäytetyö.

Virtanen, T. 2002. Four views on security. Espoo: Teknillinen korkeakoulu. Väitöskirja.

Wiio, O.A. 1994. Johdatus viestintään. 6.painos. Helsinki: Weilin Göös.

Yukl, G.A. 2002. Leadership in organizations. 5. painos. Upper Saddle River: Prentice Hall.

Julkaisemattomat

Riskienhallintapolitiikka 2019. Riskienhallintapolitiikka. Viitattu 14.6.2020. https://terho.thl.fi/wiki01/display/sismaar/Riskienhallintapolitiikka

THL työjärjestys 2020. Työjärjestys THL 2255/0.00.00/2019. Astuu voimaan 1.1.2020. Viitattu 21.7.2020. https://terho.thl.fi/wiki01/pages/viewpage.action?pageId=27165506&preview=/27165506/150159082/Ty%C3%B6j%C3%A4rjestys.pdf

THL työjärjestys 2020 organisaatio. Työjärjestys THL 2255/0.00.00/2019, THL organisaatio. Viitattu 21.7.2020. https://terho.thl.fi/wiki01/pages/viewpage.action?pageId=27165506&preview=/27165506/158673909/Organisaatio%20liite%201.pdf

THL työjärjestys 2020 erityistehtävät. Työjärjestys THL 2255/0.00.00/2019, liite 4, Laitoksen henkilöstölle määrätyt erityistehtävät. Viitattu 21.7.2020. https://terho.thl.fi/wiki01/pages/viewpage.action?pageId=27165506&preview=/27165506/166372783/Liite%204%20Erityistehtävät.pdf

Turvallisuusryhmä 2020. THL intranet. Viitattu 25.8.2020. https://terho.thl.fi/wiki01/x/OXZ6Ag

Kuviot

Taulukot

Liitteet

Liite 1: Sanasto

Käsite	Selite
Digitaalinen turvallisuus	Digitaalinen turvallisuus on digitaalisessa muodossa olevien tietojen ja niiden käsittelemisen, siirtämisen ja säilyttämisen turvallisuudesta varmistamista, Digitaalisella turvallisuudella vaikutetaan myös fyysisen ympäristön turvallisuuden toteutumiseen.
Kyber	Kyber-sana tulee kreikan sanasta kybero, jonka merkityksiä ovat ohjata, opastaa ja hallita. Kyber tarkoittaa sähköisessä muodossa olevan informaation käsittelyä. Kyber on etuliite, jolla viitataan tieto-ja viestintäteknologian mahdollistaman digitaalisen maailman ilmiöihin, tapahtumiin, toimijoihin, toimintoihin, toimintatapoihin ja normeihin. Lyhyesti, digitaalinen bittien maailma. Kyber -etuliitettä käytetään esim. sanoissa kyberturvallisuus, kyberuhka, kyberhyökkäys, kybertoimintaympäristö, kybersota, kyberaltis prosessi.
Kyberturvallisuus	Kyberturvallisuus on tietoturvaa laajempi käsite ja sillä varmistetaan, että kybertoimintaympäristöön voi luottaa ja sen tarkoituksenmukaisesta toiminnasta voidaan huolehtia. Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle. (kts. kyberhyökkäys) Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä (”yhteisöllinen tietoturva”). Menettelyjen avulla pystytään estämään tietoturvauhkien toteutuminen, ja niiden mahdollisesti toteutuessa estämään, lieventämään tai sietämään niiden vaikutuksia. Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle.
Kyberhyökkäys	Kyberhyökkäys tarkoittaa bittien maailman kautta tapahtuvaa hyökkäystä, jolla voidaan tuottaa haittaa, vahinkoa ja tuhoa sekä fyysiseen, että bittien maailmaan. Kyberhyökkäyksen tarkoituksena voi olla myös tiedon varastaminen tai laitteiden ja järjestelmien käytön estäminen.
Kybertoimintaympäristö	Kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö.
Tietoturvallisuus	Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa myös oloja, joissa tietoturvariskit ovat hallinnassa.
Jatkuvuuden hallinta	Jatkuvuuden hallinnan tarkoituksena on mahdollistaa organisaation häiriötön toiminta kehittämällä varautumis-, jatkuvuus-, toipumis- ja valmiussuunnittelua. Suunnitelmien avulla organisaatio voi varautua erilaisiin normaaliolojen häiriötilanteisiin sekä poikkeusoloihin. Jatkuvuuden hallinta

	edellyttää toimintaan liittyvien riskien ja muiden toimintaan vaikuttavien riippuvuuksien tunnistamista.
Kokonaisturvallisuus	Kokonaisturvallisuudella tarkoitetaan yhteiskunnan elintärkeiden toimintojen turvaamista viranomaisten, järjestöjen, elinkeinoelämän ja kansalaisten yhteistoimintana. Yhteiskunnan turvallisuusstrategiassa (VNpp 2017) on määritetty yhteiskunnan elintärkeät toiminnot: johtaminen, kansainvälinen ja EU-toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus, väestön toimintakyky ja palvelut sekä henkinen kriisinkestävyys
Riskienhallinnan periaatteet	Organisaation johdon päättämät riskienhallintaan liittyvät periaatteet ja tavoitteet, jotka on kuvattu riskienhallintapolitiikka tai -periaatteet dokumentissa.
Riskienhallinnan puitteet	Koostuvat osatekijöistä, jotka yhdessä muodostavat organisaation riskienhallinnan suunnittelun, toteutuksen, seurannan, katselmoinnin ja jatkuvan kehittämisen perustan ja organisoinnin.
Riskienhallinnan prosessi	Sisältää hallintaperiaatteiden, -menettelyjen ja -käytäntöjen järjestelmällisen soveltamisen viestintään ja tiedonvaihtoon sidosryhmien kanssa, toimintaympäristön määrittelemiseen liittyviin toimintoihin sekä riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan ja katselmointiin.
Jäännösriski	Riskiin käsittelyn jälkeen jäävä riski, jota ei voida tai ei haluta poistaa. Jäännösriskeihin voi sisältyä tunnistamattomia riskejä.
Riski	Epävarmuuden vaikutus tavoitteisiin. Vaikutus on poikkeama odotetusta. Vaikutus voi olla myönteinen tai kielteinen suhteessa odotusarvoon. Riski kuvataan useimmiten viittaamalla tapahtumaan ja/tai seurauksiin ja ilmaistaan todennäköisyydellä ja vaikutusten yhdistelmänä.
Riskianalyysi	Prosessi, jolla pyritään ymmärtämään riskin luonne ja määrittämään riskitaso. Riskianalyysi on riskin merkityksen arvioinnin ja riskin käsittelyä koskevien päätösten perusta. Riskianalyysi sisältää riskin suuruuden arvioinnin.
Riskien arviointi	Kokonaisprosessi, joka kattaa riskien tunnistamisen, riskianalyysin ja riskin merkityksen arvioinnin.
Riskien käsittely	Riskien muokkaamisprosessi, jossa päätetään esimerkiksi seuraavista toimenpiteistä Riskin torjuminen tai poistaminen päättämällä olla aloittamatta tai jatkamatta riskin aiheuttavaa toimintaa Riskin ottaminen tai lisääminen jonkin mahdollisuuden saavuttamiseksi Riskin lähteen tai syyn poistaminen Todennäköisyyden muuttaminen tai todennäköisyyteen vaikuttaminen Seurausten muuttaminen tai vaikutuksiin varautuminen Riskin jakaminen yhden tai useamman osapuolen kanssa (esimerkiksi sopimuksin tai riskin rahoittamisella Riskin tietoinen säilyttäminen ja sietäminen
Riskien tunnistaminen	Riskien havaitsemisen ja kuvaamisen prosessi
Riskienhallinta	Koordinoitu toiminta, jolla johdetaan, ohjataan ja hallitaan organisaation riskejä
Riskien luokitus	Arvioitavan kohteen luokittelun apuväline. Riskien luokitteluun ei ole yhtä ainoaa kaikille sopivaa mallia tai tapaa. Organisaation riskien luokittelu tulee suunnitella ja toteuttaa organisaation toiminnan erityispiirteet huomioon ottaen. Keskeistä on, että organisaatio käyttää omassa toiminnassaan yhteisesti sovittua ja yhdenmukaista riskiluokitusta.

	Luokittelu malli voi olla esimerkiksi strategiset riskit, operatiiviset riskit, taloudelliset riskit ja vahinkoriskit (käytössä THL:ssä)
Riskimatriisi	Riskimatriisin avulla luokitellaan riskin suuruus tapahtuman seurausten vakavuuden ja esiintymisen todennköisyyden perusteella. Matriisi auttaa hahmottamaan riskin merkittävyyttä ja sitä, miten riski suhteutuu muihin riskeihin.
Riskien sietokyky	Riskimäärä, johon organisaatiolla on valmius sitoutua riskien määrittelyn jälkeen.
Resilienssi	Joustavuus, kyky sietää epävarmuutta ja sopeutua muutoksiin sekä kyky selviytyä ongelmatilanteista ja yllättävistä muutoksista. Resilienssin lähtökohtana on ajatus siitä, että turvallisuutta vaarantavat tilanteet syntyvät toimintojen odottamattomista yhdistelmistä, eivät niinkään toimintavirheistä tai häiriöistä, joita voidaan hallita suunnittelulla. Turvallisuuden hallinta onnistuu, jos toimintatavat joustavat tilanteiden ja olosuhteiden mukaisesti. Resilienssiin liitettyjä määreitä ovat joustavuus, kimmoisuus ja palautumiskyky.
Tiedolla johtaminen	Tiedolla johtamisella tarkoitetaan oikeaan tietoon perustuvaa päätöksentekoa, jossa oikea tieto saadaan eri lähteistä ja dataa analysoimalla. Moderni tiedolla johtaminen vaatii organisaatiolta kykyä kehittyä ja muuntautua monipuolisesti. Tiedolla johtamisen osa-alueita ovat kulttuuri, osaaminen, organisaatiorakenne ja teknologia.
Sisäinen valvonta	Menettelyt, joilla varmistetaan: Talouden toiminnan laillisuus sekä tuloksellisuus Varojen ja omaisuuden turvaaminen Oikeat ja riittävät tiedot organisaation taloudesta ja toiminnasta
Uhka	Epätoivottu, kielteinen vaikutus organisaatioon tai järjestelmään, jossa ei ole olemassa positiivista mahdollisuutta.
Varautuminen	Tarkoitetaan sellaisia ennakoivia toimia, jotka suunnitellaan esimerkiksi häiriötilanteiden tai poikkeusolojen varalle: Valmiussuunnitelmaa, joka laaditaan esim. valmiuslain tai yhteiskunnan turvallisuusstrategiassa kuvatun velvoitteen perusteella Jatkuvuussuunnitelmaa, joka laaditaan esim. prosessin tai laajan palvelukokonaisuuden häiriötilanteiden aikaisen toiminnan valmisteluksi Toipumissuunnitelmaa, joka laaditaan järjestelmien häiriötilanteista selviytymiseksi.

Sanastolähteet

Advian 2020. Mitä on tiedolla johtaminen? Viitattu 10.7.2020. https://www.advian.fi/mita-on-tiedolla-johtaminen

Kalliomaa, M., Hänninen, T., Sikanen, T., Reinikainen, V. (toim.). 2018. Turvallinen Suomi 2018. Tietoja Suomen kokonaisturvallisuudesta. Turvallisuuskomitea.

Limnéll, J., Majewski, K., Salminen, M. 2014. Kyberturvallisuus. Helsinki: Docendo.

Peltomäki, J. & Noppa, K. 2015. Rikos meni verkkoon, Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum.

TSK 2017. Kokonaisturvallisuuden sanasto. Helsinki: Sanastokeskus TSK.

VM 2017b. Ohje riskienhallintaan, liitteet 1-6, Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI). Helsinki: Valtiovarainministeriö.

VM 2020. Valtiovarainministeriön verkkosivu. Riskienhallintapolitiikka liite 2. Viitattu 2.5.2020. https://vm.fi/riskienhallinta/riskienhallintapolitiikka

Liite 2: Teemakysymykset

Haastateltaville on lähetetty 20.6.2020 sähköpostilla pyyntö osallistua haastatteluun. Haastatteluun varattiin kaksi tuntia aikaa ja se nauhoitettiin. Haastattelut pidettiin Skypellä.

Seuraavassa haastattelun sisältö. Teksti jaettiin johdannon ja teemojen otsikkotasojen osalta haastateltaville etukäteen, mutta toistettiin myös haastattelun aluksi.

Teemahaastattelu

Teemahaastattelulla pyritään selvittämään mikä on tällä Terveyden ja hyvinvoinnin laitoksen turvallisuuden johtamisen tämän hetkinen tilanne. Teemoja on yhdeksän ja lisäksi on vapaan sanan osio.

Johdanto

Olen Mikael Inkinen ja opiskelen Laurea ammattikorkeakoulussa turvallisuusjohtamisen maisteritutkintoa (YAMK, MBA). Työskentelen THL:ssä tietopalvelut (TIPO) osastolla ja tietohallintopalvelut (TIPA) yksikössä ICT-kehittämispäällikkönä ja yksikön varapäällikkönä ja olen opiskellut nykyistä tutkintoa työn ohessa. Olen aikaisemmin suorittanut alemman korkeakoulututkinnon turvallisuusjohtamisessa ja nyt jatkanut sitä ylemmällä tutkinnolla. Opinnäytetyön valmistelu ja teoriaosuuden kirjoitus on tapahtunut kevään 2020 aikana, teemahaastattelut on tarkoitus tehdä kesällä ja lopullinen kirjoitustyö syksyyn mennessä. Työn on tarkoitus olla valmis elokuun loppuun mennessä.

Tämä teemahaastattelu liittyy Laurealle opinnäytetyönä tehtävään kehittämistutkimukseen, jonka tarkoituksena on havaita ongelmakohtia ja kehittää turvallisuuden johtamista Terveyden ja hyvinvoinnin laitoksella. Tutkimuksen teoriaosuuden ja dokumenttianalyysin lisäksi on tämä teemahaastattelu. Tarkoitus on haastatella 3-6 Terveyden ja hyvinvoinnin laitoksen turvallisuuteen ja turvallisuuden johtamiseen liittyvää henkilöä.

Opinnäytetyöni aiheena on ”Turvallisuuden johtamisen kehittäminen Terveyden ja hyvinvoinnin laitoksella”.

Haastatteluun olen varannut kaksi tuntia ja haastattelu nauhoitetaan. Opinnäytetyö on julkinen, mutta jos haastattelussa tulee asioita, jotka halutaan salata, jätän ne pois julkisesta julkaisusta. Toivon, että voidaan käydä kaikki kysymykset läpi tällä yhdellä haastattelukerralla. Itse haastatteluvastauksia ei sellaisenaan sisällytetä opinnäytetyöhön, vaan ne jäävät vain minun haltuuni ja opinnäytetyöhön tulee niistä tulkinnat. Haastattelu tehdään koronatilanteesta johtuen Skypellä.

Onko sinulla mitään kysyttävää haastattelun kulusta tässä vaiheessa?

Kiitos, että olet suostunut haastatteluun.

Haastattelukysymykset

Teemahaastattelu on yksilöhaastattelu ja kysymysten tarkoitus on minulle saada ymmärrys siitä, mikä on Terveyden ja hyvinvoinnin laitoksen turvallisuuden ja riskienhallinna kokonaiskuva ja miten turvallisuuden johtaminen on organisoitu sekä mitä mahdollisia kehittämiskohteita siitä löytyisi. Herätteenä aiheelle on toiminut Matias Virran vuonna 2014 tekemä opinnäytetyö (Laurea, turvallisuusala) ”Riskienhallintajärjestelmän luominen Terveyden ja hyvinvoinnin laitokselle”, jossa esitetään jatkotutkimustarpeena turvallisuusjohtamisen kehittämistä riskienhallinnan pohjalta sekä Cristian Jämsenin tekemä turvallisuusjohdon koulutusohjelman tutkielma ” Turvallisuusjohtamisjärjestelmä osana organisaation johtamisjärjestelmää, Integraation edellytykset ja mahdollisuudet”, jossa on tutkittu miten turvallisuudenjohtaminen ja organisaation johtamisjärjestelmä sovitetaan yhteen sekä on esitetty jatkotutkimuksen aiheena miten turvallisuuden johtamista tulisi kehittää.

Tutkimus keskittyy turvallisuuden johtamiseen, mutta riskienhallinta on isossa roolissa, koska sen perusteella ja ohjaamana turvallisuustoimenpiteitä ja turvallisuuden johtamista toteutetaan. Näkökulma riskienhallintaan on riskienhallinnan standardit, hyvät käytänteet ja valtiohallinnon ohjeistus. Pohjana on käytetty myös THL:n turvallisuuteen liittyvää materiaalia niiltä osin kuin se on ollut saatavilla ja sitä ei ole luokiteltu. Työn ohjaajana toimii THL:ssä palvelujohtaja Mikko Nissinen ja Laureassa professori ja turvallisuusjohtaminen -koulutusohjelman pääopettaja Jukka Ojasalo.

Teemoja on yhdeksän kappaletta sekä vapaan sanan osuus ja esitän tarvittaessa niistä lisäkysymyksiä.

1. **Teema: Turvallisuusjohtamisen yleiskuva**
   Terveyden ja hyvinvoinnin laitoksessa (THL) toimii monta turvallisuuteen liittyvää nimikettä. Olen tunnistanut ainakin seuraavat: Turvallisuuspäällikkö, tietoturvapäällikkö, tietosuojavastaava, työsuojelupäällikkö, valmiuspäällikkö ja bioturvapäällikkö sekä laatupäällikkö. Lisäksi laitoksella on erikseen valmiusjohtaja. Osa turvallisuuden organisoinnista on Hallinnon tukipalvelun (HATU) yksikön ja palvelujohtajan vastuulla (turvallisuusryhmän vetäjä) ja osa muiden yksiköiden vastuulla.
   Miten arvioisit THL:n turvallisuuden johtamista ja organisoitumista kokonaisuutena?

2. **Teema: Turvallisuuden organisointi ja vastuuttaminen**
   Turvallisuus on nykypäivänä keskiössä ainakin kaikissa suurissa organisaatioissa ja erityisesti valtiohallinnossa virastolta edellytetään turvallisuuden huomioimista kaikessa toiminnassa.

Miten arvioisit, että turvallisuuden organisointi ja vastuuttaminen THL:ssä on vastannut tähän vaatimukseen?

3. **Teema: Riskienhallinnan kattavuus**
   Miten riskienhallintaa seurataan ja dokumentoidaan THL:ssä ja onko siihen osallistettu kaikki osastot ja koko henkilöstö?
   Miten laajasti arvioisit, että riskit tulee tunnistetuksi ja huomioiduksi sekä arvioiduksi tämän päivän THL:n toiminnassa?

4. **Teema: Globaalien riskien seuranta**
   Maailmanlaajuisesti turvallisuustilanne vaihtelee ja koko ajan ilmaantuu uusia uhkia, joilla voi olla vaikutusta myös THL:n toimintaan. Uhkien kohdentuvuus Suomeen ja erityisesti valtiohallintoon myös vaihtelee esimerkkinä vaikkapa kyberuhat tai radikalisoituminen ja sitä kautta terrorismi.
   Onko THL:ssä vastuutettu globaalien riskien seurantaa jollekin tai joillekin ja tuodaanko niitä arvioitavaksi THL:n strategian ja toiminnan näkökulmasta?

5. **Teema: Jatkuvuuden hallinta ja kyberuhat**
   Kyberuhat on turvallisuuden osa-alue, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan ja organisaatioiden kriittisiin toimintoihin. Kyberturvallisuusajattelussa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja kriisivarautumisen ajattelua.
   Kyberuhkien toteutuminen voi olennaisesti vaikuttaa THL:n toimintaan.
   Miten tämänhetkisessä organisaatiossa huomioidaan kyberuhat ja miten niiden seuraaminen on organisoitu ja otettu huomioon jatkuvuuden hallinnassa?

6. **Teema: Kansallinen vaikuttavuus ja yhteistyö**
   THL on suuri organisaatio, jossa turvallisuuden organisoinnilla ja riskienhallinnalla on suuri kansallinenkin merkitys osana valtiohallintoa.
   Miten arvioisit THL:n turvallisuuden organisoinnin ja vastuiden toimivan tällä hetkellä kansallisen turvallisuuden ja yhteistyön näkökulmasta ja miten näkisit yhteistyön merkityksen ja toimivuuden muiden kansallisten toimijoiden kanssa?

7. **Teema: Kansainvälinen yhteistyö**
   Turvallisuustyö on kansainvälistä työssä, jossa olennaisena osana on saada tietoa ja jakaa tietoa kansainvälisille yhteisöille.
   Miten näkisit, että kansainvälistä yhteistyötä toteutetaan THL:ssä turvallisuuden

näkökulmasta?

8. **Teema: Hyviä turvallisuuden ja riskienhallinnan esimerkkejä**
   Turvallisuuden alueita, joita olen tunnistanut THL:ssä on toimitilaturvallisuus, työsuojelu, bioturvallisuus, laboratorioturvallisuus, tietoturvallisuus ja tietosuoja, valmiustoiminta sekä matkustusturvallisuus.
   Onko myös jotain muita kokonaisuuksia, joita en ole tunnistanut? Mikä turvallisuuden tai riskienhallinnan alue toimii mielestäsi parhaiten THL:ssä ja miksi?

9. **Teema: Turvallisuuskulttuuri**
   Turvallisuuskulttuurilla tarkoitetaan organisaation kykyä ja tahtoa ymmärtää, millaista turvallinen toiminta on, millaisia vaaroja organisaation toimintaan liittyy ja miten niitä voidaan ehkäistä, sekä kykyä ja tahtoa toimia turvallisesti. Turvallisuuskulttuuri on dynaaminen ja muokkautuva tila. (VTT 2008)
   Miten luonnehtisit THL:n turvallisuuskulttuuria?

10. **Vapaa sana**
    Haluatko vielä tuoda esiin muita näkemyksiä THL riskienhallinnasta, turvallisuudesta tai muusta aiheesta?

Kiitos haastattelusta.

Liite 3: Turvallisuuteen liittyvät standardit ja lainsäädäntö osa-alueittain Terveyden ja hyvinvoinnin laitoksella.

Turvallisuuteen liittyviä standardit, jotka on listattu THL:n intranetissa:

SFS-**ISO 31000**:2018. Riskienhallinta. Ohjeet.

EN **ISO/IEC 27000**:2017. Informaatioteknologia. Turvallisuustekniikat.Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto.

SFS-EN **ISO/IEC 27001**:2017. Informaatioteknologia. Turvallisuustekniikat.Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

CWA 15793. Laboratory biorisk management.

Turvallisuuden osa-alue	**Lainsäädäntö**
Työturvallisuus (ote työturvallisuusohjeesta)	Laki 1347/1988 työterveyshuoltolaki Laki 738/2002 työturvallisuuslaki Laki 309/2005 vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta Laki 379/2011 pelastuslaki Laki 599/2013 kemikaalilaki Laki 717/2001 syöpäsairauden vaaraa aiheuttaville aineille ja menetelmille ammatissaan altistuvien rekisteri Laki 527/2014 ympäristönsuojelulaki Säteilylaki 859/2018, voimaan 15.12.2018 STM:n asetus 921/2010 liitteineen biologisten tekijöiden luokituksesta VNA 769/2015 ammattitautiluettelosta VNA 708/2013 hyvän työterveyshuoltokäytännön periaatteista … VNA 715/2001 kemiallisista tekijöistä töissä ml. VNA 602/2015 VNA 603/2015 lisääntymisterveydelle työssä vaaraa aiheuttavista tekijöistä ja vaaran torjunnasta VNA 1485/2001 terveystarkastuksista erityistä sairastumisen vaaraa aiheuttavissa töissä VNA 716/2000 työhön liittyvän syöpävaaran torjunnasta VNA 933/2017 työntekijöiden suojelemiseksi biologisista tekijöistä aiheutuvilta vaaroilta VNA 85/2006 työntekijöiden suojelemisesta melusta aiheutuvilta vaaroilta VNA 403/2008 työvälineiden turvallisesta käytöstä ja tarkastamisesta VNp 1407/1993 henkilönsuojainten valinnasta ja käytöstä työssä VNp 1409/1993 käsin tehtävistä nostoista ja siirroista VNp 1405/1993 näyttöpäätetyöstä Vnp 922/1999 työntekijöille aiheutuvan suuronnettomuusvaaran torjunnasta VNp 687/2015 työpaikkojen turvamerkeistä ja niiden vähimmäisvaatimuksista
Tietoturvallisuus (ote tietoturvallisuusohjeesta)	Niin julkishallinnossa kuin Terveyden ja hyvinvoinnin laitoksessa käsitellään runsaasti sekä julkista että salassa pidettävää tietoa. Suomen lainsäädännössä on laajasti tietoturvavelvoitteita – toisin sanoen myös lainsäädäntö lähtee siitä, että tietoturvallisuus on hoidettava asianmukaisesti. Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain

	(julkisuulaki, 621/1999) ja asetuksen (1030/1999) lisäksi useisiin muihinkin lakeihin ja säännöksiin. Näistä Terveyden ja hyvinvoinnin laitoksen toimintoja tärkeimpinä koskevat henkilötietolaki (523/1999) sekä tietoturva-asetus (681/2010). Henkilötietojen ja henkilörekisterin osalta erityisvaatimuksista vastaa henkilötietolaki. Tietoturva-asetus toimii pohjana valtionhallinnossa toteutuvalle tietoturvallisuudelle. Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädeltyjä perusoikeuksia. Julkisuuslainsäädännön mukaan tieto on **aina lähtökohtaisesti** julkista, ellei se julkisuuslain tai muiden säädösten perusteella ole salassa pidettävää. Tietojen lain mukaisesta käsittelystä on aina huolehdittava.
Muut turvallisuuden osa-alueet	Ei saatavilla lainsäädännön listausta.

Liite 4: Riskienhallinnan standardeja ja arviointimenetelmiä

Riskienhallinnan standardeja ja hyviä käytänteitä ovat mm. ISO 31000, COSO-ERM, PEST-analyysi ja PESTLE-malli sekä vaikutusanalyysi. Seuraavassa on kukin kuvattu lyhyesti.

SFS-ISO 31000 Riskienhallinta

SFS-ISO 31000 auttaa organisaatiota luomaan riskienhallinnan puitteet, joiden avulla voidaan tehokkaasti tunnista, arvioida ja käsitellä riskien vaikutusta organisaation tavoitteiden saavuttamiseen. Standardin tavoitteena on luoda organisaation riskienhallinnan kulttuuri, jossa henkilöstö ja sidosryhmät ovat tietoisia riskien seurannan ja hallinnan merkityksestä. (SFS 31000)

ISO 31000 standardi on käsitelty omassa kappaleessaan itse tekstissä.

COSO-ERM -riskienhallinta

Sisäisen valvonnan lähtökohdista ja sisäisen valvonnan riskienhallinnan tarpeisiin on tuotettu kansainvälinen ja erityisesti yrityksissä laajasti käytössä oleva kaupallinen COSO tai COSO-ERM riskienhallinnan malli. COSO-ERM tulee sanoista *The Committee of Sponsoring Organizations of The Treadway Comission, Enterprise Risk Management*.

COSO-ERM (2017) on edellisen julkaisun (2004 julkaistiin ”Enterprise Risk Management - Integrated Framework”) jälkeen päivitetty asiakirja, jonka otsikko on nyt ”Enterprise Risk Management – Integrated with Strategy and Performance” korostaa riskin huomioon ottamisen tärkeyttä sekä strategian laatimisprosessissa että suoritustavoitteessa. Päivitetyn julkaisun ensimmäinen osa tarjoaa perspektiivin nykyisistä ja kehittyvistä yritysriskien hallinnan käsitteistä ja sovelluksista. Toinen osa, ”Puitteet” (Framework), on jaettu viiteen helposti ymmärrettävään komponenttiin, jotka sopivat eri näkökulmiin ja toimintarakenteisiin parantamaan strategioita ja päätöksentekoa.

1. Riskien hallinta ja kulttuuri (Risk Governance and Culture)
2. Riskien, strategian ja tavoitteiden asettaminen (Risk, Strategy and Objective-Setting)
3. Täytäntöönpanoriskit (Risk Execution)
4. Riskitiedotus ja raportointi (Risk Information, Communication and Reporting)
5. Yrityksen riskienhallinnan ja suorituskyvyn seurata (Monitoring Enterprise Risk Management Performance)

PESTLE-malli ja PEST-analyysi

Riskien arvioinnissa voi käyttää apuna myös PESTLE-mallia, jossa riskien juurisyitä arvioidaan tarkemmin. Toisin sanoen arvioidaan niitä syitä, jotka mahdollistavat heikkouksia ja joilla on vaikutuksia organisaation toimintaan. PESTLE-mallissa arvioidaan seuraavia juurisyitä.

P	Politiikka (Politics)	Valtio-ohjaus, säätely, poliittinen ohjaus, verotus
E	Talous (Economy)	Talouskasvu tai -lasku, korot, inflaatio, vaihtokurssit
S	Yhteiskunta (Society)	Kulttuuri, terveys, ikääntyminen, turvallisuus, väestönkasvu, työllisyys
T	Teknologia (Technology)	Automaatio, tuotekehitys, teknologinen muutos
L	Laki (Law)	Lainsäädäntö, tullit, tietoturva, hankinta, työsuojelu, ICT
E	Ympäristö tai ekologisuus (Environment or Ecology)	Sää, ilmasto, ilmastonmuutos, ympäristötietoisuus

PESTLE-mallia (kirjoitetaan myös PESTEL) voi käyttää riskien arvioinnissa myös toimintaympäristön muutosten hahmottamiseen ja näiden muutosten aiheuttamien riskien tunnistamiseen. (Vahti 2017b)

Malli on alunperin ollut PEST-analyysimalli, mutta siihen on erityisesti UK:ssa haluttu lisätä lain ja ympäristön tuoma ulottuvuus ja tämä laajennettu malli on käytössä myös Suomessa. PEST-analyysia voidaan laajentaa pienempiin osiin jaettavilla luokilla, jotka painottavat eri asioita. Tästä esimerkkinä ovat PESTLE (ekologisuus), STEEPLE (eettisyys), demokraattisuus (STEEPLED) tai monikulttuurisuus (SPELIT).

PEST-analyysia käytetään kuten SWOT-analyysia (*Strengths, Weaknesses, Opportunities, Threads*) eli määritellään nelikenttä, johon sijoitetaan yrityksen toimintoon liittyviä riskejä peilaten niitä politiikan, talouden, yhteiskunnan ja teknologian näkökulmista. PEST-analyysin tekeminen on tärkeää erityisesti aloitteleville yrityksille ja ulkomaiden toimintoja aloitteleville yrityksille. Yritykselle on tärkeää ymmärtää minkälaisia poliittisia, taloudellisia, yhteiskunnallisia ja teknologisia riskejä yrityksen operatiiviseen toimintaa ja eri sektoreihin sisältyy, jos ollaan laajentamassa toimintoja Yhdysvaltoihin, Afrikkaan tai Aasiaan. Riskit ovat näissä esimerkkikohteissa hyvin erilaiset keskenään ja verrattuna toimintaan Suomessa.

Vaikutusanalyysi

Vaikutusanalyysillä (*BIA, Business Impact Analysis*) tarkoitetaan toiminnan keskeyttävien tai toiminnan jatkuvuutta häiritsevien uhkien tunnistamista sekä toimintaan liittyvien riippuvuuksien tunnistamista. Tieto- ja kyberturvallisuuden näkökulmasta vaikutusanalyysissä erityisesti valtiohallinnon tai muun julkisen sektorin organisaation toiminnan kannalta tarkasteltavia asioita ovat muun muassa

- Vaikutukset omaan operatiiviseen toimintakykyyn

- Vaikutukset säädösperusteisten tehtävien suorittamiseen (vrt. myös yhteiskunnan elintärkeät tehtävät
- Vaikutukset yhteiskunnalle
- Riippuvuussuhteet ja niiden vaikutukset
    - Oman organisaation riippuvuus toisesta osapuolesta tai palvelusta tai toisista organisaatioista ja palveluista
    - Toisen organisaation tai palvelun riippuvuus oman organisaation tuottamasta palvelusta tai toiminnasta

Huolellisesti toteutetulla vaikutusanalyysillä (ns. BIA-analyysi) voidaan selvittää esimerkiksi palvelun tai järjestelmän tärkeys, kriittiset riippuvuudet, toimintaa uhkaavat riskit ja uhat sekä tarvittavat jatkokehitystoimet. (VM 2017b)

Riskienhallinnan vastuukuvaus – RACI-malli

Riskienhallinnan vastuut pitää olla määritelty riskienhallintapolitiikassa. Viime kädessä riskienhallinnasta vastaa organisaation ylin johto. RACI-mallin avulla voidaan määritellä erilaiset roolit riskienhallinnassa. RACI-malli sisältää neljä erilaista roolia eli

1. Vastuullinen henkilö (Responsible, R) suorittaa annetun tehtävän tai on osa suoritustiimiä. Jokaisella tehtävällä tulee olla ainakin yksi vastuullinen henkilö.
2. Vastuussa oleva (Accountable, A) henkilö valvoo, että tehtävä tulee valmiiksi. Jokaisella tehtävällä on vai yksi vastuuhenkilö.
3. Neuvonantajalta (Consulted, C) voidaan kysyä ohjeita ja neuvoja tehtävän suorittamiseen. Jokaisella tehtävällä voi olla nollasta lukemattomaan määrään neuvonantajia.
4. Tiedotettava (Informed, I) on henkilö, jolle tiedotetaan tehtävän suorittamisesta. Jokaisella tehtävällä voi olla nollasta lukemattomaan määrään tiedotettavia.

Onnistuneessa RACI-mallissa useimmiten ylemmän tason vastuullinen henkilö (R) on alemman tason vastuussa oleva henkilö (A). Neuvonantajan (C) ja tiedotettavan (I) rooli ja tehtävät voivat vaihdella organisaatioittain ja organisaatioiden sisälläkin hyvin paljon. (VM 2017b)

RACI-mallin mukaisten vastuiden kuvauksissa (RACI-matriisi) käytetään tyypillisesti excel-taulukkoa, mutta muitakin kuvaustapoja voidaan käyttää, kuten kalanruotokaaviota. (VM 2017b)

Alla on esimerkki RACI-mallista palvelujohtajan, palvelupäällikön, SMO:n (palveluhallintatoimisto), tietoturvapäällikön ja hankintapäällikön suhteen

RACI	Palvelujohtaja	Palveluvastaava	SMO	Tietoturva-päällikkö	Hankintayk-sikkö
Palveluluettelon ylläpi-täminen	A	C	I	I	C
Asiakasraportointi	A	R	C	C	C
Ratkaisujen räätälöinti ja tiedotus	I	A	R	I	C
Asiakaspalautteeseen vastaaminen	I	A	R	I	-

RACI-taulukko näyttää eri toimijoiden vastuut ja siihen voidaan tarvittaessa vedota, jos jokin toiminto esimerkiksi projektissa on hidastunut tai sitä ei ole suoritettu.

Todettakoon lisäksi, että muitakin riskien arviointimenetelmiä on useita. Näitä ovat esimerkiksi HAZOP, HACCP, RCA, CBA, FTA, Bayes, VaR, Deplhi ja CORAS. Näitä ei ole käsitelty tässä, mutta niistä löytyy lisätietoja verkosta ja kirjallisuudesta.