Tuomas Kokkomäki
Mika Nortunen

HERÄTE

VALIDOITU RISKIEN ARVIOINNIN PROSESSIMALLI ORGANISAATION MENESTYKSEN TUKEMISEKSI

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

TIIVISTELMÄ

Kokkomäki, Tuomas; Nortunen, Mika
Heräte – validoitu riskien arvioinnin prosessimalli organisaation menestyksen tukemiseksi
Jyväskylä: Jyväskylän yliopisto, 2016, 197 s.
Tietojenkäsittelytiede, pro gradu -tutkielma
Ohjaajat: Salo, Markus; Moilanen, Panu

Riskien arviointi on osa organisaation kilpailukykyä, jolloin ketterät sekä dynaamiset toimintatavat ovat ratkaisevassa asemassa. Epävarmuus ja toimintaympäristön nopeat muutokset tuovat mukanaan myös mahdollisuuksia. Laadukas riskien arviointi on keino erottua kilpailijoista, varmistaa osaltaan organisaation luotettavuus ja trendien tunnistamisen kautta löytää uusia mahdollisuuksia tulevaisuuden innovaatioille. Yhä monimutkaistuva maailma luo organisaatiolle tarpeen tehdä tehokkaita toimenpiteitä entistä nopeammin. Organisaatioiden tulee pystyä reagoimaan nopeasti muuttuvan toimintaympäristön asettamiin haasteisiin. Tutkimuksen tavoitteena oli muodostaa tieteellisen tutkimuksen, riskien arviointiin soveltuvien menetelmien, kuten standardien ja tutkimuksen aikana suoritettujen tietoturvajohtajien haastatteluiden perusteella ketterä ja dynaaminen riskien arvioinnin prosessimalli. Muodostetun prosessimallin on tarkoitus auttaa organisaatioita yhtenäistämään riskien arvioinnin prosessia organisaation eri tasoilla ja tuottamaan yhdenmukaista ja vertailukelpoista materiaalia riskien hallitsemiseksi ja tulevan riskien arvioinnin taustamateriaaliksi. Tutkimus toteutettiin kaksivaiheisena laadullisena tutkimuksena, jonka empiirinen materiaali kerättiin yhteensä kuudesta suomalaisesta finanssialan organisaatioista. Muodostettu riskien arvioinnin malli validoitiin esittelemällä se kolmelle turvallisuuden ammattilaisille. Malli tarjoaa mahdollisuuden mahdollisimman monipuoliseen tiedon keräämiseen. Mallin taustalla on ajatus uhkien sekä muiden herätteiden kattavasta tunnistamisesta, riskien arvioinnin nopeuttamisesta, yksinkertaistamisesta ja yhdenmukaistamisesta organisaation strategian mukaisesti. Tieto ja tilannekuva ovat aina jossain määrin puutteellisia. On tärkeää, että riskien arvioinnin prosessi on joustava ja dynaaminen. Malli pyrkii esittämään riskien arvioinnin prosessina, jossa olemassa olevaa tietoa käytetään mahdollisimman tehokkaasti hyväksi ja sitä pyritään aktiivisesti täydentämään prosessin edetessä. Mallin tavoite on pyrkiä mahdollisimman kattavaan tietoon ja tilannekuvaan. Tutkimuksen näkökulma on informaatioteknologian ja tietoturvajohtajan näkökulma, mutta mallin muodostamisessa on pyritty käytettävyyteen myös muilla toimialoilla.

Asiasanat: riskienhallinta, riskien arviointi, standardit, kyberturvallisuus, tilannekuva, prosessi

ABSTRACT

Kokkomäki, Tuomas; Nortunen, Mika
Trigger – validated risk assessment process model in order to support the organization's success
Jyväskylä: University of Jyväskylä, 2016, 197 p.
Computer Science, Master's Thesis
Supervisors: Salo, Markus; Moilanen, Panu

Risk assessment is part of the competitiveness of the organization. This makes agile and dynamic approaches crucial. The uncertainty and rapid changes in the operating environment also bring opportunities to the organizations. High-quality risk assessment is a way of differentiation from competitors, to ensure the reliability of the organization and through the identification of trends to find new opportunities for future innovations. Increasingly complex world is creating a need for the organizations to take effective measures faster and faster. Organizations must be able to respond quickly to the challenges posed by rapidly changing business environment. The aim of this study was to establish an agile and dynamic process model for risk assessment based on scientific research, risk management standards and interviews of information security officers. Formed process model is intended to help organizations to harmonize risk assessment process at different levels of organization and to provide consistent and comparable material to control the risks and for the background material for future risk assessment of the organization. The study was conducted as a two phase qualitative study, in which the empirical material was collected from a total of six Finnish financial sector organizations. The generated model of risk assessment was validated by presenting it to three security professionals. The generated model offers the opportunity to collect as versatile data as possible. In the background of this model is the idea of identification of threats as well as other possible triggers. The process of this model is aiming to comprehensive identification of these triggers and speeding up, simplification and harmonization of risk assessment in accordance with the organization's strategy. Information and situational awareness are always to some extent incomplete and, therefore, it is important that the risk assessment process is a flexible and dynamic. Model aims to present a risk assessment as a process in which existing data is used as efficiently as possible and it will actively seek complementarity as process progresses. This model's objective is to ensure the widest possible knowledge and situational awareness. The approach if this study is an information technology and information security officer point of view, but the formulated risk assessment model is intended to have usability also outside of this context.

Keywords: risk management, risk assessment, standards, cyber security, situational awareness, process

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Riskienhallinta saa ohjauksen strategian kautta ja määrittää riskien arvioinnin perusteet. Riskien arviointi on osa organisaation kilpailukykyä, jolloin ketterät sekä dynaamiset toimintatavat ovat ratkaisevassa asemassa. Epävarmuus ja nopeat muutokset toimintaympäristössä tuovat mukanaan myös mahdollisuuksia. Laadukas riskien arviointi on keino erottua kilpailijoista, varmistaa osaltaan organisaation luotettavuus ja trendien tunnistamisen kautta löytää uusia mahdollisuuksia tulevaisuuden innovaatioille. Päivittäistä operatiivista toimintaa ja riskien arviointia ei tule erottaa toisistaan. Organisaation strategian toteuttamisen kannalta oikein ajoitetut ja tehokkaat toimenpiteet luovat mahdollisuuden menestykseen. Riskien arviointi on edelleen uhkien tunnistamista, mutta toisaalta uhat tuottavat mahdollisuuksia tulevaisuuden innovaatioille. Innovaatiot taas auttavat organisaatioita liiketoimintansa kehittämisessä.

Organisaatioissa tunnistetaan yleisesti tarve aikaisempien prosessien ketteröittämiselle ja usein myös yksinkertaistamiselle. Mayryn (2016) mukaan organisaatioissa ei tunneta strategiaa. Harva johdosta tai varsinkaan henkilöstöstä tietää organisaation strategian sisältöä tai edes sitä, mihin suuntaan organisaatiota ollaan tulevaisuudessa viemässä. Organisaation johtoryhmästä vain 13 prosenttia tietää mikä on yrityksen suunta, esimiehistä vain 8 prosenttia kykenee kertomaan mitkä ovat yrityksen tärkeät strategiset painopistealueet ja työntekijöistä ainoastaan 2 prosenttia tuntee yhtiön strategian sisältöä. (Mayry 2016). Kyseiset henkilöt tekevät kuitenkin päivittäin töitä organisaation menestyksen turvaamiseksi. Analysoidun riskitiedon jakaminen, toimintaa koskevan tiedon kertyminen ja tästä oppiminen tuottavat organisaatiolle mahdollisuuden valjastaa käyttöön organisaatioiden henkilöstön huonosti tunnistetut voimavarat riskien perusteena olevien tietojen, herätteiden, osalta.

Aikaisempi tutkimus on ollut määrältään melko vähäistä ja se on ollut teknisesti suuntautunutta ja jättänyt ihmis- ja liiketoimintalähtöisen näkökulman varjoonsa. (Adams & Sasse, 1999; Bulgurcu, Cavusoglu & Benbasat, 2010; Siponen & Willison, 2007). Riskien arviointi voidaan nähdä toiminnaksi, jonka kautta organisaatio pyrkii kartoittamaan vahvuuksiaan ja heikkouksiaan. Tämän toiminnan analysoinnin kautta organisaatio myös asemoi itseään toimintaympäristöönsä. Porter (1979) mukaan tätä tehtäessä tulisi välttää staattisia

menetelmiä. Sen sijaan tulisi pyrkiä ottamaan huomioon trendit ja tulevaisuuden mahdollisuudet. Voidaankin kysyä, tukevatko nykyiset riskien arvioinnin menetelmät Porterin 37 vuotta sitten esittämää tarvetta?

Tutkimuksen tavoitteena on muodostaa tieteellisen tutkimuksen, riskien arviointiin soveltuvien menetelmien, kuten standardien ja tutkimuksen aikana suoritettujen haastatteluiden perusteella riskien arvioinnin prosessimalli. Muodostettu prosessimalli auttaa organisaatioita yhtenäistämään riskien arvioinnin prosessia organisaation eri tasoilla ja tuottamaan yhdenmukaista ja vertailukelpoista materiaalia riskien hallitsemiseksi ja tulevan riskien arvioinnin taustamateriaaliksi. Tieto ja tilannekuva ovat aina jossain määrin puutteellisia ja tämän vuoksi on tärkeää, että riskien arvioinnin prosessi on joustava ja dynaaminen. Mallin tavoite on pyrkiä mahdollisimman kattavaan tietoon ja tilannekuvaan. Tavoitteena oli luoda holistinen malli, joka luo riskien arvioinnille uutta arvoa organisaation menestystekijänä. Päätutkimuskysymys on: "*Miten riskien arvioinnin prosessi tulisi suorittaa tietoturvallisuusjohtajien näkökulmasta, jotta se tukisi organisaation menestystä?*" Tutkittavan aiheen käsittelyä kohdeorganisaatioissa pyritään havainnollistamaan apukysymyksellä: "*Miten riskien arvioinnin tulokset vaikuttavat organisaation tietoturvaperiaatteiden laadintaan?*" Tutkimuskysymyksen ja apukysymyksen tehtävä on myös johdattaa tutkimuksen lukijaa organisaation strategian kautta aina strategiaa toteuttaviin toimenpiteisiin kuten tässä tapauksessa tietoturvapolitiikkaan. Riskien arvioinnin tulisi tässä yhteydessä vaikuttaa sekä organisaation strategiseen päätöksentekoon, että käytännön toimenpiteisiin riskienhallitsemiseksi. Kaikkien prosessien tulee lopulta tukea organisaatioiden strategiaa, jota yksityisellä sektorilla kutsutaan liiketoimintastrategiaksi.

Tutkimus toteutetaan kaksivaiheisena laadullisena tutkimuksena, jonka empiirinen materiaali kerätään suomalaisista finanssialan organisaatioista. Muodostettu riskien arvioinnin malli validoidaan esittelemällä se tietoturvallisuuden ammattilaisille.

Tutkimus tehtiin parityönä ja kummatkin tutkijat osallistuivat työn tekemiseen yhtä suurella panoksella. Tehdyn työn osa-alueita on mahdotonta nimetä kummankaan tutkijan tekemäksi, koska työtä on tehty koko prosessin ajan yhteisen päämäärään eteen ja tutkijat ovat jatkuvasti suorittaneet vertaisarviointia toistensa tekemää työtä kohtaan.

1.1 Tutkimuksen tausta

Tutkimuksen taustassa kerromme tutkimuksen tutkimuskysymystä laajemmin ilmiöön liittyviä yhteiskunnallisia näkökulmia. Pääministeri Juha Sipilän hallituksen strategisessa hallitusohjelmassa Suomeen kohdistuvana uhkana mainitaan uudenlaiset turvallisuusuhat, joihin kuuluvat muun muassa kyberuhat. Kasvavat riskit ja uudet uhat edellyttävät koko yhteiskunnalta uudenlaista valmiutta ja varautumista. (Valtioneuvoston kanslia, 2015).

Kyberturvallisuuden toteuttamisen lähtökohta on ollut melko teknologiakeskeinen, eikä sitä ole huomioitu sekä ihmiset ja prosessit sisältävänä koko-

naisvaltaisena käsitteenä. VTT:n laatiman ja Valtioneuvoston kanslian helmikuussa 2016 julkaiseman *Kyberosaaminen Suomessa - Nykytila ja tiekartta tulevaisuuteen* -tutkimuksen mukaan Suomen kyberosaamisessa on neljä kehittämisaluetta. Yksi neljästä osaamisalueesta on monitieteinen kyberturvallisuusosaaminen. Laaja-alainen ja monitieteinen näkökulma on selvästi teknistä näkökulmaa heikommin kehittynyt. VTT:n tutkimuksessa mainitaan erityisesti kyberturvallisuuden osaaminen ihmis- ja käyttäjänäkökulmasta, taloudellinen näkökulma ja oikeudellinen näkökulma. (VTT, 2016). Tutkimus riskien arvioinnista pyrkii osaltaan vastaamaan tunnistettavissa olevaan tarpeeseen laaja-alaisesti ja monitieteisesti hyödyntäen niin tietojenkäsittelytieteellistä-, tietojärjestelmätieteellistä- kuin liiketaloustieteellistätutkimusta ihmis- ja käyttäjänäkökulmista. VTT:n tutkimuksessa informaatioteknologian sekä yhteiskunta- ja kauppatieteenalojen yhdistelmä on ollut Suomen tieteen "merkittävin kasvukomponentti kansainvälisillä tiedejulkaisuilla mitattuna". (VTT, 2016).

Sisäministeriö julkaisi ensimmäisen Valtioneuvoston selonteon sisäisestä turvallisuudesta 19.5.2016. Sisäisen turvallisuuden selonteon mukaan suorituskyvyn kehittämisen kannalta "tilannekuvan merkitys on korostunut ja toimintaympäristö on muuttunut pysyvästi". Selonteon mukaan "toiminnassa on välttämätöntä huomioida muuttuneen ja entistä ennakoimattoman toimintaympäristön muutokset". Toimintaympäristön muutosta ja siihen liittyviä ilmiöitä pyritään ennakoimaan aikaisempaa proaktiivisemmin ja tuomaan tätä kautta saatavat tulokset vaikuttavammin erityisesti määrärahakehys- ja talousarviovalmistelun yhteyteen. Toimintaympäristön muutosnopeuden, ennakoimattomuuden ja käytettävissä olevien resurssien välisen suhteen yhteensovittamisen merkitys korostuu". Selonteon perusteella tilannekuva ja saatavilla olevien resurssien mukainen priorisointi muuttuvassa toimintaympäristössä ovat keskeisiä ohjaavia tekijöitä suorituskyvyn kehittymisen kannalta. (Sisäministeriö, 2016b).

Tutkimuksen kohderyhmänä ovat finanssialan yritykset. Finanssialan yritykset ovat tutkimuksen kohteena erityisen mielenkiintoinen, koska yritysten päivittäinen toiminta tapahtuu pääosin digitaalisessa toimintaympäristössä. VTT:n (2016) tutkimuksen mukaan tietoturvaloukkauksia tehdään jatkuvasti, mutta suurin osa niistä ei tule yleiseen tietoon vallitsevan vaikenemisen kulttuurin vuoksi. Finanssialan yritykset ovat olleet tiedottamisen suhteen varsin avoimia ja havaituista uhista ja hyökkäyksistä on tiedotettu yhteistyössä viranomaisten kanssa. Esimerkiksi palvelunestohyökkäykset ovat saaneet julkisuutta erityisesti pankkeihin kohdistuneiden hyökkäysten ansiosta. (Helsingin seudun kauppakamari, 2015). Kyberturvallisuuskeskuksen suomalaisille tietoturvaloukkausten tutkimiseen keskittyneille tietoturvayrityksille tekemän kyselyn mukaan organisaatioiden oma kyky havaita muun muassa kohdistettuja hyökkäyksiä on heikko. Havainto vastaa myös Kyberturvallisuuskeskuksen kokemuksia ja käsitystä maailmanlaajuisesta tilanteesta. (Viestintävirasto, 2014). Kyberturvallisuus mielletään usein asiaksi, joka koskettaa ainoastaan suurempia organisaatioita. Huoltovarmuuskeskuksen pienille ja keskisuurille yritykselle suuntaama kyberturvallisuusopas kuitenkin toteaa, että nykyään kyberturvallisuus on tärkeä asia jokaiselle yritykselle. Huoltovarmuuskeskus määrittelee kyberuhat tietoturvallisuuden loukkausten aiheuttamiksi uhiksi, jotka

kohdistuvat yrityksen, sen asiakkaiden tai sidosryhmien toimintaan. (Huoltovarmuuskeskus, 2013). Kyberturvallisuus sijoittuu osaksi riskienhallinnan kokonaisuutta. Digitaaliseen toimintaan liittyvä turvallisuus on noussut yhteiskunnassamme yhä merkittävämpään rooliin. Niin yritysten, kuin koko yhteiskunnan toiminta on yhä enemmän riippuvainen digitaalisten palveluiden toimivuudesta.

1.2 Aiemmat tutkimukset

Organisaatioissa tehdään riskien arviointia monella tasolla. Tässä tutkimuksessa riskien arviointia tarkastellaan tietoturvajohtajien näkökulmasta finanssialan organisaatioissa. Aiempaa tutkimusta tarkasteltiin informaatioteknologian kautta, koska maailman kuvataan muuttuvan yhä nopeammin digitaalisuuden seurauksena (Mattila, 2007; Limnéll, Majewski & Salminen, 2014). Teoreettisen viitekehyksen muodostamisessa hyödynnettiin tieteellistä kirjallisuutta pääosin tietojärjestelmätieteen alalta. Tutkimuksen rajaus on kuvattu tarkemmin johdannon alaluvussa "Tutkimuksen tavoitteet ja näkökulma" (1.3).

Tietojärjestelmien turvallisuudesta ei ole tehty merkittävästi tutkimusta. Julkaisujen määrä on aiheen tärkeydestä huolimatta vähäinen (Bulgurcu ym., 2010). Siponen ja Willison (2007) toteavat tietojärjestelmien turvallisuuden tutkimuksen olevan aliedustettuna suurimmissa kansainvälisissä tutkimusjulkaisuissa. Siposen ja Oinas-Kukkosen (2007) mukaan tietoturvallisuuden tutkimus on pääasiassa keskittynyt teknisiin ongelmiin ja tutkimukset ovat olleet matematiikkaan ja matemaattiseen- tai filosofiseen logiikkaan perustuvia. Muiden kuin pelotevaikutukseen (deterrence theory) perustuvien keinojen käyttöä tietoturvallisuuden loukkausten ehkäisyssä on tutkittu vähän. Siponen ym. (2007) mukaan motivaatioon tai etiikkaan perustuvien keinojen käyttö on tutkittu pääosin vähän. Adamsin ja Sassen (1999) mukaan suurin osa aikaisemmasta tutkimuksesta keskittyy teknisten järjestelmää turvaavien mekanismien tutkimiseen, mutta ei kyseisten mekanismien käytettävyyteen.

Edellisessä kappaleessa kuvattiin yleisesti tietojärjestelmien turvallisuuden tutkimusta. Seuraavaksi kuvataan tarkemmin keskeiset tieteelliset kirjallisuusviitteet, joihin tutkimus perustuu. Alla olevat kuvaukset eivät ole järjestetty julkaisun merkityksen mukaisesti vaan kuvaamaan julkaisujen syy-yhteyttä tutkimuksen aiheeseen.

Porterin (1979) mukaan yrityksen asemoinnissa toimintaympäristöön tulee välttää käyttämästä staattisia arviointimenetelmiä, jotka eivät ota huomioon toimialan trendejä ja tulevaisuuden mahdollisuuksia. Arvioinnin tulee perustua kokonaisarvioon toimialan tilasta ja kehityksestä. Vaikka yrityksen strategia perustuu tarkkoihin analyyseihin, jotka johto kokoaa yhteen, ei tarkoituksena ole soveltumattomien tiukasti määriteltyjen arviointimenetelmien käyttö. (Porter, 1979). Tämä tutkimus pyrkii osaltaan vastaamaan tähän haasteeseen. Tutkimuksessa muodostettavan mallin tavoitteena on ohjata organisaation riskienhallintaa aktiivisempaan ja aloitteellisempaan suuntaan siten, että toiminnan analysoinnin kautta organisaatio kykenee entistä paremmin hahmottamaan

toimintaympäristön kehittymisen suunnan pelkän vallitsevan tilanteen havainnoinnin sijaan.

Rasmussenin (1997) mukaan riskienhallintaan osallistuvat sosio-teknisissä järjestelmissä useiden eri alojen ammattilaiset, mutta tutkimusta tehdään pääsääntöisesti erillään muista toimijoista yhden tieteenalan sisällä. Tutkimus tulisi kuitenkin laajentaa poikkitieteelliseksi, jolloin kaikki yhteiskunnan toimijat voitaisiin ottaa paremmin huomioon. Tämä ei kuitenkaan tarkoita, että olisi tarvetta ainoastaan soveltavalle tutkimukselle. Rasmussen ehdottaa perustutkimusta muun muassa ihmisille luontaisen päätöksenteon toimintatavoista muutoksen ja paineen alla, vaaraa aiheuttavien tapahtumien luokittelun ja näiden hallinnan sekä yhteiskunnan toimijoiden välisen yhteistoiminnan osalta. (Rasmussen, 1997). Tämä tutkimus pyrkii kehittämään riskienhallintaa ja -arviointia entistä monitieteellisempään suuntaan siten, että riskien arviointi ja analysointi tapahtuisi enemmän organisaatiota osallistavalla tavalla hyödyntäen laajemmin koko organisaation osaamisen rajatun turvallisuushenkilöstön lisäksi.

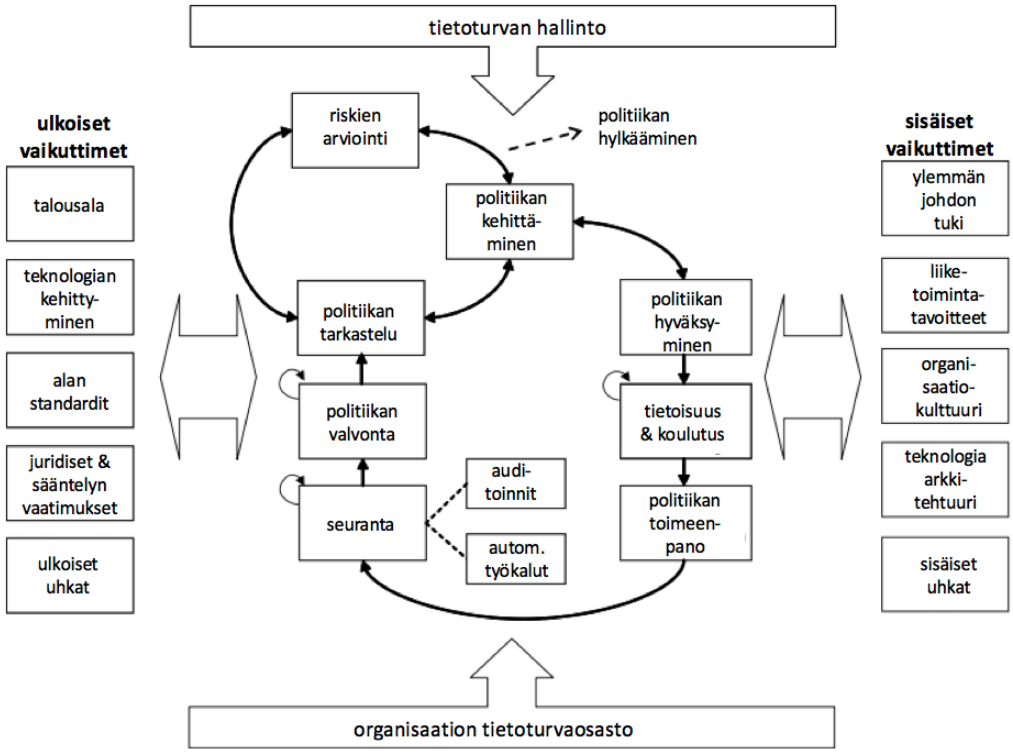
Soomro, Shah ja Ahmed (2016) mukaan tietoturvallisuuden johtaminen tarvitsee kokonaisvaltaisempaa eli *holistista* näkemystä. Tieto- ja viestintäteknologian (ICT) rajattomat mahdollisuudet ovat tuoneet organisaatioille tarpeen turvata omaisuuttaan ja liiketoimintaansa entistä paremmin. Johtamisella on yleisesti vaikutusta kaikkiin liiketoiminnan tapahtumiin. Tietoturvallisuus on johtamis- ja liiketoiminnallinen ongelma, joten ylimpien johtajien tulee olla tietoisia tietoturvallisuuspolitiikoiden kehittämisestä ja täytäntöönpanosta. (Chang & Ho, 2006; Soomro ym., 2016). Soomro ym. (2016) mukaan organisaation johdon sitoutumisella informaatioturvallisuuden kehittämiseen ja toteuttamiseen on huomattava vaikutus sen laatuun. Soomro ym. (2016) tarjoavat artikkelissaan myös kattavan listauksen vuosina 2004 - 2014 tehdyistä informaatioturvallisuuteen ja sen johtamiseen liittyvistä artikkeleista. Kokonaisvaltaisen näkemyksen lisäämiseksi tässä tutkimuksessa muodostettava riskien arvioinnin malli pyrkii yhdenmukaistamaan organisaatioiden tapoja suorittaa riskien arviointi. Arvioinnin tulosten ollessa paremmin yhdenmukaisia ja vertailtavia on organisaatiolla mahdollisuus muodostaa kokonaisvaltaisempi näkemys turvallisuuden tilanteesta. Tätä kautta turvallisuuden johtaminen voi saavuttaa paremman tuloksen.

Shameli-Sendi, Aghababaei-Barzegar ja Cheriet (2016) ovat muodostaneet yhteensä 125:n informaatioturvallisuuden riskien arviointiin liittyvän tutkimuksen synteesinä uuden riskien arvioinnin taksonomian. Tämän luokittelun avulla he pyrkivät vastaamaan organisaatioiden haasteeseen sopivan riskien arvioinnin menetelmän valinnassa. Shameli-Sendi ym. (2016) näkevät vanhan taksonomian (laadullinen, määrällinen tai semi-määrällinen) liian rajoittuneena verrattuna nykyajan nopeasti muuttuvaan toimintaympäristöön. He pyrkivät tarjoamaan tutkimuksessaan uuden ja kattavamman luokittelun, jonka avulla organisaatioiden on helpompi valita oma näkökulmansa riskien arvioinnin toteuttamiseen. Tutkijat tuovat selkeästi ilmi taksonomian eri elementtien vahvuudet ja heikkoudet sekä listaavat olemassa olevien riskien arvioinnin menetelmien näkökulmia. Shameli-Sendin ym. (2016) tutkimus sisältää lisäksi suuren määrän muita viittauksia tietojärjestelmiä ja -turvallisuutta käsitteleviin tutkimuksiin. (Shameli-Sendi, Aghababaei-Barzegar & Cheriet, 2016). Tässä tutki-

muksessa muodostettavaa riskien arvioinnin mallia pyritään tarkastelemaan myös Shameli-Sendi ym. (2016) muodostaman taksonomian ja sen arvioinnin kautta.

Baskerville (1991) on tutkimuksessa *"Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security"* käynyt läpi riskianalyysin mahdollisia vaihtoehtoisia käyttötapoja. Baskervillen mukaan riskianalyysi on menetelmänä väärin ymmärretty. Menetelmän kehittäminen kvantitatiivisesta, tilastoihin perustuvasta menetelmästä kohti organisaation johdon ja turvallisuusasiantuntijoiden kommunikointimenetelmää on perusteltua. (Baskerville, 1991). Vaikka Baskerville suhtautuukin riskien arviointiin ja analysointiin kriittisesti hän tunnustaa sen käytettävyyden ennen kaikkea kommunikaation välineenä johdon ja turvallisuusasiantuntijoiden välillä. Baskerville kuvaa artikkelissaan myös vaihtoehtoisia menetelmiä riskianalyysille. Näitä ovat esimerkiksi ammattilaisen mielipide (certified professional opinion) ja tilastollisten menetelmien käyttö. Baskerville tiedostaa riskien arvioinnin ja analysoinnin merkityksen organisaatioiden toiminnan kannalta, mutta hänen mukaansa siihen liittyy käytetystä menetelmästä riippumatta epäonnistumisen vaaroja. (Baskerville, 1991). Tämä tutkimus pyrkii muuttamaan riskien arvioinnin toteuttamista siten, että sitä suorittavien organisaatioiden olisi mahdollista saada sen tuloksena luotettavampia tuloksia. Baskervillen esittämät vaihtoehdot luovat osaltaan pohjaa tässä tutkimuksessa muodostettavalle riskien arvioinnin mallille.

Knapp, Morris, Marshall ja Byrd (2009) ovat kehittäneet tietoturvapolitiikan muodostamiseen kuvion 1 mukaisen prosessimallin.



KUVIO 1 Tietoturvapolitiikan muodostamisen prosessimalli (Knapp ym., 2009)

Malli on muodostettu informaatioturvallisuuden ammattilaisille suunnatun kyselyn tulosten perusteella ja se on lisäksi validoitu kyselyyn aiemmin osallistumattomien asiantuntijoiden avulla kahdessa eri vaiheessa. Tämän lisäksi malli on arvioitu arvostetun informaatioturvallisuuskongressin yhteydessä. Prosessimalli esittää tietoturvapolitiikan laatimiseksi kattavan mallin, joka pyrkii huomioimaan tietoturvapolitiikan laatimiseen vaikuttavat tekijät mahdollisimman kattavasti. (Knapp ym., 2009).

Knapp ym. (2009) korostavat mallin useista kohdista viittä, joille heidän mukaansa on olemassa tutkimuksen materiaalista esiin nousseiden käytännön kokemusten lisäksi runsaasti tukea alan kirjallisuudesta. Knappin ym. (2009) malli esittää tietoturvapolitiikan laatimisen iteratiiviseksi prosessiksi, jota täytyy toteuttaa aktiivisesti myös tietoturvapolitiikan valmistumisen jälkeen. Se on kehämäinen prosessi, jossa vaiheita toistetaan ja tarvittaessa tehtyjä suunnitelmia ja päätöksiä arvioidaan uudelleen. He korostavat organisaation kouluttamista ja tietoisuuden lisäämistä sekä sitä, että muodostetun tietoturvapolitiikan käyttöönottoon panostetaan riittävästi. Ilman käytännön täytäntöönpanoa tietoturvapolitiikan olemassaololla ei ole mitään merkitystä. He painottavat myös organisaation ylimmän johdon roolia tietoturva-asioiden itsessään tulisi olla ennen kaikkea hallinnon asia, ei erillinen tekninen yksityiskohta. Tietoturvapolitiikan laatimiseen, kehittämiseen ja ylläpitämiseen liittyy varsinaisen prosessin lisäksi useita sisäisiä ja ulkoisia vaikuttimia, joiden olemassaolo tulisi tiedostaa. Näitä vaikuttimia ovat esimerkiksi ulkoiset uhkat, kuten hakkerit. (Knapp ym., 2009).

Knappin ym. (2009) malli on saanut osakseen myös kritiikkiä. Alshaikh, Maynard, Ahmad ja Chang (2015) kritisoivat kyseistä mallia liiasta yleisyydestä. Heidän mukaansa Knappin ym. prosessimalli ei tarjoa riittävästi kuvauksia tietoturvapolitiikan johtamisen käytäntöihin. (Alshaikh ym., 2015).

Knapp ym. (2009) muodostama malli tietoturvapolitiikan laatimiseen soveltuu myös viitekehykseksi riskien arvioinnin toteuttamiseen. Mallissa esitetyt sisäiset ja ulkoiset tekijät kuvaavat kattavasti myös riskien arvioinnissa huomioon otettavia vaikuttimia. Myös riskien arvioinnin ja sitä seuraavan toiminnan (mallissa tietoturvapolitiikka) sekä edellä mainittuja seuraava vaikutuksen arvioinnin sykli ovat sovellettavissa muuhunkin riskien arvioinnin tulosten vaikutusten alla olevaan toimintaan, kuin tietoturvapolitiikan laatimiseen.

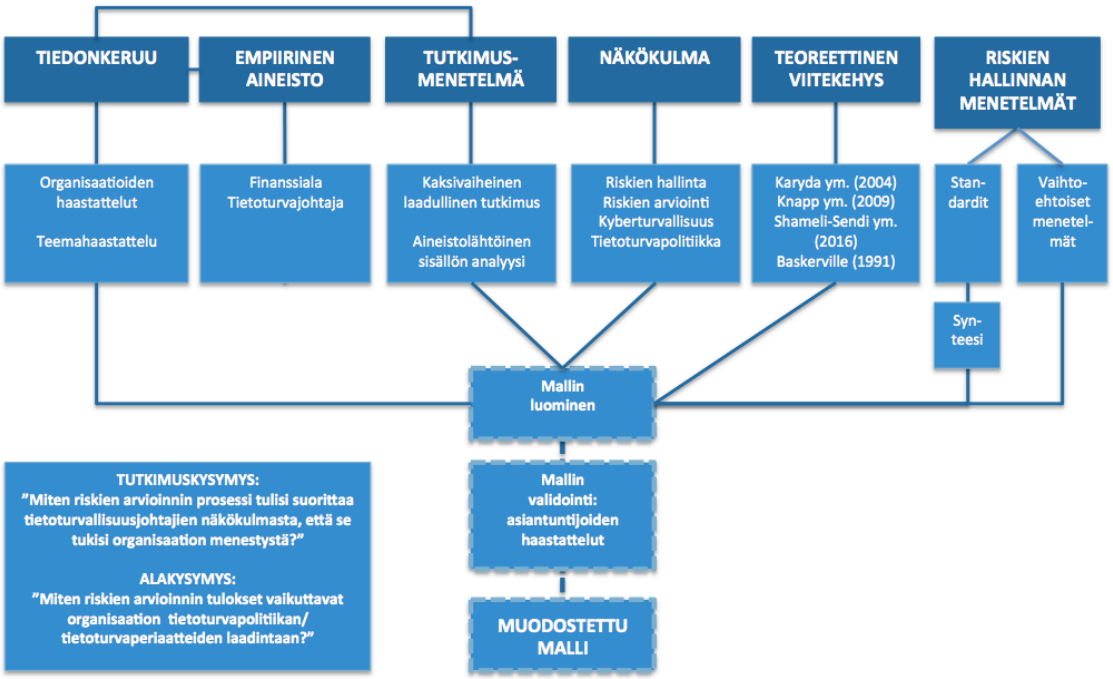
1.3 Tutkimuksen tavoitteet ja näkökulma

Tutkimuksen aiheen valinnan ja toteutuksen taustalla oli halu löytää uusia käytännön hyötyä tuottavia innovaatioita. Tutkijat eivät halunneet tehdä pro gradu -tutkielmaa ainoastaan suoritusmerkinnän vuoksi, vaan halusivat saada aikaiseksi jotain uutta ja innovatiivista. Lähtökohta on varsin kunnianhimoinen, mutta Hardyn (1940) ja myöhemmin Hakalan (2002) mukaan kaikki maailman parhaat tieteen saavutukset ovat “kunnianhimon synnyttämiä”. Sitran (2016) mukaan tulevaisuuden toimintaympäristö vaatiikin sekä kunnianhimoisia tavoitteita että ketteriä toimintatapoja.

Siposen (2015) mukaan tieteellisen tutkimuksen taustalla ja tutkimusten motivaation kuvailussa on usein pyrkimys käytännön hyötyyn, mutta tutkimukset eivät usein lopulta tuota varsinaista käytännön hyötyä. Tässä pro gradu -tutkielmassa pyrittiin kaksivaiheisen laadullisen tutkimuksen kautta löytämään näkemys uusien innovaatioiden tarpeesta riskien arvioinnin prosessissa ja mahdollisista keinoista uusien innovaatioiden kehittämiseksi. Toisessa vaiheessa pyrittiin vastaamaan havaittuun tarpeeseen laatimalla käytännön hyötyä tuottavan mallin. Laadittu malli tulee nähdä ennen kaikkea uusien innovaatioiden mahdollistajana. Organisaatiolla on liiketoimintastrategia, jota kaiken muun toiminnan tulee tukea. Riskien arvioinnin tulee näin ollen tukea organisaation strategiaa ja tuottaa organisaatiolle menestymisen eväitä.

Tutkijoiden omaa kiinnostusta ohjasivat työelämässä hankitut kokemukset organisaatioiden tarpeesta tehdä prosesseista ketterämpiä. Ketteryys tarkoittaa usein myös useiden osittain päällekkäin suoritettavien prosessien yhdenmukaistamista. Tutkimuksen tavoitteena oli luoda malli, jota organisaatiot voivat käyttää omien organisaatiokohtaisten riskien arvioinnin menetelmien laadinnassa. Tietylle organisaatiolle tai toimialalle laadittu malli olisi rajannut mahdollisesti mallin laajempaa käytettävyyttä. Näin ollen tutkimuksen syvempi idea toimintojen ketteryydestä ja yhdenmukaistamisesta olisi kärsinyt. Tutkimuksen ulkopuolelle on tietoisesti rajattu yksityiskohtaisen riskien arvioinnin menetelmän laatiminen tutkimus-ekonomisista syistä. Formaalin, määrämuotoisen menetelmän laadintaan tarvittaisiin organisaatioon liittyvää yksityiskohtaista tietoa.

Puusan ja Juutin (2011) mukaan teoreettinen viitekehys muotoutuu tutkijoiden perehtyessä laajasti alan teoksiin ja aikaisempiin tutkimuksiin, jolloin tutkijoiden ymmärrys tutkittavaa aihetta kohtaan syventyy. Teoreettiseen viitekehykseen valitaan tutkimuksen pääkäsitteet ja perehdytään pääkäsitteiden erilaisiin merkityksiin. Tutkijoiden tulee ymmärtää huolellisen tarkastelun kautta ovatko määritellyt pääkäsitteet keskeisimpiä rakennusaineita, joiden varaan tutkimus rakennetaan. (Puusa & Juuti, 2011). Puusan ja Juutin (2011) mukaan käsitteiden määrittelyn ohella tutkija syventää esiymmärrystään valitusta kohdeilmiöstä ja pyrkii löytämään työllensä teoreettisen perustelun. Teoreettinen perustelun löytäminen kuvaa mitä ilmiöstä jo tiedetään ja millaiset näkökulmat ovat jääneet huomioimatta. Tutkijan tulee toisin sanoen osoittaa työlleen niin sanottu tutkimusaukko, johon työ on mahdollista asemoida. Teoriakatsaus auttaa tutkijaa tekemään perusteltuja rajauksia ja päättämään tutkimuksen näkökulmasta. (Puusa & Juuti, 2011). Kuviossa 2 esitellään tutkimuksen rajaukset, näkökulma ja viitekehys:



KUVIO 2 Tutkimuksen rajaukset, näkökulma ja viitekehys

Tutkimukseen valittiin tietoturvallisuusjohtajien näkökulma, koska pro gradu -tutkielmaan kerätyn tiedon perusteella tulevaisuudessa digitalisaatio ja tätä kautta tapahtuva organisaatioiden toimintaympäristön muutos vaativat erittäin pitkälle vietyjä digitaalisen turvallisuuden ratkaisuja. Kyberturvallisuuden tärkeyttä kuvaa Sitran maailmaa muuttavista megatrendeistä laatima muistio, jossa teknologia, keskinäisriippuvuus ja jännitteinen maailma ovat kuvattu kolmeksi keskeiseksi muutosvoimaksi (Sitra, 2016). Tavoitteena oli, että pro gradu -tutkielmaprosessin aikana kehitettyä mallia ja sen osia voidaan aidosti käyttää osana organisaatioiden omia prosesseja. Mallin käyttömahdollisuudet eivät rajaudu tutkielman aiheen mukaisesti ainoastaan riskien arviointiin tai finanssialaan, vaan mallia on mahdollista käyttää toimialasta ja prosessin tyypistä riippumatta.

Tutkimuksen kohderyhmäksi valittiin suomalaisia finanssialan organisaatioita niin yksityiseltä kuin julkiselta sektorilta. Kohderyhmän valintaa ohjasi erityisesti toimiala ja sen riippuvuus digitaalisesta turvallisuudesta ja yhteistyöstä sekä sen globaali toimintaympäristö. Tarkoitus on tuoda toimialalta, jossa digitaalisuus ja riskien arviointi ovat toiminnan kannalta kriittisiä menestystekijöitä, hyviä käytänteitä myös aikaisemmassa kehitysvaiheessa oleviin organisaatioihin. Tulevaisuudessa yksi tärkeimmistä menestystekijöistä on yhteistyö yli organisaatio- ja toimialarajojen. Tutkimukseen osallistuneet organisaatiot finanssialalta kertoivat avoimesti omista käytänteistään epäonnistumiset mukaan lukien.

Tutkimuksen tavoitteeseen pääsemiseksi selvitettiin, miten organisaatioiden suorittama riskien arviointi tapahtuu ja mikä vaikutus sillä on organisaation menestykseen tietoturvallisuusjohtajien näkökulmasta. Varsinaisen tutkimuskysymyksen apuna käytettiin kysymystä siitä, miten riskien arviointi käy-

tännössä vaikuttaa organisaatioiden tietoturvaperiaatteiden muodostumiseen. Tutkimus tapahtui kartoittamalla organisaatioiden käytännön tavat toteuttaa riskien arviointi yhdistäen se olemassa oleviin riskien arvioinnin menetelmiin, standardeihin ja kirjallisuudesta löytyvään tietoon. Yhdistettäessä organisaatioiden käytännön kokemukset ja toimintatavat tutkimuksen teoriaan luotiin malli, jossa yhdistettiin olemassa olevien standardien käytänteet sekä organisaatioiden hyväksi havaitsemat tavat toteuttaa riskien arviointi ja konkretisoida se tietoturvaperiaatteiden muodossa. Tietoturvaperiaatteet (tai tietoturvapolitiikka) otettiin osaksi tutkimusta, koska se on konkreettisesti organisaatioista löytyvä asiakirja, jolla on tarkoitus vähentää organisaatioon ja sen tietojärjestelmiin kohdistuvia riskejä. Riskien arviointi luo pohjan riskienhallinnalle ja sen tuloksena laadittaville ja toteutettaville keinoille, joilla pyritään vaikuttamaan riskeihin. Tutkimuksessa pyritään vastaamaan seuraavaan kysymykseen:

Miten riskien arvioinnin prosessi tulisi suorittaa tietoturvallisuusjohtajien näkökulmasta, jotta se tukisi organisaation menestystä?

Tutkimuksen tarkoituksen selkeyttämiseksi ja tutkimuksen kannalta soveltuvien haastateltavien rekrytoinnin helpottamiseksi tutkimusta lähestyttiin seuraavan apukysymyksen kautta:

Miten riskien arvioinnin tulokset vaikuttavat organisaation tietoturvapolitiikan/tietoturvaperiaatteiden laadintaan?

Kysymystä lähestyttiin olemassa olevien tietoturvaperiaatteiden/-politiikan kautta kuvaamalla, miten tietoturvaperiaatteet organisaatioissa laaditaan. Tutkimus haluttiin liittää tutkimuksen moniulotteisen aiheen vuoksi organisaatioissa konkreettisesti löytyvään turvallisuustyökaluun eli tietoturvapolitiikkaan. Tietoturvapolitiikka tai -periaatteet perustuvat organisaation omaan strategiaan ja liiketoimintaympäristön luomiin tarpeisiin. Tästä syystä tietoturvapolitiikka sopii erinomaisesti apukysymykseksi haastateltavien rekrytointia ja keskusteluyhteyden avausta ajatellen. Tutkimuksen aikana siirryttiin vaiheittain strategian kautta tapahtuvasta ohjauksesta, riskienhallinnan kautta riskien arviointiin, jonka lopulta tutkimustiedon perusteella tulisi vaikuttaa tietoturvapolitiikkaan. Tutkimukseen valitut teemat ja käsitteiden avaaminen ovat luonteva polku strategiasta konkreettisiin toimenpiteisiin.

Tutkimuksen teoreettisen viitekehyksen, neljän standardin synteesin, vaihtoehtoisten menetelmien, kirjallisuuden sekä suomalaisissa finanssialan organisaatioissa tapahtuvien ensimmäisen vaiheen haastattelujen pohjalta laadittu malli yhdistää riskien arviointiin sekä tieteellistä että käytännön tietoa. Toisessa vaiheessa muodostettu riskien arvioinnin prosessimalli esiteltiin kyberturvallisuuden asiantuntijoille. Asiantuntijoiden valinnassa painotettiin yksittäisen organisaation rajat ylittävää osaamista ja asiantuntijuutta. Asiantuntijoilta kysyttiin muun muassa, olisivatko he valmiita käyttämään mallia omassa organisaatiossaan tai teoreettisesti kuvitellussa organisaatiossa. Asiantuntijoiden palautteen perusteella malliin tehtiin tarvittavat muutokset.

2 RISKIEN ARVIOINTI

Riskin käsitteen määritteleminen on melko hankalaa. Riski määritellään eri tieteenaloilla ja edelleen tieteenalojen sisällä vaihtelevasti. Tieteellisten julkaisujen ulkopuolella organisaation toimintaympäristö määrittää riskin käsitettä. Douglas (1990) on kuvannut riskin määritelmää tutkimuksen julkaisuajankohdan sekä ajan ja tilan suhteen. Esimerkiksi 1700 -luvulla riski liittyi uhkapeleihin ja 1800 -luvulla merenkäynnin vakuutustoimintaan. 1900 -luvulla riskiä tutkittiin laajemmin talouteen liittyen. 2000 -luvulla riskit nähdään yleisesti negatiivisena tekijänä toiminnassa. (Douglas, 1990; Gerber & Von Solms, 2005). Tekniikassa ja teollisuudessa riskit ovat kasvaneet. Toisaalta toisilla aloilla riskit ovat jopa vähentyneet. Tämä kuvaa riskit käsitettä erinomaisesti. Riski käsitellään ajan ja paikan suhteen. Riskin käsite on Douglasin mukaan siirtynyt poliittiseen keskusteluun, jolloin sen painoarvo teknisin laskutoimituksin tehtävissä todennäköisyyksien määrittämisissä on vähentynyt. (Douglas, 1990). Suomen Pankki jakaa pankkitoiminnan riskit valuuttariskiin, korkoriskiin, luottoriskiin, likvidiysriskiin ja operatiiviseen riskiin. (Suomen Pankki, 2016). Tutkimuksessa riskien arviointia lähestytään finanssialan organisaatioiden tietoturvajohtajien näkökulmasta keskittyen erityisesti operatiivisiin riskeihin ja vielä tarkemmin tietoturvallisuuden riskeihin. Youngin (2009) mukaan organisaatiot erityisesti liikemaailmassa ovat riippuvaisia informaatioteknologiasta, joten tietoturvallisuuden arvioinnissa riskiperusteinen lähestymistapa on yksi parhaista tavoista arvioida turvallisuuden tasoa.

Riskien arviointi sijoittuu osaksi laajempaa riskienhallinnan viitekehystä. Yleisesti riskienhallinnan voidaan tulkita tarkoittavan seurauksiltaan merkittävien kielteisten tapahtumien (riskien) hallittua määrittelyä sekä niihin varautumista. Merkittäviksi riskeiksi voidaan määritellä ne, jotka vaikuttavat organisaation päätöksentekoon. Riskienhallinta on prosessi, joka nivoutuu toimintoihin, joiden riskejä käsitellään. Ahteensuun (2008) mukaan ”riskit ovat vahingonuhkia, joihin yksilö liittää tietyn tapahtuman tai asiaintilan esiintymiseen negatiivisen arvo-ominaisuuden.” Riskien arvioinnin tuloksena pyritään saavuttamaan uhkiin liittyvää tietoa, joka on niin luotettavaa, kuin mahdollista. Tätä tietoa käytetään päätöksenteon perustana. (Ahteensuu, 2008). Riski koostuu tapahtuman todennäköisyydestä ja sen seurausvaikutuksista. Riskin suu-

ruus voidaan määritellä sen arvioidun todennäköisyyden ja vaikutuksen tulona. Tätä kautta riskit voidaan asettaa järjestykseen ja niitä voidaan vertailla. (Sisäministeriö, 2016a).

VTT:n (2003) mukaan organisaation riskit eivät aina löydy yhtä menetelmää käyttämällä. Esimerkiksi teollisuudessa käytetään useita menetelmiä tarkasteltavan kohteen mukaan. Yhtä menetelmää saatetaan käyttää karkean tason tunnistusmenetelmänä, toista menetelmää teknisen järjestelmän tarkasteluun ja kolmatta menetelmää ihmisten työtehtävien tarkasteluun. (VTT, 2003). Riskiä arvioitaessa riski otetaan tavallisesti huomioon vain suppeasti sen aiheuttaman vahingon tai odotetun vahingon perusteella. (Bodin, Gordon & Loeb, 2008). Baskervillen (1991) mukaan riskienhallinnan menetelmät ovat alttiita turhille ja kustannuksia aiheuttaville toimille. Toisin sanoen, jos uhat arvioidaan ainoastaan tieteellisin perustein, tapahtumiin saatetaan ylireagoida. (Baskerville, 1991).

Tietoturvallisuuden kehitys on nopeaa ja tästä syystä useissa tutkimuksissa (mm. Baskerville, 1991; Bandyopadhyay, Mykytyn & Mykytyn, 1999); Gerber & Von Solms, 2005) ehdotetaan suurempien kokonaisuuksien huomioimista riskien arviointia laadittaessa. Virhe voi esiintyä sosio-teknisissä järjestelmissä niin ihmisen toiminnan kuin tekniikan toimintahäiriön seurauksena (Turner, 1978). Tästä johtuen riskien arvioinnissa täytyy huomioida sekä tekniset että sosiaaliset tekijät. Hamiltonin (2015) mukaan finanssialalla, kuten vakuutustoiminnassa riskienhallinta perustuu tilastollisiin menetelmiin tietyltä näyteryhmältä. Vakuutuksen myöntäjä haluaa tietää vakuutettavan mahdolliseen riskikäyttäytymiseen liittyvät asiat. Vakuutuksenmyöntäjä määrittää vakuutuksen hinnan arvioimalla tämän riskin toteutumiseen mahdollisesti johtavia ominaisuuksia. Yksittäisen vakuutuksenottajan profiilia verrataan otantaan vastaavista vakuutuksenottajista. (Hamilton, 2015). Vastaavaa kattavaa tilastoa ei ole saatavissa esimerkiksi kyberturvallisuuden riskien arviointiin liittyen. Tästä johtuen tutkimuksessa pyritään selvittämään organisaation käytäntöä ja verrata tätä olemassa olevaan tutkimustietoon ja standardeihin.

Riskien arvioinnin määritelmä tarkentuu edelleen tämän pro gradu -tutkielman edetessä. Seuraavaksi käsitellään muun muassa riskien arviointia ohjaavia tekijöitä, jolloin riskien arvioinnin tarkoitusta kyetään kuvaamaan syvemmin. Tutkimuksessa käsitellään myöhemmin neljää standardia, joista muodostettiin synteesi. Kyseisissä standardeissa on myös standardikohtaisesti määritelty riskienhallinnan ja riskien arvioinnin käsitteet.

2.1 Riskien arviointia ohjaavat tekijät

Riskien arviointia ohjaavista tekijöistä tarkastellaan seuraavaksi organisaation strategiaa, riskienhallintaa, organisaatiokulttuuria ja tietoturvapolitiikkaa riskien vähentämisen keinona.

2.1.1 Strategia

Strategia kuvaa niitä keinoja, joilla organisaatio aikoo tuottaa arvoa osakkeenomistajille, asiakkailleen ja kansalaisille (Kaplan & Norton, 2004). Strategiat syntyvät joko suunnitteluprosessin kautta tai kehittyen vähitellen organisaation erilaisten toimivien yksiköiden välisessä vuorovaikutuksessa (Porter, 1980). Porterin mukaan strategia on yrityksen asemointia toimintaympäristöön ja kilpailuedun saavuttamista tämän asemoinnin kautta. Asemointi tapahtuu havainnoimalla oman toimintaympäristön muutoksia ja vastaamalla toimintaympäristön tarpeisiin. (Porter, 1980). Porterin (1979) mukaan yrityksen tulee ymmärtää kilpailua toimintaympäristössään. Porter arvioi markkinoiden kiinnostavuutta viiden vaikuttavan voiman kautta: kuluttajien markkinavoiman, tuottajien markkinavoiman, uusien kilpailijoiden uhan, korvaavien hyödykkeiden uhan, sekä toimialan kilpailun tason suhteen (Porter, 1979). Strategia ohjaa muun muassa riskienhallintaa, jonka osa riskien arviointi on. Riskien arvioinnin on näin ollen mahdollista olla osa strategian muutosvoimia. Porterin näkemys on, että painopisteen tulee olla kuitenkin strategian suunnitteluprosessissa. (Porter, 1980). Kirjallisuudessa on esitetty (mm. Mantere, Tienari, Vaara & Välikangas, 2008) strategiaa Porterin näkemyksestä poiketen parhaimmillaan johdon ja henkilöstön välisenä yhteisenä kielenä. Menestyksekästä liiketoimintaa rakennetaan Mantere ym. (2008) mukaan ennen kaikkea merkityksellisissä ympäristöissä. Strategia on ajattelua ja puhetta, johon moni osallistuu ja jonka kautta monet elävät ja kehittyvät ajassa ja ympäristössä. Strategialla on siis merkitystä organisaation kehittymiselle, hyvinvoinnille, johtamiselle ja loppujen lopuksi yhä paremmille tuotteille, palveluille ja kannattavuudelle. (Mantere ym., 2008).

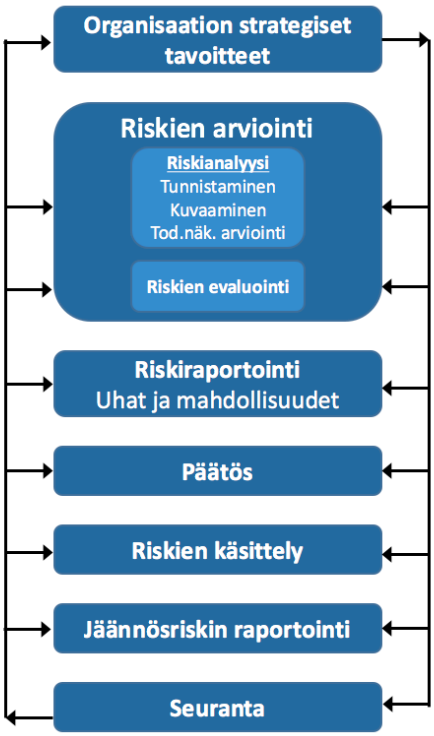
Organisaation toimintojen tulee tukea organisaation strategiaa. Strategian tunteminen organisaation kaikilla tasoilla on erittäin tärkeää, mutta Maarika Mayryn (2016) tekeillä olevan väitöskirjatutkimuksen mukaan organisaation johtoryhmästä vain 13 prosenttia tietää mikä on yrityksen suunta, esimiehistä vain 8 prosenttia kykenee kertomaan mitkä ovat yrityksen tärkeät strategiset painopistealueet ja työntekijöistä ainoastaan 2 prosenttia tuntee yhtiön strategian sisältöä. Tutkimuksessa oli mukana 150 erikokoista organisaatiota ja vastaajina lähes 10000 työntekijää organisaatioiden eri tasoilta. (Mayry, 2016). Johtajien tulee kyetä kuvaamaan strategiaa, jotta he voivat viestiä siitä toisilleen ja henkilöstölle. Strategian tulisi muun muassa ohjata organisaation resursseja. Resurssien tulee kohdistua oikein, jotta organisaatio pystyy toteuttamaan strategiaa muuttuvassa ympäristössä. (Kaplan & Norton, 2004). Mattilan (2007) mukaan muutos on yritysten toimintaympäristöä leimaava pysyvä ilmiö. Kyky sopeutua muutokseen on nostettu niin organisaation, johtajan kuin työntekijän menestymisen edellytykseksi. Mattilan (2007) kuvailema sopeutuminen yhdistetään usein ketteriin toimintamalleihin. Dozin ja Kososen (2007) mukaan ketteryyden luomisen ja ylläpitämisen kolme keskeistä ominaisuutta ovat strateginen herkkyys, yhteinen sitoutuminen ja resurssien joustava käyttö. Tämä edellyttää kuitenkin avointa strategiaprosessia ja pitkäjänteistä työtä tavoitteiden saavuttamiseksi. Resurssien joustavuuden osalta henkilöstön ja tiedon liikutel-

tavuus sekä toiminnan modulaarisuus edesauttavat ketterien toimintatapojen kehittymistä.

2.1.2 Riskienhallinta

Riskienhallinnan käsitettä määriteltäessä tulee ottaa huomioon määrittelyn asiayhteys. Riskienhallinnalla voi olla toimijoille erilainen merkitys riippuen siitä, millä alalla organisaatio tai henkilö toimii (Lanne, 2007). Riskienhallinnan yleispätevä luokittelu on haastava tehtävä, koska selitykset perustuvat usein tiettyihin oletuksiin (Harms-Ringdahl, 2004). ISO määrittelee riskienhallinnan koordinoiduiksi aktiviteeteiksi, joiden avulla organisaation toimintaa pyritään ohjaamaan ja hallitsemaan riskeihin liittyen. (ISO Guide, 2009).

Riskienhallinta on keskeinen osa minkä tahansa organisaation strategista johtamista (IRM, 2002). Se on monimutkainen prosessi, joka edellyttää koko organisaation sitoutumista (NIST, 2011). Riskienhallinta on prosessi, jossa organisaatiot käsittelevät riskit ja liittävät ne toimintaansa tavoitteenaan saavuttaa toimintaansa hyödyttävää etua. Hyvän riskienhallinnan tavoitteena on näiden riskien identifiointi ja käsittely. Riskienhallinta jäsentää näiden tekijöiden vaikutusta organisaation toimintaan. Onnistuessaan riskienhallinnan prosessi lisää organisaation menestymismahdollisuuksia ja vähentää epäonnistumisen todennäköisyyttä. Riskienhallinnan tulisi olla jatkuva ja kehittyvä prosessi, joka läpäisee kaikki organisaation prosessit. Riskienhallinnan tulisi käsitellä organisaation toimintaan liittyvät riskit niin menneisyydessä kuin nykyisyydessä, mutta etenkin tulevaisuudessa. Riskienhallinnan kautta organisaation strategia tulisi kääntää taktisiksi ja operatiivisiksi tavoitteiksi, joiden kautta vastuuta kyetään jakamaan koko organisaation läpi. (IRM, 2002). Esimerkkinä riskienhallinnan prosessista on Institute of Risk Management esittämä kuvion 3 kaltainen menetelmä (IRM, 2002).



KUVIO 3 Esimerkki riskienhallinnan prosessista (IRM, 2002)

Riskienhallinta kuvataan kehämäiseksi prosessiksi, joka alkaa organisaation strategian asettamista tavoitteista. Toiminta etenee riskien huolellisen analysoinnin ja arvioinnin kautta uhkien ja mahdollisuuksien hahmottamiseen. Päätösten kautta riskejä kohtaan kehitetään toimenpiteet ottaen huomioon aina olemassa oleva "jäännösriski". Seuranta on jatkuvaa ja ymmärryksen lisääntyessä tulee arvioita ja menetelmiä kehittää jatkuvasti paremmaksi.

Lanne (2007) sanoo, että riskienhallinta on "suunnitelmallista, järjestelmällistä ja jatkuvaa johtamisperiaatteiden, menettelytapojen sekä käytäntöjen hyväksikäyttämistä organisaation resursseihin ja (liike)toimintaan eri tavoin vaikuttavien riskien analysoimiseen, merkityksen arvioimiseen ja valvomiseen." (Lanne, 2007).

NIST määrittelee riskienhallinnan prosessiksi, joka sisältää organisaation toiminnan, suojattavat varannot ja yksilöt. Riskienhallinnan kautta organisaatio suorittaa riskien arvioinnin, toimenpiteet riskien vähentämiseksi sekä toimenpiteet turvallisuustilanteen jatkuvan seuraamisen toteuttamiseksi. (FIPS 200, 2006).

Yhteenvetona voidaan todeta, että riskienhallinta on prosessi, johon koko organisaation täytyy sitoutua. Organisaation johdon tulee asettaa riskienhallinnalle tavoitteet ja resurssit sekä sitouttaa henkilöstö sen toteuttamiseen. Riskienhallinta tulee nähdä johdonmukaisena prosessina, jossa arvioidaan konkreettiset riskit ja määritellään keinot, joilla riskejä pyritään minimoimaan. Riskienhallinta ei ole suoritus, jonka tuloksena saadaan pysyvät toimintatavat organisaation riskienhallintaan. Riskiympäristön jatkuva valvonta ja toiminnan muuttaminen tarvittaessa on olennainen osa riskienhallinnan kokonaisuutta.

Tietojärjestelmiin liittyvien riskien hallinta on monimutkainen ja monitahoinen toimi. Sen toteuttaminen vaatii koko organisaation osallistumista siten, että siihen sitoutuvat kaikki organisaation tasot aina strategisen tason johtajista toteuttavan tason työntekijöihin. Riskienhallinta voidaan nähdä kokonaisvaltaisena prosessina, joka on integroitu organisaation kaikkeen organisaation toimintaan. (NIST, 2010; NIST, 2011).

Gordonin, Loebin ja Sohailin (2003) mukaan organisaatioiden lisääntynyt kytkeytyminen Internetiin on lisännyt niiden potentiaalisia haavoittuvuuksia esimerkiksi tietomurroille, vandalismille ja palvelunestohyökkäyksille. Kyberturvallisuuteen liittyvät turvallisuuskysymykset ovat nousseet yhä suuremmaksi prioriteetiksi organisaatioiden johtohenkilöiden asialistalla. Tietoverkkokeskeisen liiketoiminnan sisältämät riskit eivät kuitenkaan ole pohjimmiltaan uusia. Monet riskit ovat olemassa ilman informaatioteknologiaakin. Informaatioteknologia tuo riskeille ja riskienhallinnalle mukanaan uusia erityispiirteitä. (Gordon ym., 2003). Organisaation toiminnan kannalta on kriittistä, että nämä erityispiirteet osataan ottaa huomioon osana riskienhallinnan kokonaisuutta. Kyberympäristö tekee monista riskeistä täysin ajasta ja paikasta riippumattomia ja monen organisaation toiminta on täysin riippuvainen sähköisten järjestelmien toiminnasta. Tämän vuoksi kyberturvallisuuden osuus riskienhallinnassa tulisi olla merkittävä.

Riskienhallinnan tulisi ottaa huomioon mahdollisuuksien mukaan kaikki tiedossa olevat järjestelmiin kohdistuvat riskit. Niiden lisäksi tulisi kyetä huomioimaan mahdollisesti tulevaisuudessa kehittyvät haavoittuvuudet. Kyberriskienhallinnan ja -arvioinnin pitäisi olla kaikkien turvallisten tietojenkäsittelyympäristöjen perustana. (Siegel, Sagalow & Serritella, 2002). Heidän mukaansa kyberturvallisuuden riskienhallinnan ei tulisi olla lähtöisin ainoastaan teknisestä näkökulmasta. Riskienhallinnan tulisi sisältää ihmiset, prosessit, teknologia ja liiketaloudellinen näkökulma. Tämän kattavan arvioinnin kautta voidaan päättää, mitkä teknologiat ja prosessit otetaan käyttöön havaittujen riskien vähentämiseksi. (Siegel ym., 2002). Siegel ym. sanovatkin, että perusteellisen riskienhallintaprosessin tulisi sisältää useita näkökulmia aina fyysisestä turvallisuudesta tietoverkkojen haavoittuvuuksien kartoittamiseen. Lisäksi tulisi toteuttaa penetraatiotestausta sekä henkilöstön haastatteluita. (Siegel ym., 2002).

Gordon ym. (2003) määrittävät informaatioteknologiaan liittyvän riskienhallinnan olevan prosessi, jonka alussa arvioidaan riskit. Tämän jälkeen tehdään tarvittavat toimenpiteet riskien vähentämiseksi hyväksyttävälle tasolle ja riskien pitämiseksi sopivalla tasolla. (Gordon ym., 2003). Kyberturvallisuuden riskienhallinta on ennen kaikkea johtajien vastuulla. Ylimmän johdon tulee taata tavoitteiden toteuttamiseksi riittävät resurssit ja heidän täytyy olla tietoisia myös kyberturvallisuuteen liittyvän riskienhallintaprosessin tekemisestä ja tuloksista. Tietohallintojohtaja (tai muu vastaava) vastaa oman vastuualueensa suunnittelusta, budjetoinnista ja suorituskyvystä. Kaikkien päätösten tulisi perustua tehokkaan riskienhallinnan toteuttamiseen. Organisaation tehtävän kannalta tärkeän tiedon ja järjestelmien suojaamisella voidaan saavuttaa organisaatiolle merkittäviä hyötyjä. Riskienhallinta voidaan määritellä prosessiksi, joka auttaa IT-johtajia suhteuttamaan suojatoimenpiteiden taloudelliset kustannukset. (NIST, 2002).

Merkittävän haasteen kyberturvallisuuden riskienhallinnalle luo historiallisen datan puute. Tietoverkkokeskeisen yhteiskunnan ollessa suhteellisen uusi asia, on vaikea perustaa päätöksiä esimerkiksi jonkin tapahtuman esiintymisen todennäköisyyteen. Perinteisempien riskien suhteen historiatietoa on löydettävissä. Kyberturvallisuuteen liittyvien tapahtumien historiatieto on perinteisiin riskeihin nähden huomattavan suppea. Tämä suppeus johtuu informaatioteknologian lyhyestä historiasta sekä siitä, että organisaatiot eivät välttämättä ole halukkaita raportoimaan esimerkiksi omista tietomurroistaan. (Gordon ym., 2003). Kuten kaikessa riskienhallinnassa, myös kyberturvallisuuteen liittyen, tulee ymmärtää, että kaikista toimenpiteistä huolimatta on aina olemassa niin sanottu jäännösriski. Riskiä ei voida poistaa täysin. (NIST, 2002; Gordon ym., 2003; Gerber & Von Solms, 2005). Organisaation tulee määrittää hyväksyttävän riskin taso myös kyberturvallisuuteen liittyen.

2.1.3 Organisaatiokulttuuri

Lämsän ja Hautalan (2005) mukaan tunnetuimpia organisaatiokulttuurin määritelmiä on Edgar Scheinin 1987 julkaistussa kirjassaan "Organisaatiokulttuuri ja johtaminen" käyttämä määritelmä. Scheinin (1987) mukaan "organisaatiokulttuuri on perusolettamusten malli, jonka jokin ryhmä on keksinyt, löytänyt tai kehittänyt oppiessaan käsittelemään ulkoiseen sopeutumiseen tai sisäiseen yhdentymiseen liittyviä ongelmia. Organisaatiokulttuuri koostuu suhteellisen pysyvistä arvoista, uskomuksista, tavoista, perinteistä ja käytännöistä, jotka organisaation jäsenet jakavat keskenään, opettavat uusille työntekijöille ja siirtävät sukupolvelta seuraavalle sukupolvelle." (Schein, 1987). Lämsän ja Hautalan (2005) mukaan organisaatiokulttuurin käsite voidaan jakaa kolmeen päätehtävään. Ensinnäkin organisaatiokulttuuri tuottaa yhteisen identiteetin organisaation jäsenille tarjoamalla vastauksia kysymykseen, keitä ja millaisia olemme. Toiseksi organisaatiokulttuuri edistää ihmisten sitoutumista organisaation perustehtäviin yhteisen "maailmantulkinnan" kautta. Kolmanneksi organisaatiokulttuuri selventää ihmisten käyttäytymisen pelisääntöjä muodostamalla perustan sille, miten työpaikalla on sopivaa käyttäytyä. (Lämsä & Hautala, 2005). Huomionarvoista on, että Lämsän ja Hautalan (2005) mukaan organisaatiokulttuuri kehittyy ihmisten tarinoissa sekä yhteisissä tapahtumissa. Tarinat organisaation perustajien kovasta työmoraalista ja sankariteoista sekä onnistumisista opettavat organisaation jäseniä arvostamaan kovaa työntekoa ja käytännön kokemusta muodollisen koulutuksen sijaan. Organisaation kehittäminen kulttuuria muuttamalla on hidasta. Mattilan (2007) mukaan kulttuuri on opittua ja siksi myös muutettavissa, vaikkei sitä pystykään komentamaan. Karlöfin ja Helin Lövingssonin (2006) mukaan todellisten muutosten aikaansaamiseksi tulee ottaa huomioon totutut käyttäytymistavat ja -normit. Vaikka kulttuuriin vaikuttaminen tapahtuu hitaasti ja usein monien mutkien kautta, se on välttämätöntä, sillä laajankaan uudistuksen vaikutukset eivät voi kestää, jos kulttuuri asettuu niitä vastaan (Mattila, 2007). Organisaatioita voi verrata kehittyviin järjestelmiin, joissa tehdään paikallisia sopeutuksia sen mukaan, mitä markkinoilla, työntekijöiden parissa tai muiden tärkeiden sidosryhmien joukos-

sa tapahtuu. (Karlöf & Helin Lövingssonin, 2006). Organisaatiokulttuurin muutosta edistävät seuraavat asiat (Lämsä & Hautala, 2005):

- Henkilöstön ja johdon koulutus ja kehittäminen
- Muutokset toimintatavoissa ja -rutiineissa sekä fyysisessä työympäristössä
- Muutokset organisaatiorakenteessa
- Uusien käsitteiden, puhetapojen ja tarinoiden käyttöönotto
- Äkillinen, dramaattinen ja ulkoinen muutospaine
- Uudet henkilöstön arviointi- ja palkitsemisperiaatteet
- Esimiehen ja avainhenkilöiden vaihtuminen ja
- Uusia ihanteita luovat arvo- ja periaatejulistukset

Scheinin (1987) tutkimus on vienyt mahdollisesti pisimmälle organisaatiokulttuurin merkityksen johtamisessa. Scheinin mukaan johtajan ainoa tärkeä tehtävä on luoda ja johtaa kulttuuria. Mattilan (2007) mukaan johtajan tulee tarjota organisaation jäsenille viitekehys, jonka kautta asiat selittyvät ja tulevat ymmärretyksi. Tsohou, Karyda, Kokolakis ja Kiountouzis (2006) tutkivat organisaatioiden tietojärjestelmien riskienhallintastrategioiden muodostumista kulttuuriteorian kautta. Kulttuuriteoriaa on sovellettu eri instituutioissa, aloilla ja aihepiireissä, mutta ei tietojärjestelmien turvallisuudessa. (Altman & Baruch, 1998). Useat tutkijat ovat yhdistäneet kulttuuriteorian kuitenkin juuri riskienhallintaan (Tsohou ym., 2006; Lima & Castro, 2005; Marris, Langford & O'Riordan, 1996; Rayner, 1984). Tsohou ym. (2006) mukaan tietojärjestelmien osana olevilla ihmisillä on erilaisia näkemyksiä esimerkiksi riskien tiedostamisessa. Näkemykset riskeistä rakentuvat suurelta osin kyseisen ihmisen maailmankuvan perusteella. Marris ym. (1996) tutkimuksessa vaihtelua ihmisten riskien havaitsemiskyvyssä perusteltiin kulttuuritekijöillä, vaikka maailmankuvan kaltaiset moniulotteiset tutkimuskysymykset ovat hankalia tutkia tutkimuksessa käytetyn kaltaisella kyselylomakkeella. Tsohou ym. (2006) mukaan riskienhallintaan sisältyy erityisen paljon ihmisen toimintaa ja ihmiset havaitsevat riskejä eri tavalla. Riskien tunnistaminen ja arviointi ovat ihmisen sosiaalista ja inhimillistä toimintaa. Tietojärjestelmien käyttäjätasot, kuten esimerkiksi loppukäyttäjät tai johto, painottavat eri riskejä. Koetut riskit perustuvat omiin kokemuksiin, mediasta saatuihin vaikutteisiin ja tuttavien kertomuksiin. (Tsohou ym., 2006). Roth (2015) mukaan aika ja tila sekä käyttäytyminen ja ajattelu ovat erilaisia eri kulttuureissa. Sosiaalisesta, poliittisesta tai sodankäynnin näkökulmasta aiemmin lähestyttyjen asioiden arviointi kulttuurin näkökulmasta sekä yksilön että kansallisesta näkökulmasta avaa uusia mahdollisuuksia. Turvallisuusriskien arviointi ei ole koskaan helppoa. Arviointi perustuu kuitenkin aina analyyttiseen ja intuitiiviseen lähestymistapaan. (Roth, 2015). Kulttuuri ohjaa finanssialan yritysten tietoturvapolitiikan muodostumisessa samankaltaisesti kuin Al-Rodhan (2015) kuvaa valtioiden siirtyessä kansallisen sääntelyn piiristä osaksi isompaa kansainvälistä toimintaympäristöä. Finanssialan yritykset joutuvat kansainvälisessä toimintaympäristössä ottamaan huomioon historialliset

tekijät kuten kertyneet kokemukset, uskomukset, kulttuurin vaikutuksen, maantieteellisen sijainnin ja materiaalien sekä resurssien riittävyyden.

Kulttuurilla on merkitystä, koska se on vahva, piilevä ja usein tiedostamaton sarja voimia, jotka määrittävät sekä yksilö- että ryhmäkäyttäytymistämme, käsitystapojamme, ajatusmallejamme ja arvojamme. Organisaatiokulttuuri määrittää strategiaa, päämääriä ja toimintatapoja. Organisaatioiden näkemys on usein johtajien ja ylempien esimiesten arvoja ja ajatusmalleja kuvaava. Jotta organisaatioista saadaan tehokkaampia ja toimivampia, kulttuurin rooli organisaatioissa tulee ymmärtää. (Schein, 2009).

2.1.4 Tietoturvapolitiikka riskienhallinnan keinona

Tässä luvussa kuvataan tietoturvallisuuden ja tietoturvapolitiikan käsite sekä tietoturvapolitiikan käyttö riskienhallinnan keinona. Luvun sisältö kietoo organisaation strategian konkreettiseen riskienhallinnan välineeseen, joka varsinkin tiukasti säännellyn finanssialan organisaatioista oletetaan löytyvän. Luvussa kuvataan tietoturvapolitiikan käsitteen lisäksi tieteellistä tutkimusta tietoturvapolitiikan roolista organisaatioissa. Tutkimuksen kohderyhmän ollessa vahvasti säädelty finanssiala ja haastateltavien ollessa turvallisuusjohtajia on tietoturvapolitiikan kuvaaminen luonnollinen valinta osaksi tutkimusta.

Tietoturvalla tai tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus (Sanastokeskus TSK, 2004). Tietoturvallisuus on määritelty ISO/IEC 27000:2009 standardissa luottamuksellisuuden, eheyden ja käytettävyyden (CIA, *confidentiality, integrity, availability*) säilyttämisenä (ISO/IEC 27000:2009, 2009). Tietoturvallisuuden tarkoitus on varmistaa kolme asiaa: vain oikeutuksen saaneilla käyttäjillä (luottamuksellisuus, *confidentiality*) on pääsy oikeisiin tietoihin, toiseksi käyttäjillä on pääsy täydellisiin tietoihin (eheys, *integrity*) ja kolmanneksi pääsy on mahdollista aina tarvittaessa (saatavuus, *availability*) (Whitman & Mattord, 2010; Turvallisuus- ja puolustusasiain komitean sihteeristö, 2013). Dhillon ja Backhouse (2000) kuvaavat CIA:n (*confidentiality, integrity, availability*) periaatteet hyvin rajallisiksi, koska ne keskittyvät lähinnä tietojärjestelmissä olevan datan, tiedon, turvaamiseen. Teknologian kehitys kulkee lisäksi vahvasti toiseen suuntaan, koska tiedon jakaminen pyritään rakentamaan niin, että se on saatavissa missä ja milloin tahansa. (Dhillon & Backhouse, 2000). Halen ja Swusten (1998) mukaan turvallisuuden tieteen alalla käytetään yleisesti käsitettä turvallisuussäännöt, jonka voi määritellä seuraavasti:

> Turvallisuussääntö on määritelty järjestelmän tila tai määritelty toimintatapa ennakoitavaan tilanteeseen, mikä on muodostettu ennen tapahtumaa sekä asetettu ja/tai hyväksytty järjestelmässä keinona parantaa turvallisuutta tai saavuttaa vaadittu turvallisuuden taso (Hale & Swuste, 1998).

Sanastokeskus TSK:n (2004) määritelmän mukaan tietoturvapolitiikalla tarkoitetaan "organisaation hyväksymää näkemystä organisaation tietoturvan päämääristä, periaatteista ja toteutuksesta". Bulgurcu kuvaa tietoturvapolitiikkaa selvitykseksi työntekijöiden roolista ja vastuista organisaation tiedon ja

teknisten resurssien turvaamisessa (Bulgurcu ym. 2010). Bulgurgun esittämä määritelmä on laajasti käytössä tieteellisissä julkaisuissa (Boss, Kirsch, Angermeier, Shingler ja Boss, 2009; D'Arcy, Hovav & Galletta, 2009; Dhillon, 1997; Herath & Rao, 2009; Peltier, 2004; Peltier, 2005). Tietoturvallisuuspolitiikan on tarkoitus tarjota riittävät turvallisuusmekanismit ja -käytänteet organisaation tietojärjestelmien turvaamiseksi (Peltier, 1999; Wood, 1999). Whitman ja Mattord (2010) mukaan organisaatioilla on yleensä kolmen eri kategorian tietoturvapolitiikoita:

1. Organisaatiotason tietoturvapolitiikka (EISP, Enterprise information security policy) kuvastaa organisaation strategista IT -suunnitelmaa ja yleisesti tietoturvan sävyä organisaatiossa.

2. Aihekohtaiset tietoturvapolitiikat (ISSP, Issue specific security policies) kuvaavat säännöt hyväksyttävälle käytökselle tietyn teknologian kuten sähköpostin tai internetin käytön osalta.

3. Järjestelmäkohtaiset politiikat (SysSP, System-specific policies) ovat teknisiä tai hallinnollisia luonteeltaan. Hallinnoivat asetuksia tai teknologian tai välineiden käyttöä esimerkiksi käyttö-oikeuslistojen (ACL, access control list) avulla.

Tietoturvapolitiikassa tulee alussa määritellä, miten tietoturvallisuus ja tietoturvapolitiikka organisaatiossa määritellään (Höne & Eloff, 2002a), koska tietoturvallisuuteen liittyvät määritelmät ja termit vaihtelevat lähteestä riippuen. Tietoturvapolitiikka laaditaan yksittäiselle organisaatiolle organisaatiokulttuuri ja laaja lukijajoukko huomioiden (Höne & Eloff, 2002a; Gerber & Von Solms, 2005). Tietoturvapolitiikan muodostaminen vaatii yhteisen näkemyksen sisällöstä, kattavuudesta ja siitä kuka sen hyväksyy (Höne & Eloff, 2002a). Purserin (2016) mukaan organisaatiot voivat tehdä paperilla erinomaiselta näyttäviä politiikoita toiminnoilleen, mutta tämä ei vielä tarkoita, että käyttäjät motivoituvat käyttämään niitä. Haasteet politiikoiden luomisessa liittyvätkin juuri käytettävyyteen. (Purser, 2016). Limnéllin (2015) mukaan Suomessa on totuttu näkemään kybermaailma vaikeana ja jopa pelottavana asiana. Kyberturvallisuudessa on kysymys kuitenkin suurelta osin muusta kuin tekniikasta. Limnéllin mukaan, vaikka tekniikan laittaisi kuntoon, on ihmisen toiminnalla mahdollista aiheuttaa merkittävää tuhoa. Niin sanottu *human factor* eli inhimillinen tekijä on asia, johon pystyy vaikuttamaan koulutuksella ja tiedottamisella. (Limnéll, 2015).

Tietoturvapolitiikka konkretisoi organisaation tahdon henkilöstölle ja pyrkii tekemään toiminnasta ennakoitavampaa sekä luotettavampaa. Johnston, Warkentin ja Siponen (2015) mukaan organisaatioiden turvallisuusjohtajat pyrkivät turvallisuuskoulutuksen, harjoittelun ja tietoisuuden lisäämisen kautta valvomaan tietoturvapolitiikan noudattamista. Höne ja Eloffin (2002a) mukaan johdon sitoutuminen tietoturvapolitiikkaan on tärkeintä, jotta tietoturvallisuushenkilöstöllä on todellinen mahdollisuus toimenpiteillään vaikuttaa organisaation turvallisuuden parantamiseen ja käytänteiden noudattamiseen. Turvalli-

suusajattelun siirtäminen organisaation henkilöstölle tuo näkemykset käytännön työhön, joten turvallisuustyön pitää olla osa koko organisaation henkilöstön työnkuvaa. (Työsuojelu, 2016). Työturvallisuuslaki (738/2002) säätelee turvallisuustyötä ainoastaan yleisellä tasolla ja luo pohjan turvallisuusjohtamiselle työnantajan velvollisuuksien kautta. Työnantajan on riittävän järjestelmällisesti selvitettävä työstä ja olosuhteista aiheutuvat haitat ja vaaratekijät. (Työturvallisuuslaki, 738/2002).

Kelly Rainer Jr., Marshall, Knapp ja Montgomery (2007) mukaan turvallisuusjohtajien ja organisaation johdon tulee optimaalisen turvallisuuden tason saavuttamiseksi toimia entistä enemmän yhteistyössä. Tämän lisäksi liiketoimintajohtajilla tulee olla perustiedot organisaation tietoturvallisuuden teknisistä ominaisuuksista ja turvallisuusjohtajilla tulee olla osaamista niin laskentatoimesta, rahoituksesta, markkinoinnista, henkilöstöjohtamisesta, organisaatiokäyttäytymisestä ja projektijohtamisesta. (Kelly Rainer Jr. ym., 2007). Viron tietoturvallisuusviranomaisen, *RIA (Riigi Infosusteemi Amet)*, vuoden 2014 raportin tulosten mukaan organisaatioiden johtajien tietoisuutta informaatioteknologiasta tulee parantaa järjestelmällisen koulutuksen avulla (RIA, 2014). IBM (2012) tutkimusraportissa kyselyyn vastanneista yritysten johtajista 46 % kertoi liiketoiminnan osa-alueista maineen liittyvän erittäin läheisesti informaatioteknologian mahdollisiin riskeihin. Vastaavasti 41 % kertoi sääntöjen noudattamisen ja 40 % brändin maineen olevan erittäin vahvasti liitettävissä IT-riskeihin. (IBM, 2012). Gerber ja Von Solms (2005) mukaan informaatioteknologia tulee nähdä osana suurempaa kokonaisuutta, jotta organisaation tietoturvallisuusvaatimukset voidaan huomioida yksilöllisesti. Gordon ym. (2015) mukaan yritykset eivät tee investointeja kyberturvallisuuteen muusta toiminnasta erillään. Riskianalyysia laadittaessa tulee huomioida sekä organisaation aineelliset, että aineettomat varat, jotta analyysi huomioi lainsäädännölliset, kulttuuriin perustuvat ja muut sosiologiset tekijät. (Gerber & Von Solms 2005). Karyda, Kiountouzis & Kokolakis (2001) ja Karyda, Kiountouzis & Kokolakis (2005) mukaan tietoturvapolitiikan tulisi turvata tietojärjestelmien osien lisäksi koko järjestelmän toimivuutta, mutta merkittävistä resursoinnista huolimatta turvallisuuspolitiikat eivät saavuta tavoitteitaan. Turvallisuuspolitiikoiden tai -käytänteiden nähdään rakentuvan organisaation ominaisuuksien mukaan (Gerber & Von Solms, 2005; Kelly Rainer Jr. ym., 2007). Tietoturvapolitiikka kasvaa ja mukautuu organisaation vision ja toiminnan mukana. Organisaatioiden kulttuurit eivät ole valmiita, vaan ne kehittyvät koko ajan asteittain mukautuen paikallisten olosuhteiden, menneiden tapahtumien, johtamistyypin ja henkilöstön olojen mukaan (Reason, 1998). Höne ja Eloff (2002b) kuvaavatkin tietoturvallisuuspolitiikan jatkuvasti eläväksi asiakirjaksi.

Vaikka liiketoiminnan tiedon turvaaminen on organisaation toiminnassa strateginen ongelma (Hedström, Kolkowska, Karlsson & Allen, 2011; Hu, Hart & Cooke, 2007) organisaatiot kuitenkin luovat usein omat politiikkansa muiden organisaatioiden malleja kopioiden tai kaupallisista tai avoimista lähteistä saatavilla olevien mallien perusteella (Höne & Eloff, 2002a). Mallien lainaaminen johtuu usein puutteellisista taidoista. (Höne & Eloff, 2002a). Höne & Eloffin (2002a) mukaan *leikkaa ja liitä* -mallilla (cut & paste) rakennetut politiikat kuvaavat harvoin organisaation kulttuuria ja eivät johda todelliseen tehokkaaseen

ohjeistukseen. Höne ja Eloff (2002b) tietoturvallisuus ei saa olla käyttäjille epämukava tai vieras konsepti. Organisaation omaa kulttuuria kuvaavalla tietoturvallisuuspolitiikalla on mahdollista saada todellista vaikutusta käyttäjien toiminnassa, koska teknisin käsittein ja yksityiskohtaisesti laadittu tietoturvallisuuspolitiikka on usein vaikea ymmärtää ja asiakirjan tarkoitus katoaa. Kiehtovasti ja jopa hauskasti laadittu asiakirja taas kutsuu lukemaan ja saa käyttäjät kiinnittämään huomionsa asiakirjan sisältöön. Tämä edellyttää kuitenkin aina, että tietoturvallisuuspolitiikan olemassa olosta kerrotaan asiakirjan kohteena oleville käyttäjille. (Höne & Eloff, 2002b).

Kraemer, Carayon ja Clem (2009) mukaan teknisillä ratkaisuilla ei voida poistaa ihmisen toiminnasta johtuvia tekijöitä. Organisaation vaikutuksen ymmärtäminen on turvallisuustoimijoille ensiarvoisen tärkeää. Tieto- ja informaatioturvallisuuden hallintaohjelmat, riskienhallintaprosessit, ovat välttämättömiä organisaation tilan ja haavoittuvuuksien seurannassa. (Kraemer ym., 2009). Adams ja Sassen (1999) mukaan tietojärjestelmien käyttäjät eivät noudata turvallisuusohjeita ja -sääntöjä. Tehokas ja vaikuttava tietoturvallisuuspolitiikka rakentuu tiivistettynä ihmisten ja liiketoiminnan ympärille. Ihmiset suunnittelevat, ottavat käyttöön ja murtavat tietojärjestelmät, joten ihmisen toiminta tulee ottaa yhä tarkemmin huomioon. Tietojärjestelmien turvallisuuden tulisi olla tunnettu ja vakavasti otettava organisaation prosessi. Tietoisuutta organisaation tietojärjestelmien turvallisuuteen liittyen tulee näin ollen jakaa mahdollisimman laajasti. (Adams & Sasse, 1999). Albrechtsen mukaan organisaatioiden henkilöstö tulee motivoida järjestelmien turvalliseen käyttöön, mutta liian tiukkojen turvallisuuspolitiikoiden käyttöä tulee välttää, koska mitä tiukempia määräykset ovat, sitä enemmän henkilöstö pyrkii järjestelmien käytettävyyteen turvallisuuden kustannuksella (Albrechtsen, 2007). Herath ja Rao (2009) mukaan käyttäjien tulee olla innokkaita politiikoiden noudattamiseen ja kokea noudattaminen tärkeäksi, jotta organisaation tieto ja tekniset resurssit voidaan turvata. Käyttäjien rooli ja vastuu tulee tulevaisuudessa olemaan entistä suuremmassa roolissa tietoturvallisuuden hallinnassa. Dhillon ja Backhousen (2000) mukaan käyttäjät ohjataan turvaamaan organisaatioiden aineellista ja aineetonta omaisuutta sekä reagoimaan mahdollisiin haitallisiin tapahtumiin. Spears ja Barki (2010) sekä Karyda ym. (2005) mukaan käyttäjät tuovat lisäarvoa organisaation tietojärjestelmien turvallisuuden suunnittelussa, analyysissa ja testauksessa, koska samalla tietoisuus mahdollisista uhkista lisääntyy.

Tietojärjestelmien väärinkäyttö on tutkimuksessa todettu pääasialliseksi tietojärjestelmien turvallisuuden ongelmaksi organisaation sisäpiiriläisten, kuten työntekijöiden osalta (mm. Bulgurcu ym., 2010; Gordon, Loeb, Lucyshyn & Richardson, 2006). Ongelmaan on mahdollista puuttua ennaltaehkäisemällä ja ohjeistamalla henkilöstöä. D'Arcy ym. (2009) tutkimuksessa luodun mallin perusteella tietoisuus organisaation turvallisuustoimista vaikuttaa käyttäjien kokemaan rangaistuksen mahdollisuuteen. Boss ym. (2009) tutkivat tietoturvallisuuspolitiikoiden noudattamisen pakollisuutta. Tutkimuksessa havaittiin turvallisuuspolitiikoiden noudattamisen pakon motivoivan käyttäjiä sääntöjen noudattamiseen. (Boss ym., 2009).

Tietoturvapolitiikalla on organisaatioiden toiminnassa oma paikkansa. Tällä hetkellä tietoturvapolitiikan tarkoituksesta ja laajuudesta käydään jatku-

vaa keskustelua. Usein politiikat ovat hyvin pitkiä ja vaikeasti luettavia asiakirjoja, joita organisaation henkilöstö ei lue. Tietoturvapolitiikka tulisi kirjallisuuden perusteella nähdä kuitenkin lukemaan kutsuvaksi ja ymmärrettäväksi ohjeistukseksi, joka tukee organisaation strategiaa. Tietoturvapolitiikan hyödyntämisessä ja liittämisessä organisaation strategiaan on vielä nykyisin haasteita.

3 RISKIT ORGANISAATIOIDEN TOIMINTAYMPÄRISTÖSSÄ

Tässä luvussa kuvataan finanssialan organisaatioiden toimintaympäristöä tällä hetkellä ja tulevaisuudessa. Riskien tarkastelussa keskitytään tutkimuksen näkökulman mukaisesti informaatioteknologiaan liittyvien riskien tarkasteluun kyberturvallisuuden näkökulmasta. Luvun lopussa kuvataan, miten toimintaympäristön riskejä on mahdollista tunnistaa. Tutkimuksen tärkein lopputulos, muodostettava riskien arvioinnin prosessimalli, vastaa ideaalitilanteessa tässä luvussa kuvattuihin haasteisiin uhkien ja mahdollisuuksien tunnistamisessa.

Finanssialan toimijoita ovat pankit, vakuutusyhtiöt, rahoitusyhtiöt, arvopaperin välittäjät ja sijoitusrahastoyhtiöt. Suomessa Finanssialan Keskusliitto (FK) vastaa toimijoiden edunvalvonnasta. Finanssialan Keskusliitto toimii yhteistyössä eurooppalaisten kattojärjestöjen EBF:n (European Banking Federation), Insurance Europen ja EFAMA:n (European Fund and Asset Management Association) kanssa. (Finanssialan Keskusliitto, 2016). Vuoden 2014 lopussa Suomessa oli 291 luottolaitosta, joihin kuuluu talletuspankit sekä muut luottolaitokset, jotka eivät ota vastaan talletuksia (Finanssialan Keskusliitto, 2014a). Suomessa toimi vuoden 2014 lopussa 57 kotimaista vakuutusyhtiötä. Tämän lisäksi Suomessa toimi 14 ulkomaalaisten vakuutusyhtiöiden edustustoa. (Finanssialan Keskusliitto, 2014b). Suomen kolme suurinta pankkia OP-ryhmä, Nordea Pankki Suomi Oyj ja Danske Bank Oyj ovat Euroopan Keskuspankin suoran valvonnan alla. Pienemmät pankit ovat edelleen Finanssivalvonnan valvonnassa. (Finanssialan Keskusliitto, 2014a). Elinkeinoelämän toimijoilla, kuten pankeilla on keskeinen asema erityisesti talouden ja infrastruktuurin toimivuuden varmistamisessa. Rahapolitiikan ensisijaisena tavoitteena on hintavakaus. (Valtioneuvoston periaatepäätös 16.12.2010).

3.1 Toimintaympäristön vaikutus finanssialan organisaatioiden riskeihin

Porterin mukaan toimintaympäristö kuvaa alaa, jolla yritys kilpailee muiden yritysten kanssa. Toimialan rakenne vaikuttaa siihen millaista kilpailu alalla on ja mahdolliset yrityksen käytettävissä olevat strategiat (Porter, 1980). Teece, Pisano ja Shuen (1997) mukaan yrityksen strategiseen asemaan ei vaikuta ainoastaan oppimisprosessi ja sisäisten sekä ulkoisten prosessien yhtenäisyys, vaan myös yrityksen erityiset varat, kuten räätälöidyt toimitilat, työvälineet ja vaikeasti mitattavissa olevat tietovarat. Lisäksi yrityksen maine ja suhteet tuovat oman osansa yrityksen asemaan markkinoilla. (Teece ym., 1997). Kotler ja Keller (2006) kuvaavat, että toimintaympäristön muutoksessa aikaisemmin kysyttyjen palveluiden kysyntä voi loppua ja kysyntä voi siirtyä muualle tai toisiin palveluihin. Toimintaympäristössä tapahtuu jatkuvaa muutosta, johon organisaation on mahdollista sopeutua. (Kotler & Keller, 2006).

Finanssialan Keskusliiton (2014a) mukaan pankit ovat Suomessa jatkaneet sopeutustoimiaan muun muassa henkilöstövähennyksillä, sulkemalla konttoreita, yritysjärjestelyillä sekä liiketoimintamallien uudistuksilla. Sopeutustoimien taustalla vaikuttavat palveluiden sähköistyminen, kiristynyt sääntely, heikko makrotalouden kehitys ja matala korkotaso. (Finanssialan Keskusliitto, 2014a). Finanssialan Keskusliiton pankinjohtajille laatiman neljännesvuosittaisen Pankkibarometri -kyselyn (2015) mukaan sekä yritysten että kotitalouksien luotonkysyntä oli lievässä kasvussa joulukuussa 2015 vuoden 2014 vastaavaan ajankohtaan nähden. Yritykset kysyivät lainaa lähinnä käyttötarpeisiin ja rahoituksen uudelleenjärjestelyihin. Investointeihin yritykset eivät lainaa juuri kysyneet. Vuoden 2016 ensimmäisellä neljänneksellä yritysten luoton kysynnän odotetaan jatkuvan hieman vuoden 2015 kysyntää vilkkaampana. (Finanssialan Keskusliitto, 2015). Suomen vakuutusmarkkinoille on ominaista lakisääteisistä vakuutuksista kerättyjen maksujen suuri osuus koko alan maksutulosta. Vuonna 2013 maksutulosta saatiin 61 % lakisääteisestä työeläkevakuutuksesta, lakisääteisestä tapaturmavakuutuksesta ja liikennevakuutuksesta. (Finanssialan Keskusliitto, 2014b). Puustisen (2013) mukaan arvolupaus on tärkein asia, jolla finanssialan yritys perustelee olemassaolonsa markkinoilla. Arvon ulottuvuudet (taloudellinen, toiminnallinen, emotionaalinen ja symbolinen) luovat perustan asiakkaille tarjottavalle arvolupaukselle. (Puustinen, 2013).

Suomi on osa globaalia kybertoimintaympäristöä, joka muodostuu monimutkaisesta ja -kerroksisesta maailmanlaajuisesta informaatioverkostosta (Turvallisuus- ja puolustusasiain komitean sihteeristö, 2013). Turvallisuuskomitean raportissa ”Turvallinen Suomi 2015” organisaatioiden riskit eivät ole ainoastaan kansallisia, vaan riskien arvioinnin tulee kohdistua koko globaaliin kybertoimintaympäristöön. Kansainväliset voimasuhteet, hallintarakenteet ja arvojärjestelmät muuttuvat osana suurempaa kansainvälisen järjestyksen muutosta. Globaali toimintaympäristö luo oman haasteensa organisaatioiden kykyyn havaita mahdollisia laittomia toimia ja uhkia. Yksittäisen organisaation on kuitenkin suunniteltava ja rakennettava tarpeidensa mukainen turvallisuusratkaisu omista lähtökohdistaan. (Turvallisuuskomitea, 2015).

3.2 Finanssiala osana yhteiskunnan kriittistä infrastruktuuria

Sisäministeriön (2016) kansallisessa riskiarviossa 2015 selvitettiin mahdollisia riskiskenaarioita, jotka voivat vaikuttaa Suomeen haitallisesti. Kriittinen infrastruktuuri käsittää Hagelstamin (2005) mukaan "ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan jatkuvalle toiminnalle". Kriittiseen infrastruktuuriin sisältyy sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja (Hagelstam, 2005) ja siinä on kolme kerrosta: poliittinen, taloudellinen ja tekninen (Mussington, 2002). Kriittistä infrastruktuuria ovat Valtioneuvoston päätöksen huoltovarmuuden tavoitteista (2013) mukaan muun muassa: tieto- ja viestintäjärjestelmät, -verkot ja palvelut, finanssialan palvelut ja energiantuotanto-, siirto- ja jakelujärjestelmät (Valtioneuvoston päätös 857/2013; Sisäministeriö, 2016). Yhteiskunnan elintärkeisiin toimintoihin sisältyy Valtioneuvoston periaatepäätöksen mukaisesti talouden ja infrastruktuurin toimivuus (Valtioneuvoston periaatepäätös 16.12.2010). Finanssiala ja toimialan toimintaympäristö sijoittuvat yhteiskunnan kannalta erityisen merkitykselliseen joukkoon. Suomessa tapahtuva maksuliikenne on nimittäin täysin riippuvainen toimivista tietoliikenneyhteyksistä Eurooppaan. Kohdistetulla kyberhyökkäyksellä voidaan lamauttaa yhteiskunnan toiminnan kannalta välttämätön maksuliikenne ja aiheuttaa näin epätasapainoa rahoitusmarkkinoille. Kohteesta riippuen taloudelliset ja aineelliset vahingot voivat olla jopa satoja miljoonia euroja. Pankkijärjestelmissä käsitellään merkittävissä määrin kansalaisten ja yritysten kannalta elintärkeitä tietoja. (Sisäministeriö, 2016). Gordon ym. (2015) mukaan Yhdysvaltojen kriittisestä infrastruktuurista on lähteestä riippuen noin 85 % yksityisellä sektorilla toimivien yritysten omistuksessa. Yhdysvaltojen kansallisen tiedustelun johtaja James Clapper toteaa kyberturvallisuuden olevan kriittisenä kansallisen turvallisuuden osana nykyisin terrorismia suurempi uhka. Clapper toteaa kyberhyökkäyksien kriittistä infrastruktuuria kohtaan olevan vakavia, mutta on huolestuneempi päivittäin tapahtuvista pienemmistä hyökkäyksistä ja tunkeutumisista. (Boyd, 2016).

Suomi on tietoyhteiskuntana riippuvainen tietojärjestelmien ja verkkojen toiminnasta ja tietoverkot ovat täysin riippuvaisia sähkön saatavuudesta. (Turvallisuuskomitea, 2015; Turvallisuus- ja puolustusasiain komitean sihteeristö, 2013). Suomi on sähköntuotannon osalta osittain riippuvainen tuontisähköstä. Suomen energian kokonaiskulutuksesta katettiin tuontisähköllä 5 % tammi-syyskuussa 2015. Sähköntuonti laski 8 % vuoden 2014 vastaavaan ajankohtaan verrattuna. (Tilastokeskus, 2015). Sähkön saatavuuden turvaaminen on merkittävä osa kriittisen infrastruktuurin turvaamista, koska osalle teollisuusprosesseja jopa alle 10 sekunnin sähkön saannin häiriöt voivat aiheuttaa ongelmia (Sisäministeriö, 2016). Kotitaloutemme ja elinkeinoelämämme toiminta perustuu sähköön, joten yhteiskunnan merkittävimpiä uhkia on sähköisen infrastruktuurin vakava häiriintyminen (Puolustusministeriö, 2008). Turvallisuuskomitean julkaisun (2015) "Sähköriippuvuus modernissa yhteiskunnassa" mukaan todennäköisimpiä sähkökatkon aiheuttajia ovat huonon sään mukanaan tuomat lumi, tuuli ja ukkonen. Jakelujärjestelmän tahallinen vahingoittaminen mahdollistaa yhteiskunnan toiminnan halvaannuttamisen pitkäksi aikaa. Sähköverkko-

jen ohjaus tietokoneilla mahdollistaa tunkeutumisen järjestelmään. Toisaalta sähköverkkojen rakenteelliset haavoittuvuudet altistavat ne kyberuhalle. Toteutuessaan kyberhyökkäykset vaarantavat tietojärjestelmän oikeanlaisen toiminnan. Sääilmiöiden ja tahallisen vahingoittamisen lisäksi sähkön jakeluun voivat vaikuttaa tehopula ja rannikkokaupunkien osalta meriveden nousu. (Turvallisuuskomitea, 2015). Puolustusministeriön (2008) kokoaman "Pitkä sähkökatko ja yhteiskunnan elintärkeiden toimintojen turvaaminen" julkaisun mukaan pankkien ja maksuliikenteen osalta sähkökatko aiheuttaa aluksi konttorien sulkemisen. Sulkemiselle on lisäksi syyt turvallisuusnäkökulmasta. Konttoreiden ohella käteis- ja maksuautomaateilta puuttuu varavoima. Jo hallussa olevalla käteisellä on mahdollista maksaa myös sähkökatkon aikana, mutta tämä aiheuttaa avoinna oleville kauppaliikkeille lisää työtä, koska kassa- ja varastokirjanpidot lakkaavat toimimasta. Aikaisemmin käytössä olleet leimauslaitteet eli "höylät" ovat pääosin poistuneet käytöstä. Poikkeuksen maksamiseen mahdollistaa maksun vastaanottajan mahdollinen varavoima. Tällöin pankkikorteilla voi maksaa niin kauan kuin maksupäätteessä riittää muistikapasiteettia. (Puolustusministeriö, 2008).

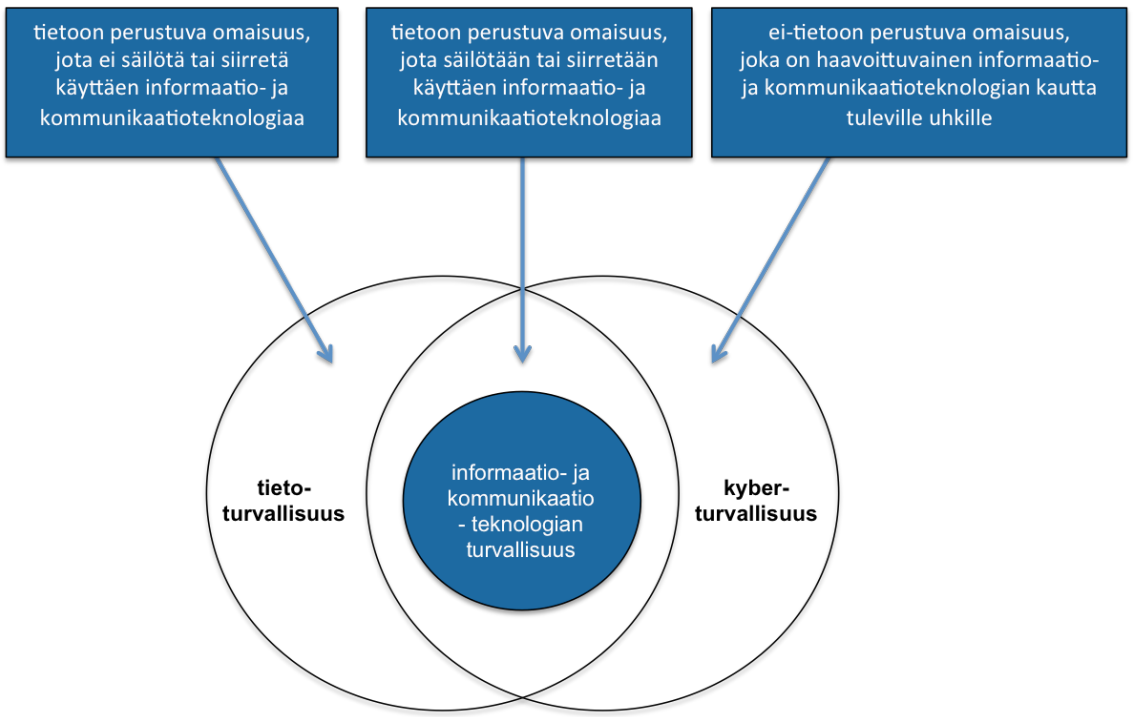
3.3 Kyberturvallisuus

Kyberturvallisuus –käsitteen käyttäminen on vakiintunut osaksi suomalaista termistöä (Limnéll, 2014). Vaikka kyberturvallisuuden käsitettä käytetään monissa eri yhteyksissä, ei sen määrittely ole yksiselitteistä eikä kyberturvallisuuden määritelmäksi löydy yhtä, yleisesti tunnustettua määritelmää. Euroopan Unioni määrittelee kyberturvallisuuden toimiksi, joita voidaan käyttää suojaamaan kyberympäristöä niiltä uhkilta, jotka voivat vahingoittaa sen toisistaan riippuvaista verkostojen ja tietojen infrastruktuuria. (Euroopan komissio, 2013). Oxford Dictionaries -sähköinen sanakirja määrittelee kyberturvallisuuden rikolliselta tai luvattomalta sähköisen tiedon käytöltä suojatuksi tilaksi, tai toimenpiteiksi tämän tilan saavuttamiseksi (Oxford Dictionaries, 2015). NIST, National Institute of Standards and Technology, määrittelee kyberturvallisuuden "kyvyksi suojata tai puolustaa kyberavaruutta (cyber space) kyberhyökkäyksiltä". (NISTIR 7298, 2013). Lehto ja Kähkönen (2015) määrittelevät kyberturvallisuuden toimenpiteiksi, joiden avulla pyritään suojautumaan kyberhyökkäyksiä ja niiden vaikutuksia vastaan. Kyberturvallisuuden kautta voidaan toteuttaa tarvittavat vastatoimet niitä vastaan. (Lehto & Kähkönen, 2015). Lehdon ja Kähkösen mukaan kyberturvallisuus rakentuu organisaation tai instituution uhka-analyysille ja kyberturvallisuuden strategia ja ohjelman rakenne sekä elementit riippuvat organisaation arvioiduista uhkatekijöistä ja riskeistä. (Lehto & Kähkönen, 2015).

Suomen kyberturvallisuusstrategia määrittelee kyberturvallisuuden seuraavasti: "Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan". Määritelmää on lisäksi tarkennettu seuraavasti:

- Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle.
- Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyä ("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." (Turvallisuus- ja puolustusasiain komitean sihteeristö, 2013).

Von Solms ja Van Niekerk määrittelevät kyberturvallisuuden kuvion 4 mukaisesti:



KUVIO 4 Tietoturvallisuuden, kyberturvallisuuden sekä informaatio- ja kommunikaatioteknologian turvallisuuden suhde (Von Solms & Van Niekerk, 2013)

Von Solmsin ja Van Niekerkin (2013) mukaan sekä kyberturvallisuuden että informaatioturvallisuuden termejä käytetään usein puhuttaessa samasta asiasta. Vaikka näillä käsitteillä onkin paljon yhteistä, ne eivät vastaa täysin toisiaan. Von Solmsin ja Van Niekerkin (2013) mukaan kyberturvallisuus on laajempi käsite kuin informaatioturvallisuus. Informaatioturvallisuus pyrkii huomioimaan ainoastaan tietoresurssien turvaamiseen pyrkivät tekijät. Kyberturvalli-

suus ottaa huomioon muutkin resurssit, joihin pystytään vaikuttamaan kybermaailman kautta. Informaatioturvallisuus voidaan siis nähdä kyberturvallisuuden yhtenä osa-alueena. (Von Solms & Van Niekerk, 2013).

Von Solms ja Van Niekerk määrittelevät, että kyberturvallisuuteen liittyen tieto sekä informaatio- ja viestintäteknologia ovat haavoittuvuuksien taustalla oleva syy. Heidän mukaansa kyberturvallisuus tulisi nähdä informaatioturvallisuuden laajennuksena. Kyberturvallisuuden tulisi heidän mukaansa olla enemmän kuin pelkästään tiedon turvaamista. Kyberturvallisuus on myös henkilöiden toiminnan suojaamista kyberympäristöön liittyen. Tämän lisäksi tulisi suojata resurssit, jotka altistuvat tieto- ja viestintätekniikan mukanaan tuomille haavoittuvuuksille. (Von Solms & Van Niekerk, 2013). Kyberturvallisuus tulee siis nähdä pelkän tiedon turvaamista laajempana kokonaisuutena, jossa otetaan lisäksi huomioon organisaation kaikki tieto- ja viestintäteknologiasta riippuvaiset toiminnot ja toimijat.

Lopuksi kuvataan lyhyesti kyberturvallisuuden tilaa tällä hetkellä. Kyberturvallisuuskeskuksen tietoturvaloukkausten tutkimiseen keskittyneille suomalaisille tietoturvayrityksille tekemän kyselyn mukaan organisaatioiden oma kyky havaita muun muassa kohdistettuja hyökkäyksiä on heikko. Havainto vastaa myös Kyberturvallisuuskeskuksen kokemuksia ja käsitystä maailmanlaajuisesta tilanteesta. (Viestintävirasto, 2014). Center for a New American Security (2013) kuvaa, että vain 6 % yrityksestä havaitsee edistyneet kyberhyökkäykset organisaation sisäisillä toimilla. Tämä tarkoittaa, että 94 % yrityksistä kuulee hyökkäyksistä viranomaisilta tai muulta taholta. Hyökkäyksiä ei havaita heti vaan hyökkäyksestä havainto hetkeen kuluu keskimäärin 416 päivää. (Center for a New American Security, 2013). Helsingin seudun kauppakamari (2015) laatimassa Yrityksiin kohdistuvat kyberuhat 2015 -tutkimuksessa kysyttiin vastaajilta kolmea suurinta estettä tehokkaan kyberturvallisuuden toteutumisessa. Suurin este tehokkaan kyberturvallisuuden toteutumiselle oli vastaajien mukaan käyttäjien piittaamattomuus tietoturvallisuudesta ja kyberuhista. Toiseksi suurin este oli kyberuhkiin liittyvän tiedon riittämättömyys. Kolmanneksi suurin este oli henkilökunnan kyberuhkiin liittyvän tieto-taidon ylläpito. Lisäksi neljänneksi esteeksi sijoittui turvallisuustoimiin ja menetelmiin liittyvän tiedon riittämättömyys. (Helsingin seudun kauppakamari, 2015). Vastaukset osoittavat, että esteiksi ei niinkään luokiteltu tekniikasta johtuvia esteitä vaan neljä suurinta estettä liittyvät inhimilliseen toimintaan ja ihmisten tieto-taitoon. Helsingin seudun kauppakamarin tutkimuksen kysymyksessä 1 kysyttiin suurimpia kyberturvallisuuden uhkia suomalaisille yrityksille. Suurimpana uhkana pidettiin phishing- ja haittaohjelmahyökkäyksiä. Toiseksi suurin uhka oli yhtiön työntekijöiden toiminnasta syntyvä sisäinen uhka. (Helsingin seudun kauppakamari, 2015). Helsingin seudun kauppakamarin tutkimuksen kaltaisiin tuloksiin ovat päätyneet myös von Solms & Niekerk (2013) ja Kraemer ym. (2009). Kraemer ym. (2009) mukaan teknisillä ratkaisuilla ei voida poistaa ihmisen toiminnasta johtuvia tekijöitä. Gordon ym. (2011) mukaan kyberturvallisuuden loukkauksilla on merkittäviä negatiivisia vaikutuksia, joiden kannalta keskeinen kysymys on, että kuinka paljon yritysten tulisi investoida kyberturvallisuuden toimintoihin. (Gordon ym., 2015).

Euroopan unionin verkko- ja tietoturvavirasto ENISA (European Union Agency for Network and Information Security) laatii vuosittain Threat Landscape -raportin, jossa analysoidaan kyber-uhat kuluneen 12 kuukauden ajalta. Viimeisin raportti on laadittu joulukuusta 2014 joulukuulle 2015. Raportin mukaan suurin osa hyökkäyksistä tehdään käyttäen matalan osaamistason vaativaa ja kehittymätöntä tai keskinkertaista tekniikkaa. (ENISA, 2016). Viron tietoturvallisuusviranomaisen RIA:n kyselyyn vastanneet IT -johtajat ja IT-turvallisuusjohtajat arvioivat järjestelmien toimintahäiriön organisaatioiden suurimmaksi riskiksi. Vastaajista 88 % arvioi organisaation riippuvuuden ICT-järjestelmistä korkeaksi tai erittäin korkeaksi. (RIA, 2014). IBM (2012) tutkimusraportin mukaan yritysten johto kiinnittää yhä enemmän huomiota informaatioteknologian häiriöihin ja niiden vaikutukseen yrityksen maineelle. Informaatioteknologian toimivuus vaikuttaa hyvin paljon asiakkaiden tyytyväisyyteen ja yrityksen maineeseen.

IBM (2012) on tutkinut yritysten johtajien näkemyksiä liittyen yrityksen maineeseen vaikuttavista informaatioteknologian riskeistä. Vastaajista 61 % piti tietomurtoja, -varkauksia ja kyberrikollisuutta vakavimpana uhkana ja jopa vakavampana uhkana kuin järjestelmien häiriötä. (IBM, 2012).

3.4 Finanssialan tulevaisuus

Finanssialan organisaatioiden kannalta tulevaisuuden keskeinen kilpailutekijä on kyberturvallisuus. Tutkimuksessa haastateltavat henkilöt ovat turvallisuusjohtajia suomalaisissa finanssialan organisaatioissa. Finanssialan toiminta on erityisen riippuvainen globaalien tietojärjestelmien toimivuudesta. Kyberturvallisuus, digitaalinen turvallisuus, luo sekä mahdollisuuksia että uhkia.

Kybertoimintaympäristön nykytilan ja tulevaisuuden ymmärtämiseksi tulee tuntea historia. Valkoisen talon entisen CIO:n (Chief information officer) Jason Healeyn (2013) mukaan eri maiden sotilaskoulutuksessa koulutetaan historiallisia sodankäynnin menetelmiä. Kyberturvallisuuden historian osalta samaa ei yhtä laajassa mittakaavassa tehdä. Healeyn mukaan historia toistaa myös kybermaailmassa itseään ja näin ollen tutkimuksen sekä historian ymmärtämisen osuutta ei voi vähätellä. Kybermaailma koetaan jatkuvasti muuttuvaksi ympäristöksi, jossa tulevaisuus on historiaa merkittävämpää ja kulman takana odottavaa suurta informaatiosotaa odotetaan. Tästä huolimatta mediassa suurennellaan kybersodan mahdollisuutta ja vähätellään pienempiä yrityksiin kohdistuvia hyökkäyksiä. (Healey, 2013).

EBA, Euroopan Unionin pankkiviranomainen, julkaisi tammikuussa 2016 Euroopan pankkijärjestelmän riskien arviointiraportin. Aikaisemmissa julkaisuissa on korostettu informaatioteknologiaan (ICT) liittyviä riskejä. Informaatioteknologian lisääntyessä ja monimutkaistuessa nopeasti kaikilla liiketoiminnan eri alueilla, ICT-riskit ovat edelleen keskeisessä asemassa operatiivisina riskeinä. EBA:n laatiman riskien arviointi kyselyn (RAQ, Risk Assessment Questionnaire) perusteella pankkeihin kohdistuneiden hyökkäysten kehittyneisyys ja monimutkaisuus ovat haasteita kyber- ja ICT-toimintojen jatkuvuuden-

hallinnalle. Haasteisiin on pyritty vastaamaan perustamalla kansallisia haavoittuvuuden testausrakenteita, jotka käyttävät uhkien tunnistamiseen tiedustelutietoa, jota kerätään julkisista ja kaupallisista lähteistä. EBA on laatimassa lisäksi EU -tason vähimmäisvaatimuksia ICT-riskien valvonnalle. Kansalliset lainsäädännöt ovat tällä hetkellä hyvin erilaisia ICT-infrastruktuuriin, digitaalisiin palveluihin ja palvelujen ulkoistamiseen liittyen. Haasteet liittyvät parhaisiin käytänteisiin ja standardeihin ICT-turvallisuudessa koko Euroopan Unionin alueella. (EBA, 2016).

3.4.1 Informaatioteknologia osana finanssialan toimintaympäristöä

Informaatioteknologia liittyy tulevaisuudessa yhä tiiviimmin organisaatioiden toimintaan kuten Lindström (2012) kuvaa:

1. internetin käyttäjien määrä on kasvussa ja moni uusista käyttäjistä ei tunne riskejä kybertoimintaympäristössä,

2. kybertoimintaympäristöön liitettyjen sovellusten määrä on kasvanut tasaisesti kahden viimeisen vuosikymmenen aikana,

3. kriittinen infrastruktuuri tulee yhä haavoittuvammaksi kyberhyökkäyksille,

4. haitalliset ohjelmat muuttuvat yhä kehittyneemmiksi ja helpommiksi käyttää ja

5. on olemassa yksilöitä ja ryhmiä, jotka tahtovat käyttää kybertoimintaympäristön mahdollisuuksia arveluttaviin tarkoituksiin.

Kujansivu, Lönnqvist, Jääskeläinen ja Sillanpää (2007) mukaan yritysten menestyminen perustuu tulevaisuudessa entistä voimakkaammin aineettomiin menestystekijöihin kuten osaamiseen, uudistumiskykyyn, palvelun laatuun, asiakastyytyväisyyteen, asiakasuskollisuuteen ja asiakkaan kokemaan lisäarvoon. Pohjolan (2015) mukaan rahoitus- ja vakuutuspalvelut ovat aineettomia ja tämän vuoksi digitoitavissa tieto- ja viestintäteknologian avulla. Walkerin (2014) mukaan pankit nähdään tällä hetkellä mediassa lähinnä negatiivisten uutisten kautta ja yritykset näkevät pankkitoiminnan kustannuseränä liiketoiminnassa. Tietotekniikalla pyritään korvaamaan tavanomaisia konttoreita ja henkilökuntaa. Kansalaiset käyttävät pankkipalveluita suurimmaksi osaksi maksaessaan laskuja. (Pohjola, 2015). Suomalaiset ovat siirtyneet käteisestä muihin maksutapoihin muuta maailmaa selvästi nopeammin (Pohjola 2015; Capgemini, 2015). Markkinat ovat vielä tällä hetkellä avoimet monenlaisille asiakkaille tarjottaville arvoille ja uuden finanssipalvelujen logiikan avulla voidaan löytää uusia menestykseen johtavia vaihtoehtoja. Uusien arvojen löytäminen vaatii kuitenkin ennen kaikkea luovuutta. (Puustinen, 2013). Walkerin (2014) ja Pohjolan (2015) mukaan tulevaisuudessakin tarvitaan finanssipalveluja, mutta ei välttämättä pankkeja ja vakuutusyhtiöitä. Ainoastaan 17 % pankkien johtajista kuvaa oman

pankkinsa olevan erittäin hyvin valmistautunut tulevaan. (PwC, 2014c). Uudet maksutavat ja asiakaskeskeisyys tuovat riskienhallinnalle uusia haasteita. PwC (2014b) ja PwC (2014c) kuvaavat kyberturvallisuuden olevan pankkien tärkeysjärjestyksen kärjessä.

Tulevaisuudessa pankkien kannalta uudet maksutavat ovat uhka, koska näitä pystyvät tarjoamaan pankkien lisäksi muutkin palveluntarjoajat. Toistaiseksi muut palveluntarjoajat ovat keskittyneet helposti automatisoitavissa olevien maksupalvelujen kehittämiseen. (Pohjola 2015). Uusien maksutapojen, kuten mobiilimaksaminen, voi Pohjolan (2015) mukaan ennakoida lisääntyvän nopeasti, koska internetin käyttäjämäärä kasvaa erityisesti kehitysmaissa älypuhelimien leviämisen myötä. Walkerin (2014) ja Pohjolan (2015) mukaan tulevaisuudessakin tarvitaan finanssipalveluja, mutta ei välttämättä pankkeja ja vakuutusyhtiöitä. Kaikki pankkien tarjoamat palvelut ovat tulevaisuudessa saatavissa verkosta, joten pankin fyysinen sijainti ei ole rajoite asiakashankinnalle, vaan teknologian, sääntöjen ja markkinointibudjetin asettamat rajat (PwC, 2014c). PwC (2014b) mukaan pankkien tulisi keskittyä enemmän asiakkaaseen ja tämän tarpeisiin digitaalisten kanavien kautta. PwC (2014c) tutkimuksessa 61 % pankkien johtajista totesi asiakaskeskeisen liiketoiminnan olevan erittäin tärkeä osa tulevaisuutta ja 75 % pankeista tekee investointeja tälle osa-alueella. Pankit joutuvat tekemään valintoja esimerkiksi sen suhteen, mitä asiakkaita he palvelevat ja miten kyetään tekemään liikevoittoa. Tämä edellyttää koko organisaation rakentamista ja kietomista asiakkaan ympärille (PwC, 2014c).

Ainoastaan 17 % pankkien johtajista kuvaa pankin olevan erittäin hyvin valmistautunut tulevaan. (PwC, 2014c). Uudet maksutavat ja asiakaskeskeisyys tuovat riskienhallinnalle uusia haasteita. PwC (2014b, 2014c) kuvaavat kyberturvallisuuden olevan pankkien tärkeysjärjestyksessä kärjessä. Vahva ja itsenäinen riskienhallintatoiminto, joka on keskittynyt keskeisten taloudellisten riskien seuraamiseen ja hallintaan on toiminnan kannalta kriittisessä roolissa. PwC (2014b) mukaan suurimmat esteet haasteeseen vastaamiseen löytyvät tarvittavasta taloudellisesta panostuksesta ja teknologian asettamista rajoitteista. Pankkitoiminnan voittajat resursoivat tulevaisuudessa merkittäviä summia kyberturvallisuuteen. 71 % pankki- ja talousmarkkinoiden toimitusjohtajista pitivät tutkimuksessa kyberturvallisuutta muita uhkia suurempana uhkana. Proaktiivinen toiminta on toiminnan kannalta elintärkeää ja vuoteen 2020 mennessä johtavat pankit ovatkin rakentaneet kyberturvallisuusstrategiansa, joka on sidottu liiketoiminnan tavoitteisiin, riskienhallinnan malleihin ja sääntöjen asettamiin vaatimuksiin. (PwC, 2014c). Puustinen (2013) tiivistää finanssipalvelujen tulevaisuuden logiikan seuraavasti: "Finanssiyritysten tulee tulevaisuudessa pyrkiä innovatiivisiin prosesseihin, jotka johtavat ratkaisuihin ja uusiin liiketoimintamahdollisuuksiin, asiakaslähtöiseen innovaatiotoimintaan, uudenlaisiin, yllättäviin ja aidosti ihmislähtöisiin toimintatapoihin ja tuotteiden tai palvelujen muodostamaan palveluun, jonka tarkoituksena on olla osa asiakkaan arkea" (Puustinen, 2013). Cederbergin (2015) mukaan kyberturvallisuudessa on huomattavissa seuraavat kymmenen suurta trendiä:

1. Digitalisaatio jatkuu ja tulee osaksi kaikkea elämäämme ja toimintaamme

2. Ihmiset tulevat yhä riippuvaisemmaksi digitaalisista palveluista

3. Modernit yhteiskunnat tulevat yhä haavoittuvammaksi tulevaisuudessa, koska monimutkaiset toisiinsa yhteydessä olevat järjestelmät on vaikea suojata kokonaisvaltaisesti.

4. Kyberturvallisuuden haasteet muuttuvat yhä kansainvälisemmiksi keskinäisestä riippuvuudesta johtuen.

5. Uudet teknologiset innovaatiot tulevat pääosin yksityiseltä sektorilta, joka turvallisuuden näkökulmasta sekä lisää että uhkaa turvallisuutta.

6. Kilpailu kyberaseista jatkuu samankaltaisesti kuin panssarivaunujen ja panssarintorjunta-aseiden välinen kilpailu.

7. Kyberrikollisuus haastaa yhteiskuntia ja taloudelliset menetykset tulevat kasvamaan entisestään. Yhteistyö rikollisuuden torjunnassa julkisen ja yksityisen sektorin välillä kehittyy.

8. Kybervallan käsitteellä tulee olemaan vaikutusta kansainväliseen politiikkaan ja valtataisteluun. Trendi tukee kyberaseiden kehitystä.

9. On erittäin todennäköistä, että tulevaisuudessa tulee olemaan kyberkatastrofi, joka muuttaa käsitystämme kyberturvallisuudesta.

10. Kybertoimintaympäristön tulevaisuuden voittajat kykenevät tasapainoilemaan turvallisuustarpeiden ja kybermaailman taloudellisen potentiaalin välillä.

Sisäministeriön (2016) raportin mukaan digitaalisen tiedon hyödyntäminen tulee määrittämään merkittävällä tavalla yhteisöjen ja kansakuntien aseman globaalissa kilpailussa. Tämä koskee niin perinteisiä elinkeinoelämän aloja, vientiteollisuutta kuin julkishallintoa. Perinteiset toimintatavat, toimialat ja markkinoiden rakenteet tulevat muuttumaan. Muutosta kiihdyttää esimerkiksi esineiden internet (Sisäministeriö, 2016). Muutos tulee seuraavien vuosien aikana näkymään muun muassa finanssialalla ja se tulee kiihdyttämään perustavalla tavalla yritysten välistä kilpailua liiketoiminnassa (Sisäministeriö, 2016).

Internet of Things (IoT, esineiden internet) on aikakautemme haaste kyberturvallisuudelle. Internet of Things -käsitettä käytti ensimmäiseksi Kevin Ashton (1999) RFID Journalin artikkelissa, jossa käsitettä kuvattiin osana toimitusketjujen johtamista. Giusto, Iera, Mora ja Atzori (2010) kuvaavat esineiden internetin integroivan virtuaalimaailman reaalimaailmaan käyttäen hyväksi erilaisia asioita tai objekteja kuten RFID-tunnisteita, sensoreita ja matkapuhelimia. Esineet tai asiat ovat yhteydessä toisiinsa ja ne jakavat keskenään yhteisen päämäärän. Näiden esineiden määrä nousee jatkuvasti ja tästä syystä hakkereilla on yhä enemmän mahdollisuuksia suunnata hyökkäyksiä. Yritykset eivät koe kyberturvallisuutta tällä hetkellä keskeiseksi kehityksen kohteeksi IoT

-tuotteiden (Internet of Things, esineiden internet) kehityksessään. Ainoastaan 48 % yrityksistä keskittyy turvaamaan IoT -tuotteidensa valmistusta kyberturvallisuuden näkökulmasta valmistusprosessin alusta alkaen ja 33 % yrityksistä uskoo, että tuotteet on turvattu tulevaisuuden kyberturvallisuusuhilta. (Capgemini, 2014). Intelin (2015) arvion mukaan esineiden internetiin (IoT, Internet of Things) kytkettyjen laitteiden määrä kasvaisi jopa 200 miljardiin vuoteen 2020 mennessä. Määrä on valtava, koska tämä tarkoittaisi 26 älykästä esinettä jokaista maapallolla asuvaa ihmistä kohden. Microsoftin arvion mukaan (2014) vuoteen 2025 mennessä 4,7 miljardia ihmistä on verkossa ja 75 % näistä ihmisistä on kehittyvistä maista.

IT -tutkimus- ja konsultointiyritys Gartner arvioi, että vuonna 2015 on maailmanlaajuisesti käytössä 4.9 miljardia verkkoon kytkettyä esinettä tai asiaa ja vuonna 2020 määrän arvioidaan nousevan 25 miljardiin (Gartner Inc., 2014). ENISA:n mukaan Internet of Things tulee tuoda käyttäjille mahdollisimman pitkälle kehitettynä niin, että tekniikka vaatii mahdollisimman vähän teknistä osaamista. Syvempi yhteistyö tekniikan tuottajien ja teknisten operaattoreiden välillä tulee yhä tärkeämmäksi. (ENISA, 2016). Nykyisin esineet kykenevät keräämään tietoa ihmisen kehosta, mutta tutkimuksessa on menetelmiä, joilla ihminen kykenee oman mielensä kautta kommunikoimaan esineiden kanssa. Koneiden yhteenliittymien nähdään tulevaisuudessa kykenevän oppimaan toisiltaan ja tekemään työtä ryhmissä, jolloin työn tehokkuus ja tieteellisten ongelmien ratkaisukyky paranevat. (Intel, 2015).

Taulukko 1 Internetin käyttäjät alueittain 2000 - 2015 (Internet World Stats, 2016)

Maanosa	**Asukasluku (2015)**	**Maailman väestöstä (%)**	**Internetin käyttäjiä (30.11.2015)**	**Käyttäjiä väestöstä (%)**	**Kasvu 2000-2015**
Afrikka	1,158,355,663	16 %	330,965,359	29 %	7231,300 %
Aasia	4,032,466,882	56 %	1,622,084,293	40 %	1319,100 %
Eurooppa	821,555,904	11 %	604,147,280	74 %	475 %
Lähi-Itä	236,137,235	3 %	123,172,132	52 %	3649,800 %
Pohjois-Amerikka	357,178,284	5 %	313,867,363	88 %	190 %
Etelä-Amerikka ja Karibia	617,049,712	9 %	344,824,199	56 %	1808,400 %
Australia ja Oseania	37,158,563	1 %	27,200,530	73 %	257 %
KOKO MAAILMA	7,259,902,243	100 %	3,366,261,156	46 %	833 %

Internetin käyttäjien määrä kasvaa edelleen. Vuosina 2000 - 2015 käyttäjämäärän kasvu on ollut voimakkainta Afrikassa, Lähi-Idässä, Aasiassa ja Etelä-Amerikassa (Taulukko 1). Käyttäjien osalta on huomattava, että kasvu on suurinta maanosissa, joissa koulutustaso, turvallisuuskulttuuri ja tietoisuus kybertoimintaympäristön haasteista eivät ole samalla tasolla kuin Euroopassa.

PwC:n laatiman tutkimuksen Sensing the future of Internet of Things (2014a) mukaan 20 % yrityksistä investoi liiketoiminnan kannalta tärkeisiin sensoreihin ja 14 % yrityksistä kokee sensoreiden olevan organisaation strategian kannalta tärkein yksittäinen kehittyvä teknologia seuraavaan 3 - 5 vuoden aikana. Finanssialalla 13 % yrityksistä aikoo investoida teknologiaan, jolla voidaan siirtää dataa esimerkiksi autosta telematiikan välityksellä auton omistajalle ja vakuutusyhtiölle. Telematiikka tarkoittaa Global Telematicsin määritelmän mukaan langattoman viestinnän ja informaatioteknologian yhdistämistä laajaalaisesti. Käsitettä käytetään usein puhuttaessa autojen käytettävyyden parantamisesta telekommunikaation keinoin, mutta tämä ei ole ainoa käyttötarkoitus. (Global Telematics, 2016; Nora & Minc, 1981). PwC (2014a) tutkimuksen mukaan finanssialalla sensoreita voidaan hyödyntää esimerkiksi ajoneuvon ajotietojen taltioinnissa, varastetun ajoneuvon hallinnassa ja kolarin sattuessa automaattisesti lähetettävässä tiedossa.

Microsoft (2014) kuvaa investoinnit kyberturvallisuuteen välttämättömiksi, koska teknologia kehittyy sekä käytettävän teknologian määrä lisääntyy ja vastaavasti teknisen asiantuntijuuden määrä vähenee. Gartner julkaisee vuosittain raportin kehittyvien teknologioiden kiinnostavuudesta. (Gartner, 2015). Vuoden 2015 osalta raportista löytyvät digitaalinen turvallisuus ja kryptovaluutat (Gartner, 2015). Useat yritykset kuten Dell, Expedia ja Paypal ovat ottaneet kryptovaluutan maksuvaihtoehdoksi. Kryptovaluutat ovat "matemaattisiin malleihin perustuvia, internetissä toimivia valuuttoja". Muutos kuvaa uskoa kryptovaluuttojen aikakauteen. (Kauppalehti, 24.10.2014). Digitaalisessa kaupassa fyysisen ja digitaalisen maailman rajan hämärtyminen sekä maailmojen sekoittuminen toisiinsa ovat merkittäviä tulevaisuuden haasteita (Gartner, 2015).

3.4.2 Rikollisuus

Tietoverkossa tapahtuvan rikollisuuden arvioidaan lisääntyvän. Rikosten helppo toteuttaminen sekä henkilöiden, pääomien ja tavaroiden vapaa liikkuvuus helpottavat rikollisten pakoilua. (Turvallisuuskomitea, 2015). Vakavissa kyberrikoksissa on usein kansainvälinen ulottuvuus ja ne aiheuttavat vakavan uhan yhteiskunnalle sekä elintärkeille tietojärjestelmille. Esimerkiksi sosiaali- ja terveydenhuolto järjestelmiin suunnattuna teot saattavat aiheuttaa uhan hengelle ja terveydelle. (Sisäministeriö, 2016). Rikolliset hyödyntävät globaalia kybertoimintaympäristöä haittaohjelmien kaupassa ja ihmisten henkilökohtaisten tietojen kuten identiteetti-, sairaus-, palvelujen kirjautumis- ja luottokorttitietojen kaupassa (McAfee Labs, 2015). Parhaat tilastot kyberrikollisuudesta tulevat finanssisektorilta, koska ala on tarkoin säädelty ja alalla kiinnitetään erityistä huomiota kyberturvallisuuteen. Esimerkiksi Meksikossa pankit menettävät

noin 93 miljoonaa dollaria ja Japanissa 110 miljoonaa dollaria ainoastaan verkossa tehtyjen petosten kautta. Yhdysvaltalaisen vähittäiskauppaketju Targetin hakkeroinnin arvioidaan maksaneen pankeille 200 miljoonaa dollaria. (McAfee Labs, 2014).

Euroopan poliisivirasto Europolin (2015) vuosittainen raportti ”Internet Organised Crime Threat Assessment (IOCTA)” kuvaa kyberrikollisuuden muuttuvan yhä aggressiivisemmaksi. Kriittiselle infrastruktuurille koituva uhka on merkittävä. Rikollisuuden eri muodot tietoverkossa vaativat tulevaisuudessa yhä vähemmän teknisiä taitoja. Esimerkiksi social engineering on yhä soveltuva keino aina petosten tekemisestä laajojen kyberhyökkäysten valmisteluun. (Europol, 2015). Poliisiammattikorkeakoulun katsauksessa 2014 (Niemi, 2014) kuvataan rikollisuuden rakenteellisten muutosten muokanneen rikollisuuden kokonaiskuvan aikaisempaa monipuolisemmaksi ja tietoliikennerikosten sekä tietoliikenneyhteyksiä hyödyntäen tehtävien rikosten olevan rikollisuusympäristön uusin ja vakavin uhka. Leppäsen ja Kankaanrannan (2014) mukaan taloudellista hyötyä tavoitteleva järjestäytynyt rikollisuus ja teollisuusvakoilu ovat uhkina vakavampia kuin uteliaan harrastelijan kokeilut päästä sisälle tietojärjestelmiin (Leppänen & Kankaaranta, 2014). Cederbergin (2015) mukaan modernien poliisiorganisaatioiden käytössä on uusia keinoja rikollisuuden torjumisessa ja tutkimisessa, kuten laajojen data-aineistojen käyttöön tarkoitettuja ohjelmistoja, joilla on mahdollista tuottaa ennakoivasti uudenlaisia näkemyksiä tulevista rikosilmiöistä. Sisäministeriön (2016) kansallisen riskiarvion 2015 mukaan kyberrikoksiin liittyvät riskit ovat joko terroristisessa tarkoituksessa tai hyötymistarkoituksessa tehtyjä kyberrikoksia ja kriittiseen infrastruktuuriin kohdistuvia kyberhyökkäyksiä. Rikos voi kohdistua tietojärjestelmien sisältämään tietoon tai kriittisen järjestelmän toimintaan. Viranomaisten, kuten poliisin tai sosiaali- ja terveysviranomaisten, tietojen päätyessä tietomurron yhteydessä julkisesti nähtäville saattaa viranomaisten toiminta vaarantua ja kansalaisten perusoikeudet kokea merkittävän loukkauksen. Haasteena kyberrikollisuuden torjunnassa on riittävien oikeudellisten toimivaltuuksien saaminen tiedon vaihtamiseksi ja yhteistyön parantamiseksi eri viranomaisten ja yksityisen sektorin välillä. (Sisäministeriö, 2016).

Kyberrikollisuuden osalta tilanne ei ole saavuttanut huippua. Liiketoiminta siirtyy yhä enemmän verkkoon, verkkoon liitettyjen laitteiden määrä kasvaa ja rikollisten käyttämät keinot kehittyvät ja muuttuvat yhä monimutkaisemmiksi. Kokonaisuus huomioiden voi ennakoida rikollisuuden määrän kiihtyvää kasvua. McAfee Labs (2014) tutkimusraportin mukaan kyberrikollisuuden määrä kasvaa edelleen. Lisäksi rikoksilla saavutettava hyöty ja toisaalta vahingon määrä kasvavat. Tämä tarkoittaa, että yritykset, jotka eivät onnistu omaisuutensa suojaamisessa ovat kilpailullisesti huonommassa asemassa. Kyberrikollisuus vähentää aiheuttamansa vahingon myötä investointeja innovointiin, koska liiketoiminnan voiton määrä vähenee. Mikäli mikään ei muutu tulee kyberrikollisuuden aiheuttamien tappioiden määrä kasvamaan. Tilanne on vielä korjattavissa, mutta on syytä pohtia millä keinoin mahdollista tulevaisuuden tapahtumien kulkua voidaan muuttaa. McAfee Labs -tutkimusraportin mukaan muutokselle on ennakoitavissa kaksi vaihtoehtoista lopputulosta:

a) Rikollisuuden kustannukset kehittyneissä maissa pysyvät suurelta osin tasaisina, vähintään yhdessä prosentissa bruttokansantuotteesta, mutta maailmanlaajuisesti kustannukset nousevat uusien tulijoiden ja kehitysmaiden alkavat kiihtyvällä tahdilla lisätä internetin käyttöä

b) Rikollisuuden kustannukset kehitysmaissa kasvavat palveluiden siirtyessä yhä enemmän verkkoon ja hakkereiden löytäessä uusia tapoja muuttaa rikoksilla haltuunsa saamat varat. (McAfee, 2014).

McAfee Labs (2014) tutkimuksessa ei löydetty uskottavaa skenaariota, jossa kyberrikollisuuden tappioiden voitaisiin nähdä vähenevän. Näkymät viittaavat pääasiassa hidastuvaan kasvuun ja suurempiin tappioihin. (McAfee Labs, 2014). Kyberrikoksien voidaan nähdä lisääntyvän jopa niin paljon, että nykyisillä voimavaroilla poliisin kyky selvittää kyberrikoksia laskee merkittävästi ja jopa niin, että kansalaisten ja yritysten luottamus kybertoimintaympäristöön heikentyy (Sisäministeriö, 2016).

3.4.3 Tiedonhankinta

Uhkiin liittyvän tiedon jakaminen on merkittävässä roolissa yleisesti kaikessa riskien hallinnassa. Tiedon jakamisen hyödyt ovat kiistattomat. Organisaatiot voivat oppia toisten organisaatioiden kokemuksista. Samankaltaisen kiinnostuksen kyberturvallisuuteen jakavien organisaatioiden kesken on jo nyt olemassa tiedon jakamisen kanavia. (Turvallisuuskomitea, 2015). Turvallisuuskomitean (2015) raportin mukaan erikoistuneista toimijoista koostuvat verkostot syntyvät tietyn tarpeen tyydyttämiseksi. Verkostot tarvitsevat verkostoon kuuluvien toimijoiden panoksen kuten informaation, jotta yhteinen tuotos kyetään tuottamaan. ENISA (2016) mukaan tiedonjakamisen kanavat ovat toistaiseksi kehittymättömiä. Ensinnäkin tiedon osalta tulisi pystyä jakamaan tarvittava tieto oikealle vastaanottajalle, mutta toisaalta kaikkea tietoa ei ole tarvetta jakaa kaikille mahdollisille vastaanottajille. Toiseksi kyberhyökkäyksien luonteelle on ominaista, että kyberhyökkäykset leviävät nopeammin kuin hyökkäyksiin liittyvä tiedustelutieto. Oikean tiedon saattaminen riittävällä nopeudella oikealle vastaanottajalle on tiedustelutiedon jakamisen kannalta keskeinen ongelma. ENISA (2016) raportissa kuvataan, että ensimmäiseksi tulisi pyrkiä saavuttamaan riittävä taso kyberturvallisuuden kyvyissä, toiseksi yhteinen ymmärrys ja vasta kolmanneksi pyrkiä lisääntyneeseen luottamukseen organisaatioiden välillä. (ENISA, 2016). Tulevaisuudessa eri maiden välinen yhteinen päämäärä tulisi suunnata yhteisten sääntöjen luomiseksi internetiin. Yhteiset lait ja standardit auttavat eri maita ymmärtämään ja ennakoimaan muiden maiden toimintaa. Yhteistyö ongelmien ratkaisemiseksi auttaa yhteisen yhä turvallisemman internetin rakentamisessa. (Microsoft, 2014). EBA (2016) mukaan Euroopan Unionissa ollaan aloittamassa yhteistyötä finanssialan instituutioiden, toimivallan omaavien viranomaisten ja ICT-palveluntarjoajien välillä. EBA on myös perustamassa EU:n sisäistä ICT-alan valvojien ja toimivaltaisten viranomaisten

verkostoa, jossa voidaan jakaa kokemuksia ja parhaita käytänteitä pilvipalveluiden käytössä ja yleisesti kyberriskeistä. (EBA, 2016).

3.4.4 Haasteita tulevaisuuden riskien arvioinnille

Cederbergin (2015) mukaan tulevaisuudessa voittajina selviävät organisaatiot, jotka kykenevät luomaan monipuolisen ja kattavan turvallisuusratkaisun. Turvallisuusratkaisu tulee koostumaan markkinatalouden lähestymistavasta, alan parhaista osaajista ja kyvystä toimia vaivattomasti kaikkien sidosryhmien kanssa kansainvälisessä ympäristössä. Center for a New American Security (2013) mukaan kyberturvallisuus on tulevaisuudessa siirtymässä passiivisesta, haitallisten tapahtumien ja loukkauksien reagoinnista, aktiiviseen tapahtumien ennalta estämiseen eli aktiiviseen kyberpuolustukseen. Muutos johtuu sofistikoituneiden hyökkääjien ja valtiollisen vakoilun lisääntymisestä verkossa. Aikaisempi passiivinen toimintakulttuuri ei toimi nykyisessä toimintaympäristössä. (Center for a New American Security, 2013). Lindströmin (2012) mukaan kybertoimintaympäristön asettamat haasteet vaativat tulevaisuudessa jatkuvaa näkökulmien välistä harkintaa. Helppoja vastauksia ei ole olemassa, joten turvallisuuspolitiikoiden laatijoiden ja lakiasiantuntijoiden tulee jatkossakin pohtia, tuleeko internetin hallinnoinnin osalta laatia säännellympi järjestelmä vai ei. Riippumatta siitä mihin lopputulokseen päädytään, tulee päätöksillä olemaan pitkäaikaiset vaikutukset kyberturvallisuuden ja tulevaisuuden kybertoimintaympäristön käytön osalta. (Lindström, 2012).

Cederbergin ja Erosen (2015) mukaan yhteiskunnan kannalta kokonaisvaltainen lähestymistapa turvallisuuteen tarvitsee pitkäjänteistä kansallisten kyvykkyyksien rakentamista. Organisaatioiden tai hallintojen sisäiset ponnistelut eivät ole enää riittäviä. Koko yhteiskunnan tulee sitoutua yhteisiin tavoitteisiin. Suomen hybridipuolustus on esimerkki turvallisuuden kokonaiskuvan hyödyntämisestä. Yhteistyö valtion, yritysten ja muiden siviiliorganisaatioiden välillä on tiivistä. (Cederberg & Eronen, 2015). Suomen kansantalouden kilpailukyvyn ja tuottavuuden kannalta on merkityksellistä, millaiseksi suomalaisten rooli kehittyy digitaalisten palveluiden globaaleissa arvoketjuissa. Tietoturvalla tulee kaikissa tapauksissa olemaan erittäin suuri merkitys yhteiskunnalliselle kehitykselle sekä ihmisten turvallisuudelle. (Sisäministeriö, 2016). Roolin kehittymisessä on huomioitava globaalin toimintaympäristön vaatimukset keskeisten kilpailutekijöiden tunnistamiseksi.

Organisaatioiden johdolta ja päätöksenteolta tulevaisuus tulee vaatimaan paljon. Tutkielman näkökulman kannalta ajateltuna digitaalinen maailma luo uusia osaamistarpeita organisaatioiden johdossa, koska muun muassa CSBC:n (2014) mukaan kyberturvallisuus ei ole enää IT-osaston ongelma vaan organisaation johdon ongelma. Killingin ja Malnightin (2005) kuvaus ylimmän johdon roolista organisaatioiden menestyksessä kuvaa hyvin suurempien kokonaisuuksien johtajuutta. Johdon tulee hallita kaksi asiaa samaan aikaan. Ensinnäkin johtajien tulee kyetä erottamaan ja tunnistamaan, miten voittaa tärkeimmät ja keskeisimmät taistelut. Toiseksi johtajien tulee kyetä hahmottamaan, miten organisaatiota viedään kohti pidemmän aikavälin tavoitteita. Tässä korostuu

organisaatioiden tehokkuuden parantaminen ja toimintojen jakautumisen, niin sanotun siiloutumisen, välttäminen. Optimaalisessa tilanteessa organisaatio voittaa taisteluita ja kehittää organisaatioita samanaikaisesti. (Killing & Malnight, 2005).

Kustannukset ja palveluilla saavutettava hyöty ovat aina merkittävässä asemassa perusteltaessa turvallisuustoimia ympäristössä, jossa kannattavuuden saavuttaminen on hankalaa. EBA:n RAQ-kyselyn perusteella vastaajista vain harva on vastannut ICT-riskeihin lisäämällä investointeja ICT-turvallisuuteen ja jatkuvuuden hallintaan. Vastauksien perusteella budjetin rajoitteet ovat toiseksi suurin haaste ICT- jatkuvuuden kehittämisessä. (EBA, 2016). Toiminnan jatkuvuuden kannalta on ratkaisevaa, että pankit jatkavat ICT -investointejaan ja kehittävät ICT-hallintoaan ja riskikulttuuriaan (EBA, 2016). PwC (2014c) mukaan pankkien puutteelliset resurssit kyberturvallisuuden osalta tuo vuoteen 2020 mennessä mukanaan kolmansien osapuolien kanssa tehtävän yhteistyön. Pankit luovat yhteistyö- ja kumppanuussopimuksia yhdessä turvallisuusalan toimijoiden kanssa. Suomessa esimerkkinä on vakuutusyhtiö IF:n ja IBM:n yhteistyö tietoturvavakuutustoiminnassa. IF:n tarjoama tietoturvavakuutus kattaa yritykseen kohdistuneen tietoverkkorikoksen aiheuttaman vahingon, asiantuntija-avun ja tapahtumista aiheutuneita kuluja. (If, 2016).

3.5 Toimintaympäristön riskien tunnistaminen

Uusien ja kehittyvien ilmiöiden sekä syntyvien uhkien ennustaminen ja hahmottaminen on haasteellista. Kybertoimintaympäristö on vaikuttanut fyysiseen maailmaan tuomalla mukanaan ennalta-arvaamattomia piirteitä. Uhkien lisäksi on toisaalta muistettava kybertoimintaympäristön mukanaan tuomat uudet mahdollisuudet. (Toivonen & Kuusisto, 2014). Saatavuus tuo yhteiskuntaamme täysin uusia ulottuvuuksia. Aiemmin tarkoin harkituilla oikea aikaisilla teoilla saatiin aikaiseksi ilmiöitä ja yhteiskunnan toiminnan muutoksia. Nykyisin maailmaa muokkaavat teot voivat syntyä missä päin maailmaa tahansa, spontaanisti ja ennen kaikkea yhden henkilön tekojen seurauksena. Mannermaa (2008) kuvaa kirjassaan "Jokuveli: Elämä ja vaikuttaminen ubiikkiyhteiskunnassa" tietoon liittyviä ilmiöitä. Mannermaan (2008) kuvaaman Woody Allen -yhteiskunnan mukaan tulevaisuudessa yhteiskunta on kaikilta osin aina auki, 24-tuntia vuorokaudessa seitsemänä päivänä viikossa. Tulevaisuuden yhteiskunnan malli mahdollistaa elämän rytmittämisen omien luontaisten ominaisuuksien ja esimerkiksi työtehtävien perusteella. Yhteiskunnan eri toimijoilla on toisaalta omat tarpeensa ja halunsa rajoittaa kyseisen kaltaista mallia. (Mannermaa, 2008). Mannermaa kuvaa instantismiksi ilmiötä, jossa palveluja tai tapahtumia ei enää odoteta, vaan kaikki on saatavilla heti. Ilmiö liittyy tiedon saatavuuteen, mutta myös muuhun ihmisen toimintaan, kuten pankkitoimintaan tai kaupassa käyntiin ja jonottamiseen ostosten kanssa. Ihminen voi paikasta riippumatta käyttää viihdepalveluja, tehdä töitä tai opiskella. (Mannermaa, 2008). Kolmanneksi Mannermaa kuvaa simplismin. Simplismillä Man-

nermaa tarkoittaa yksinkertaisuuden filosofiaa, jonka mukaan tulevaisuuden yhteiskunnassa pärjäävät henkilöt, jotka:

a) pystyvät tekemään päätöksen rajaamalla pois kaiken turhan,

b) unohtavat kaiken ylimääräisen tarpeettoman tiedon,

c) loisimalla eli käytännössä ulkoistamalla työn tunnollisemmille yhteiskunnan jäsenille,

d) käyttämällä toisia yhteiskunnan jäseniä asiantuntijoina, konsultteina. (Mannermaa, 2008).

Mannermaan tietoon liittyvät tulevaisuudenkuvat osoittavat, että ennakointi ja päätöksenteko tulevaisuuden kybertoimintaympäristössä on haastavaa. Killingin ja Malnightin (2005) Must Win Battles -strategiaopissa valitaan organisaation kannalta keskeisiä alueita ja luodaan toimintatapoja, joilla suunnataan organisaation resursseja päämäärän kannalta tärkeimpiin ja olennaisiin asioihin. Organisaation kannalta menetelmä yksinkertaistaa toimintamalleja ja auttaa keskittymään ennalta määriteltyihin kehittämistoimenpiteisiin, koska aktiivisesti seurattavia painopistealueet on valittu. Must win battles -opin kaltaista lähestymistapaa tukee Mannermaan (2008) näkemys tarpeettoman tiedon huomiotta jättämisestä eli simplismistä.

Baskervillen (1991) mukaan riskianalyysi on organisaation johdon ja informaatioturvallisuuden ammattilaisten kommunikaation väline. Riskianalyysillä pyritään vastaamaan ennakoimalla tulevaisuuden tapahtumiin yrityksen strategian mukaisesti (Baskerville, 1991). Borum, Felker, Kern, Dennesen ja Feyes (2015) mukaan organisaatioiden investoinnit teknologiaan, kuten palomuureihin ja tunkeutumisen havaitsemisjärjestelmiin (IDS), ovat soveltuvia, mutta riittämättömiä. Jatkuvassa muutoksessa tiedustelu on tärkeä tekijä. Kybertiedustelulla pyritään havaitsemaan mahdolliset riskit ja uhat kyberturvallisuudelle jo ennen hyökkäystä. Gordon ym. (2003) mukaan kyberturvallisuuden uhkien ehkäisemisessä organisaatioiden tulee aloittaa riskien arviointi määrittelemällä uhat sekä haavoittuvuudet omissa tietojärjestelmissään, että järjestelmissään olevan tiedon arvo. Strateginen kybertiedustelu vähentää mahdollisia organisaation toiminnan riskejä ja pyrkii turvaamaan yrityksen tärkeimpiä tietovarantoja, assetteja. Strateginen kybertiedustelu on proaktiivinen ja mukautuva malli kyberpuolustuksen parantamiseksi. (Borum ym., 2015). Mannermaa (1999) ja McAfeen (2014) raportti kuvaavat tulevaisuustyöskentelyn olevan maailmalla usein systemaattinen osa yrityksen strategista suunnittelua ja johtamista ja näin ollen osa organisaatioiden riskien arviointia, koska strateginen suunnittelu käyttää tulevaisuudentutkimuksen menetelmiä ja toisinpäin.

Riskianalyysi pyrkii menetelmänä löytämään vastauksia samankaltaisella tavalla, kuin tulevaisuudentutkimus tieteenalana. Tulevaisuudentutkimus voidaan nähdä joukkona "erilaisia metodologisia lähestymistapoja, joita yhdistää käyttäjän eksplisiittinen pyrkimys tuottaa niiden avulla perusteltuja, rationaali-

sia väitteitä tulevaisuudesta" (Mannermaa, 1991). Mannermaan (1991) ja alun perin Roy Amaran (1981) kolmen perusperiaatteen mukaan:

1. Tulevaisuus ei ole ennakoitavissa.

2. Tulevaisuus ei ole ennalta määrätty.

3. Tulevaisuuteen voidaan vaikuttaa valinnoilla.

Mannermaa (1991) jakaa tulevaisuudentutkimuksen paradigmat deskriptiiviseen, skenaarioparadigmojen ja evolutionaariseen tulevaisuudentutkimukseen. Mannermaan (1999) mukaan deskriptiivinen, kuvaileva tulevaisuudentutkimus, pitää sisällään menneisyydestä kulkevien kehityslinjojen jatkamista kohti tulevaisuutta. Kehityslinjojen kautta muodostetaan korkean toteutumistodennäköisyyden sisältäviä ennusteita. Näkökulma perustuu siten siihen, että tapahtumat ja aika käsitetään koostuvaksi erilaisista säännönmukaisesti toistuvista tai kehittyvistä ilmiöistä, joista on mahdollista saada tietoa seuraamalla niiden kehitystä taaksepäin tarpeeksi pitkälle ja vetämällä siitä luotettavia johtopäätöksiä tulevan kehityksen suunnan ja määrän ennustamiseksi. (Mannermaa, 1999; Rubin, 2000). Skenaarioparadigman mukaisesti tulevaisuus voidaan nähdä erilaisina vaihtoehtoina, jolloin tarkastellaan vaihtoehtoja ja vaihtoehtojen kehitystä skenaariomenetelmien avulla (Mannermaa, 1991). Evolutionaarisen tulevaisuudentutkimuksen paradigma kuvaa sosiaalisen kehityksen tai ihmisyhteisöjen muuttumista ilman suoraviivaista kaavaa. Muutos tapahtuu toisin sanoen ennakoimattomasti ja muuttuvalla vauhdilla. (Mannermaa, 1991).

Amaran (1981) sekä myöhemmin Mannermaan (1991) periaatteet 2: "Tulevaisuus ei ole ennalta määrätty" ja 3: "Tulevaisuuteen voidaan vaikuttaa valinnoilla" kuvaavat organisaatioiden proaktiivista toimintaa. Tietoyhteiskunnan ja tätä kautta kybertoimintaympäristön kehityksen mukana pysyminen edellyttää proaktiivisuutta. Rubin (2000) mukaan proaktiivisuus on kyky ja halu olla mukana tulevaisuuden tekemisessä ja suunnittelemisessa. Proaktiivisuus on myös sen tiedostamista, että tulevaisuuden suuntaan ja laatuun voidaan vaikuttaa. Organisaatio voi valita omat reaktionsa, joka taas aiheuttaa muualla yhteiskunnassamme vastareaktioita. Virheisiin reagoiminen vaikuttaa väistämättä virheen seurauksiin. (Rubin, 2000). Proaktiivisuuteen liittyvät oma aktiivisuus ja vastuu. Väitettä tukee myös kohta 1, "Tulevaisuus ei ole ennakoitavissa" (Amara, 1981; Mannermaa, 1991). Esimerkiksi Mintzbergin (1985) mukaan organisaatiot ovat poliittisen konfliktin osapuolia. Reaktioita ja vastareaktioita tulee organisaatiosta riippumatta, joten organisaatiot ovat tahtomattaankin globaalien tapahtumien seurausten vaikutuksen alla. Sitran (2016) julkaiseman "Megatrendit 2016 - tulevaisuus tapahtuu nyt" -muistion mukaan ennakointi tulevaisuuden kehityssuunnista on vaikeaa, mutta parhaiten ennakointityössä onnistuvat ne, jotka pyrkivät rakentamaan tulevaisuutta toiveidensa ja visioidensa mukaiseksi (Sitra, 2016).

Sosiaalitieteilijöiden mukaan riskianalyysin tulee ottaa teknisten ja laskennallisten tekijöiden lisäksi huomioon sosiaaliset tekijät, koska riski voi tarkoittaa eri yhteyksissä ja eri henkilöille eri asiaa (Royal Society, 1992). Tieto si-

sältää sekä teknisiä että sosiaalisia tekijöitä (Frosdick, 1997). Riskien analysoinnin tarkkuuden maksimoimiseksi on otettava huomioon saatavilla oleva tieto. Baskervillen (1991) ja Siposen (2015) mukaan tilastollisesta tutkimuksesta tietojärjestelmätieteessä puuttuu tutkimuksellinen tarkkuus, koska ei ole saatavissa vertailukelpoista materiaalia. Riskianalyysin tilastollisen tutkimuksen yhdistäminen muuhun saatavilla olevaan tietoon mahdollistaa perusteltujen päätösten tekemisen. Bandyopadhyay ym. (1999) näkevät riskianalyysille varteenotettavana vaihtoehtona holistisen näkökulman aiempien osittaisten ja epätodellisten tutkimustulosten tilalla (Bandyopadhyay ym., 1999). Gerberin ja Von Solmsin (2005) mukaan informaatioteknologia tulee nähdä kokonaisuutena, jotta organisaation tietoturvallisuusvaatimukset voidaan huomioida yksilöllisesti. Riskianalyysiä laadittaessa tulee huomioida sekä organisaation aineelliset, että aineettomat varat, jotta analyysi huomioi lainsäädännölliset, kulttuuriin perustuvat ja muut sosiologiset tekijät. (Gerber & Von Solms 2005).

Tutkimusraporttien pohjalta käsitys riskianalyysin puutteista vahvistuu. Baskervillen (1991) ja Siposen (2015) mukaan tilastollisesta tutkimuksesta tietojärjestelmätieteessä puuttuu tutkimuksellinen tarkkuus. Riskianalyysin menetelmät tietoturvallisuuden osalta on aiemmin määritetty muilta tieteenaloilta lainattujen menetelmien avulla. Tienarin ja Piekkarin (2011) mukaan määrämuotoisen informaation tuottaminen saattaa muodostua organisaatioissa itsetarkoitukseksi kuten Balanced Scorecard -menetelmässä. Balanced Scorecard, BSC tasapainotettu tuloskortti, on menetelmä erilaisten mittareiden seuraamiseen ja päätösten tekemiseen mittareista saadun tiedon perusteella (Kaplan & Norton, 1992). Organisaation johto saa käyttöönsä mittareiden datan muualta. Strategiaa mystifioidaan ja sen kuvataan olevan vain pienen joukon tehtävä, joka jatkuu pitkiä aikoja yrityksissä kuitenkaan ottamatta huomioon sen enempää muutoksia toimintaympäristössä. Seurauksena on, että strategiat eivät toteudu, henkilöstö ei toteuta strategiaa ja asiakkaat vain ihmettelevät. (Tienari & Piekkari, 2011). Strategia ja tietoturvapolitiikka omaavat näin ollen samankaltaisia ongelmia implementoinnissa. Virheitä välttäen tarkasti tehdyt strategiat sekä tietoturvapolitiikat laaditaan henkilöstölle, joka ei kuitenkaan toteuta johdon näkemyksiä. Strategiat voivat jäädä tästä johtuen vain pienen joukon laatimaksi ja arkistoitavaksi asiakirjaksi. Tienarin ja Piekkarin (2011) mukaan strategiatyössä tuleekin ottaa paremmin huomioon inhimillisten tekijöiden ja ihmisten sosiaalisten tarpeiden huomioiminen ja käsitteleminen.

Tietoturvallisuuden kehitys on nopeaa ja tästä syystä useissa tutkimuksissa (mm. Baskerville, 1991; Bandyopadhyay ym., 1999; Gerber & Von Solms, 2005) ehdotetaan suurempien kokonaisuuksien huomioimista riskianalyysia laadittaessa. Virhe voi esiintyä sosio-teknisissä järjestelmissä niin ihmisen toiminnan kuin tekniikan toimintahäiriön seurauksena (Turner, 1978). Tästä johtuen riskianalyysissä täytyy huomioida sekä tekniset että sosiaaliset tekijät. Tulevaisuuden tutkimus voidaan nähdä joukkona “erilaisia metodologisia lähestymistapoja, joita yhdistää käyttäjän eksplisiittinen pyrkimys tuottaa niiden avulla perusteltuja, rationaalisia väitteitä tulevaisuudesta". (Mannermaa, 1991). Riskianalyysin tarkoitus on uhkien ennakointi, tunnistaminen ja keinojen kartoittaminen mahdollisia vaaroja vastaan. Aiemman tutkimuksen perusteella riskianalyysissä on mahdollista hyödyntää tulevaisuuden tutkimuksen mene-

telmiä. Päätöksenteon tueksi on tällöin mahdollista hyödyntää kerättyä tutkimustietoa yli tieteenalojen rajojen.

4 RISKIEN ARVIOINNIN MENETELMÄT

Tutkimuksessa esitellään neljä riskien arvioinnin menetelmää sekä kaksi vaihtoehtoista menetelmää. Nämä menetelmät toimivat osaltaan perustana tutkimuksessa muodostettavalle uudelle riskien arvioinnin mallille.

4.1 Tutkimukseen valitut standardit

Kaksi tutkimukseen valituista menetelmistä on yleisiä riskienhallinnan menetelmiä (ISO 31000:2009, FERMA) ja kaksi menetelmää on suunnattu nimenomaan tietoturvallisuuteen keskittyvään riskienhallintaan (NIST, OCTAVE Allegro).

Mallin muodostamisen tueksi valittiin tietoisesti sekä yleisiä riskienhallinnan standardeja, että erityisesti tietoturvallisuuteen keskittyviä standardeja. Siitä huolimatta, että tutkimus tehtiin tietoturvajohtajan näkökulmasta, haluttiin malli muodostaa siten, että se soveltuisi organisaation muidenkin osa-alueiden käyttöön. Perustelut tutkimuksessa käytettävien standardien valinnoille on esitelty taulukossa 2.

Taulukko 2 Valitut riskienhallinnan ja –arvioinnin menetelmät sekä niiden valinnan perustelut

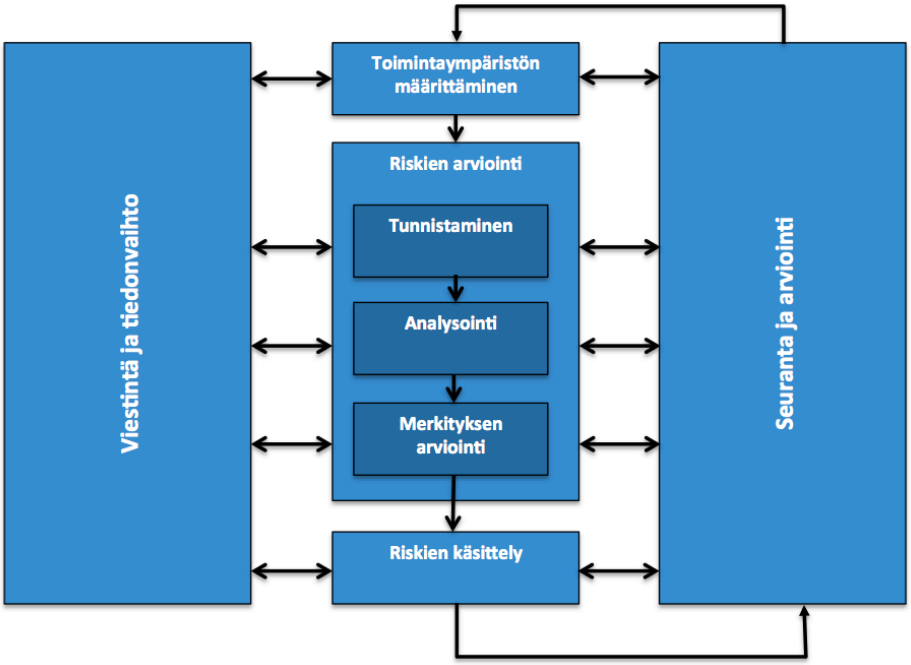
Standardi	Perustelu / kuvailu
ISO 31000	*Yleinen ja **laajasti käytössä oleva standardi**, joka tarjoaa laajasti hyväksytyt perusteet ja suuntaviivat riskienhallinnalle.*
NIST (Special Publication 800-30)	*Yhdysvaltalaisen viraston kehittämä ja ylläpitämä standardi, joka on **laajasti käytössä** etenkin Pohjois-Amerikassa. NIST tarjoaa kattavan ja yksityiskohtaisen menetelmän tietoturvallisuuteen liittyvään riskienhallintaan ja -arviointiin.*
OCTAVE Allegro	*Carnegie Mellon yliopiston kehittämä, **laajasti käytössä oleva tietoturvallisuuteen keskittyvä riskienhallinnan menetelmä**. OCTAVE-menetelmät soveltuvat myös organisaatiolle, joiden resurssit eivät mahdollista erillisten riskienhallinnan osastojen muodostamista.*
FERMA	***Eurooppalaisten riskienhallinnan kattojärjestöjen muodostama yleinen riskienhallinnan standardi**, muun muassa Suomen Riskienhallintayhdistys on FERMA:n jäsen.*

Mallin muodostamiseen liittyvien standardien valinnalla pyrittiin saamaan riittävän kattava kokonaiskuva yleisesti käytössä olevista standardeista ja sitä kautta muodostamaan synteesi, joka toimisi osaltaan mallin perustana.
Tutkimuksessa käytetyt standardit ja niiden mukaiset riskienhallinnan ja -arvioinnin menetelmät on kuvattu tarkemmin tutkimusraportin liitteissä (liitteet 6-9). Seuraavat luvut tarjoavat ainoastaan yleiskatsauksen valittuihin standardeihin.

4.1.1 ISO 31000:2009

ISO (the International Organisation for Standardization) on kansainvälinen standardisoimisjärjestö. Se on itsenäinen, ei-valtiollinen järjestö, jonka tarkoituksena on asiantuntijoiden ammattitaidon kautta jakaa tietoa ja kehittää merkityksellisiä kansainvälisiä standardeja tukemaan innovaatioita ja tarjoamaan ratkaisuja globaaleihin haasteisiin. (ISO, 2009; http://www.iso.org/iso/home/about.htm, 2016). ISO:n standardi 31000:2009 on yleinen riskienhallinnan standardi ja se soveltuu laajasti erilaisille organisaatioille ja toimijoille.

ISO (2009) mukaan tätä standardia ei ole laadittu millekään tietylle organisaatiolle tai ryhmälle, vaan sen periaatteet ovat sovellettavissa kenelle tahansa ja minkä tyyppisiin riskeihin tahansa. (ISO, 2009). ISO (2009) kuvaa riskienhallinnan prosessin kuvion 5 kaltaiseksi.



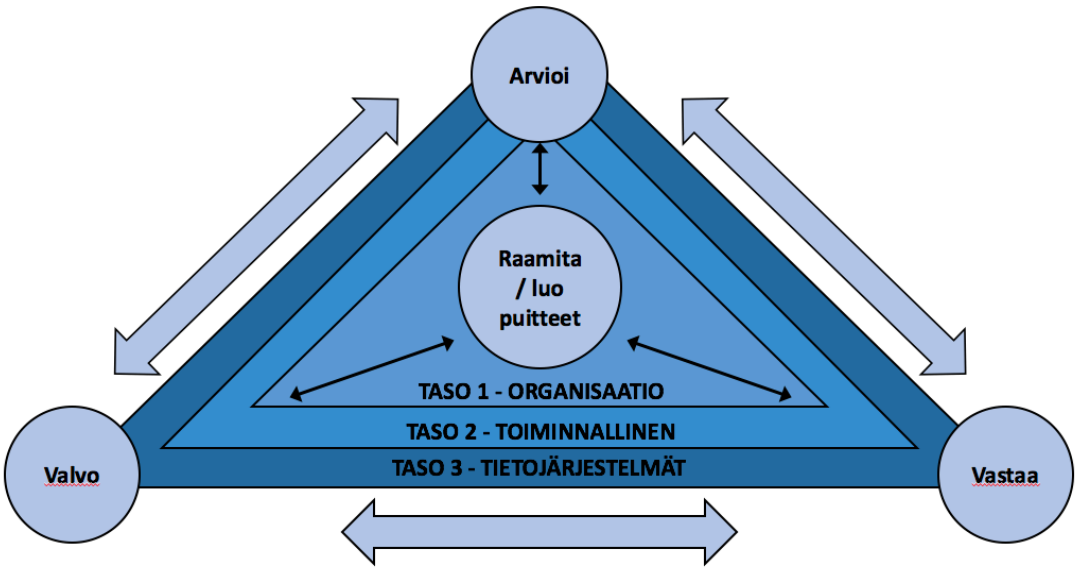
KUVIO 5 ISO 31000:2009 riskienhallinnan prosessi (ISO, 2009, 14)

ISO 31000:2009 on esitelty tarkemmin liitteessä 6.

4.1.2 NIST

NIST (National Institute of Standards and Technology) on yhdysvaltalainen virasto, joka toimii kauppaministeriön alaisuudessa. Sen tehtävänä on kehittää innovaatioita ja kilpailukykyä muun muassa tieteen, standardien ja teknologian kautta. (http://www.nist.gov/public_affairs/general_information.cfm, 2016). Special Publication 800 -sarja käsittelee NIST:n ITL:n (The Information Technology Laboratory) ohjeita, suosituksia ja standardeja liittyen informaatioturvallisuuteen. ITL:n vastuualueeseen kuuluu muun muassa tieto- ja viestintäteknisten järjestelmien johtamiseen ja teknisiin seikkoihin liittyvien standardien ja suositusten kehittäminen.

Tässä tutkimuksessa esiteltävä NIST:n menetelmä riskienhallinnan toteuttamiseen perustuu pääosin asiakirjaan "NIST Special Publication 800-39: Managing Information Security Risk". Tämä asiakirja on NIST:n merkittävin tietoturvallisuuteen liittyvä standardi, jonka tarkoituksena on tarjota ohjausta informaatioturvallisuuteen liittyvien riskien hallintaan. NIST:n riskienhallintastandardi ei ole yleinen koko riskienhallinnan kattava menetelmä, vaan se keskittyy nimenomaan informaatioturvallisuuden alueeseen. Menetelmää tulisi siis käyttää osana jotain laajempaa riskienhallinnan menetelmää. NIST käsittää riskienhallinnan ja siihen liittyvän riskien arvioinnin koko organisaation läpäisevänä prosessina, joka on esitelty kuviossa 6.



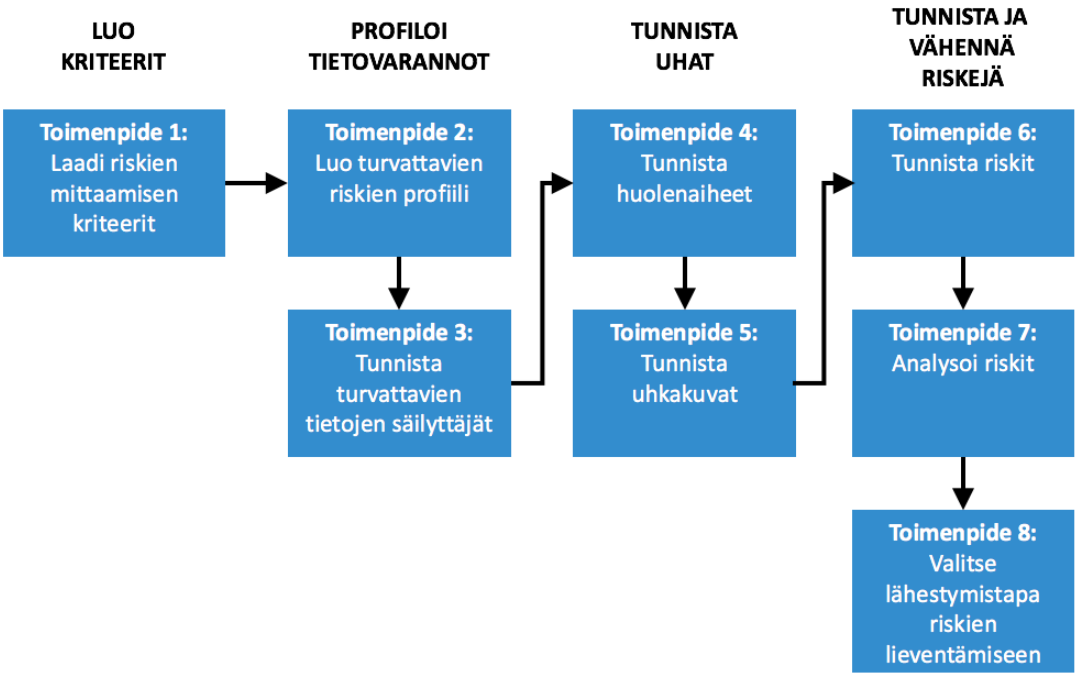
KUVIO 6 NIST:n riskienhallinnan prosessi (NIST, 2011, 32)

NIST:n standardi on esitelty tarkemmin liitteessä 7.

4.1.3 OCTAVE Allegro

OCTAVE Allegro on Carnegie Mellon yliopiston Software Engineering Instituten (SEI) uusin OCTAVE -menetelmä. OCTAVE tulee sanoista *Operationally Critical Threat, Asset, and Vulnerability Evaluation.* Suomeksi tämä tarkoittaa operatiivisesti kriittisten uhkien, suojattavien kohteiden ja haavoittuvuuksien arviointia.

OCTAVE -menetelmien tavoite ja keskeinen hyöty on mahdollisuus yhdistää organisaation tavoitteet tietoturvallisuuden tavoitteisiin. Onnistuneesti menetelmää käyttäneet organisaatiot kykenevät organisaation ja operatiivisen näkökulman liittämiseen tietoturvallisuuden riskien hallinnassa, jolloin toiminta muuttuu haavoittuvuuksien hallinnasta ja reaktiivisesta toiminnasta kohti suurempaa tietoturvallisuuden riskienhallinnan kokonaisuutta. (Caralli, Stevens, Young & Wilson, 2007). OCTAVE Allegro koostuu kahdeksasta toisiaan seuraavasta toimenpiteestä, jotka on jaettu neljään eri vaiheeseen. Kuviossa 7 kuvataan OCTAVE Allegron toimenpiteet ja vaiheet.



KUVIO 7 OCTAVE Allegron toimenpiteet ja vaiheet (Caralli ym., 2007)

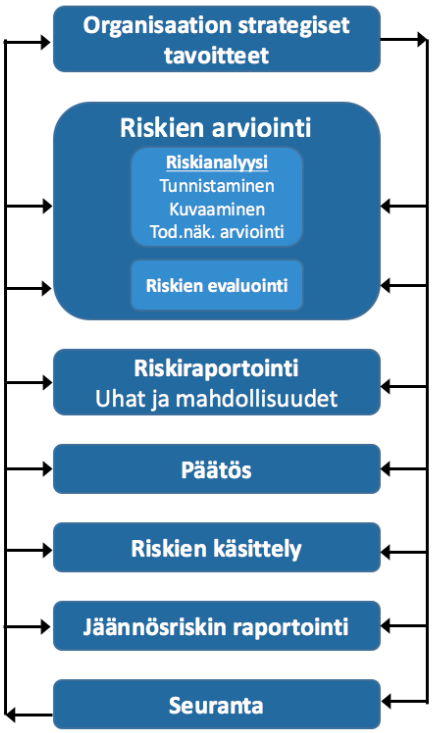
OCTAVE Allegro -standardi on kuvattu tarkemmin liitteessä 8.

4.1.4 FERMA

FERMA on kansallisten riskienhallintayhdistysten kattojärjestö, jonka tarkoitus on optimoida jäsenyhdistystensä toimintaa kansallisten rajojen ulkopuolella tarjoamalla muun muassa yhteistyöverkoston. FERMA on perustettu vuonna 1974 ja on johtava riskienhallinnan organisaatio Euroopassa. (FERMA, 2016). Suomen Riskienhallintayhdistys on FERMA:n jäsenyhdistys (Suomen Riskienhallintayhdistys, 2016).

FERMA -standardissa prosessi perustuu organisaation toiminnan tavoitteisiin. Organisaation toimijoille määritellään roolit ja vastuut riskien valvonnassa ja tiedottamisessa.

Riskienhallinnan prosessissa organisaatiot suunnitelmallisesti pyrkivät osoittamaan toimintaansa liittyvät riskit. Riskienhallinnan tavoitteena on saavuttaa jatkuvaa hyötyä kaikessa organisaation toiminnassa. Hyvän riskienhallinnan tavoitteena on riskien tunnistaminen sekä käsittely ja tätä kautta hyödyn tuottaminen organisaation toiminnalle. Riskienhallinnan tavoitteena on laittaa järjestykseen mahdolliset hyödyt ja haitat, jotka voivat vaikuttaa organisaatioon. Prosessi lisää onnistumisen mahdollisuutta ja toisaalta vähentää epäonnistumisen mahdollisuutta. FERMA:n riskienhallinnan prosessi on esitetty kuviossa 8.



KUVIO 8 FERMA -menetelmän riskienhallinnan prosessi (FERMA, 2002).

FERMA:n standardi on esitelty tarkemmin liitteessä 9.

4.2 Menetelmien yhteenveto

Tutkimuksen ensimmäisessä vaiheessa tutkittiin aiheeseen liittyvää teoriaa, taustaa ja standardeja. Teoriaa, taustaa ja standardeja tutkittiin ensimmäisessä vaiheessa erillään toisistaan. Tutkielmassa käsiteltäviksi standardeiksi valikoituivat ISO, NIST, OCTAVE Allegro ja FERMA. Standardien osalta pyrittiin löytämään yhteisiä tekijöitä sekä eroavaisuuksia. Analysoinnin jälkeen koottiin synteesi, jossa kuvataan menetelmien yhteisiä tekijöitä. Näitä tekijöitä hyödynnetään uuden riskien arvioinnin menetelmän laatimisessa. Eroavaisuudet otetaan huomioon, mutta menetelmän laatimisessa pyritään hyödyntämään juuri parhaat käytänteet ja yhteiset tekijät.

Yleisesti ottaen standardit olivat melko samanlaisia. Laajuudessa ja menetelmän kuvauksessa oli huomattavia eroja. Standardien yhteisenä ominaisuutena on pyrkimys organisaation tavoitteiden näkymiseen turvallisuuden politiikoissa. Prosessit ovat jäsenneltyjä ja vaiheittaisia, mutta prosessin kuvauksessa on näkyviä eroja. Kuvauksessa eroavaisuudet näkyvät lähinnä ohjeistuksen tarkkuudessa. Riskien arvioinnin menetelmiä ei kuvata toimintaa tarkasti määrittävänä tekijänä, vaan lähinnä organisaation tukena oman toiminnan suunnittelussa.

Standardeissa on käytännön operatiivista toimintaa painottava lähestymistapa. Toiminnan suoraviivaistamista painotetaan, joka taas edellyttää harjoittelun ja arviointiin tarvittavan tietotason vaatimusten vähentämistä. Riskien arviointiin sitoutumista ja rakentamista osaksi organisaatioiden toimintaa korostetaan.

Riskien arvioinnin, kuten koko riskienhallinnan, tulee perustua parhaaseen saatavilla olevaan tietoon ja ottaa huomioon teknisten keinojen lisäksi inhimilliset ja kulttuuriset tekijät. Riskien arvioinnin tulosten tulisi olla olennainen osa organisaation päätöksentekoprosessia. Prosessin puutteet tiedostetaan ja sallittujen poikkeuksien rajoja korostetaan eri standardeissa.

Standardeissa määritellään organisaatioiden eri toimijoiden vastuualueet sekä valvonnan järjestäminen. Riskien arvioinnin prosessin tulee kuitenkin olla avoin ja organisaation toimijoiden tulee osallistua mahdollisimman laajasti riskien arvioinnin ja –havainnoinnin toimenpiteisiin. Riskien arviointi kuvataan koko organisaation yhteiseksi asiaksi, joka pyrkii jatkuvaan kehittymiseen.

Riskien arvioinnin standardeissa organisaation riskit on kuvattu muodollisesti. Muodollista kuvausta käytetään riskien priorisoinnissa. Riskien kuvaaminen muodollisesti luo pohjan, jota vasten voidaan tarkastella mahdollisia uusia organisaation kohtaamia riskejä. Kuvausten uudelleenkäytettävyys puolustaa muodollista kuvausta.

Standardit on kuvattu sanallisen osion lisäksi kuviolla tai prosessikaaviolla. Kuvioissa oli enemmän samankaltaisuuksia kuin eroja. Kuvioissa toimenpiteet oli kuvattu NIST –menetelmää lukuun ottamatta toisiaan seuraavina vaiheina, joissa yhdistävänä tekijänä oli jonkinlainen syöte, joka tarjosi perusteet seuraavalle vaiheelle. Kuvioita tarkasteltaessa kuvion ulkoasu ja selkeys nousivat tärkeiksi ominaisuuksiksi. Mitä nopeampia riskien arvioinnin syklit ovat, sitä selkeämpiä kuvattujen toimenpiteiden tulee olla. Monitulkintaiset kuviot pakottavat lukemaan eri vaiheiden pidemmät kuvaukset. Nopeassa tilanteessa tyhjentävät, vaiheittaiset toimenpiteet, antavat riskien arvioinnin tekijälle työkalun ajatusten selkeyttämiseen. Tämä tarkastelunäkökulma oli standardien vertailussa ja synteesin luomisessa hankalin. Selkeällä ja yksiselitteisellä kuviolla on toisaalta olemassa perusteet, koska täysin aukotonta menetelmää ei ole olemassa olevan tiedon perusteella mahdollista luoda. Standardeista poimitut merkittävimmät yhteiset nimittäjät on tiivistetty alla listattuun yhteentoista kohtaan:

1. Johdon tuki prosessille sekä sitoutuminen prosessiin
Organisaation johdon tulee sitoutua prosessin toteuttamiseen. Ilman johdon konkreettista tukea prosessista puuttuu selkeä linja ja perusta.

2. Riskien arviointiin sisältyy aina epävarmuustekijöitä
Koko riskien arvioinnin (ja -hallinnan) prosessiin liittyy paljon epävarmuustekijöitä. Määrällisen esitystavan käyttäminen olisi perusteltua, jos olisi olemassa riittävä määrä todenmukaista dataa, minkä varaan päätökset voitaisiin perustaa. Koska tämä data usein puuttuu, on vaikea tehdä paikkansa pitäviä laskelmia. Laadullista esitystapaa voidaan kritisoida liiasta yleisyydestä, mutta arviointia tehdessä täytyy pitää mielessä se, että kyse on nimenomaan arvioinnista, ei eksaktista tieteestä.

3. Joustavuus, organisaation kontekstiin räätälöity menetelmä
Mitään menetelmää ei tulisi ottaa käyttöön suoraan sellaisenaan, vaan sen käyttökelpoisuus tulisi aina arvioida organisaation toiminnan, resurssien ja tavoitteiden mukaan. Menetelmän tulisi soveltua organisaation toimintakulttuuriin ja prosesseihin.

4. Kehämäinen prosessi, ei koskaan valmis
Riskien arviointi (ja -hallinta) tulee ymmärtää prosessina, joka on jatkuva. Riskien arvioinnin tulee olla jatkuvaa ja sitä täytyy suorittaa iteratiivisesti aina uusimman ja parhaimman saatavilla olevan tiedon mukaan.

5. Prosessi antaa perusteet johtajien päätöksenteolle
Riskien arviointia ei tehdä sen itsensä takia, vaan sillä on aina jokin laajempi tarkoitus ja konteksti. Riskien arvioinnin on tarkoitus tuottaa tärkeää tietoa päätöksentekijöille heidän toimintansa tukemiseksi.

6. Prosessin tulee olla hyvin valmisteltu, suunniteltu ja johdettu
Riskien arvioinnilla (ja -hallinnalla) tulee olla vahva perusta. Sen täytyy olla johdettu prosessi, jolle on asetettu selkeät perusteet ja tavoitteet. Organisaation johdon tulee olla sitoutunut prosessin suorittamiseen. Lisäksi henkilöstön tulee omata riittävä ammattitaito prosessin suorittamiseen.

7. Priorisointi, riskien arvottaminen
Mitä perusteellisempi riskien arviointi, sitä enemmän todennäköisesti nousee esille toiminnassa huomioon otettavia riskejä. Riskien suhteen joudutaan tekemään priorisointia. Priorisoinnin kautta pystytään määrittelemään, mitä riskejä otetaan huomioon, mitkä jätetään huomiotta. Perusteissa tulee olla määritelty hyväksyttävä riskien taso.

8. Prosessin kautta syvemmän ymmärryksen saavuttaminen
Riskien arvioinnin kautta organisaatio analysoi syvällisesti omaa toimintaansa. Analysoinnin kautta organisaatio voi löytää heikkouksien lisäksi vahvuuksia. Riskien arviointi tarjoaa mahdollisuuden ymmärtää organisaation toimintaa ja siihen vaikuttavat tekijät entistä paremmin.

9. Selkeä tavoitteiden asettaminen
Riskien arvioinnilla tulee olla selkeät tavoitteet. Asetettuja tavoitteita voivat olla esimerkiksi riskien arvioinnin haluttu laajuus ja tarkkuus tai esitettävien tulosten muoto (laadullinen, määrällinen). Selkeiden tavoitteiden avulla arvioinnin tuloksista saadaan todennäköisemmin vertailukelpoisia.

10. Koko organisaation sitoutuminen ja osallistuminen
Riskien arvioinnin tulee olla prosessi, joka läpäisee kaikki organisaation tasot. Pahimmassa tapauksessa se on huonosti resursoitu tehtävä, jonka tulokset edustavat yhden henkilön tai pienen ryhmän subjektiivista näkemystä asioista. Koko organisaation sitouttamisen ja osallistamisen kautta arvioinnin tavoitteet voidaan saavuttaa kokonaisvaltaisemmin ja tehokkaammin.

11. Selkeät perusteet, resurssien tarjoaminen
Riskienhallinnalle ja - arvioinnille tulee antaa selkeät perusteet ja sen suorittamiseen tulee tarjota riittävät resurssit. Jos edellä mainitut asiat eivät toteudu, koko riskienhallinnan laatu laskee ja se ei tarjoa organisaatiolle haluttua hyötyä.

Riskienhallinnassa käytettävistä standardeista on laadittu useita vertailuja. Tässä tutkimuksessa tehtyä standardien ja menetelmien vertailua tukee Risk and Insurance Management Societyn (2011) laatima tutkimus, jossa on vertailtu seuraavia standardeja (RIMS, 2011):

- ISO 31000: 2009
- OCEG "Red Book" 2.0: 2009
- BS 31100: 2008
- COSO: 2004
- FERMA: 2002
- SOLVENCY II: 2012

RIMS:n tutkimuksessa standardien vaatimuksista löytyivät muun muassa seuraavat yhtäläisyydet:

- Organisaatiolähtöinen lähestymistapa, johdon tuki ja määritellyt vastuualueet
- Jäsennellyt prosessin vaiheet, valvonta ja tunnistettujen riskien raportointi
- Ymmärrys ja vastuullisuus riskinottohalun suhteen ja sallitut poikkeamat määriteltyjen rajojen suhteen
- Riskien muodollinen dokumentointi riskien arvioinnissa
- Riskienhallinnan prosessin tavoitteiden ja toimenpiteiden perustelu ja tiedottaminen
- Riskien käsittelysuunnitelmien valvonta. (RIMS, 2011).

RIMS (2011) mukaan useissa standardeissa viitattiin operatiivisen toiminnan tukemiseen. Odotusten vastaisesti harvassa standardissa viitattiin kuitenkaan odotettujen tulosten vaikutukseen johtamisen suorituskyvyn kehittymiseen. Raportin mukaan standardeilla oli enemmän samankaltaisuuksia kuin eroavaisuuksia. Tutkimuksen mukaan tämä on osoitus siitä, että yrityksen riskienhallinta kehittyy kurinalaisesti ja luo tarkoituksenmukaisia menetelmiä myös muille kuin liiketoiminnan organisaatioille. (RIMS, 2011).

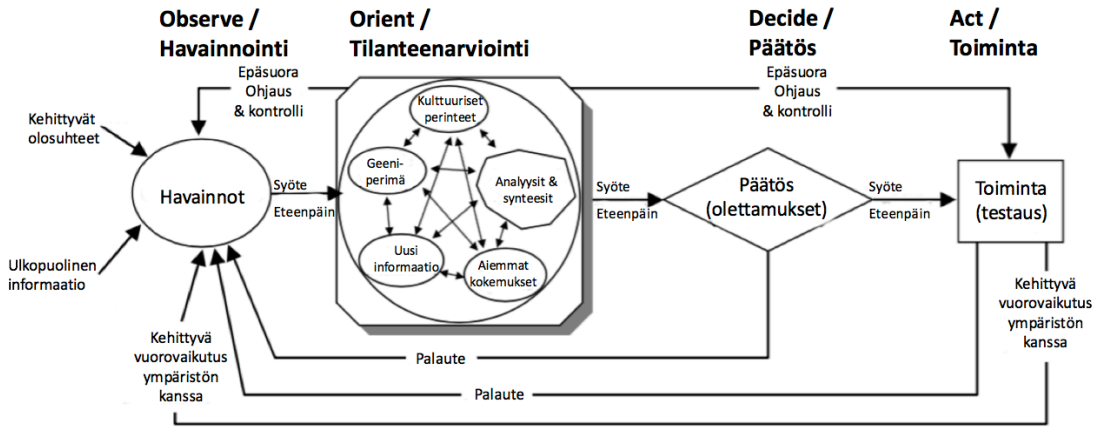
4.3 Vaihtoehtoiset menetelmät

Organisaatiot käyttävät riskien arviointiprosessissa standardien pohjalta rakennettuja organisaatiokohtaisia prosesseja. Prosessit eivät näin ollen noudata kirjaimellisesti yhtä ainoaa standardia, vaan standardeja muokataan oman tarpeen mukaan. Prosessissa voidaan käyttää myös varsinaisten standardien ulkopuolisia malleja, joissa edetään vaihe kerrallaan kohti tavoiteltua päämäärää. Alla esitellään kaksi yleisesti käytössä olevaa prosessimallia: OODA -silmukka ja PDSA -sykli. Malleja on olemassa runsaasti, mutta kirjallisuutta läpikäymällä päädyttiin kahteen seuraavaan, joita käytetään muun muassa liiketoiminnassa ja sotilastoiminnassa.

4.3.1 OODA –loop

OODA-loop on yhdysvaltalaisen John Boydin kehittämä päätöksenteon silmukka. Se on alun perin kehitetty ilmasodankäynnin tarpeisiin. (Brehmer, 2005). OODA-loopin periaatteet on myöhemmin otettu laajasti käyttöön muun muassa liiketalouden ja johtamisen alueella. Se on käytössä muun muassa Yhdysvaltojen ilmavoimissa, laivastossa ja maavoimissa sekä Ruotsin puolustusvoimissa. Laajasta levinneisyydestään huolimatta OODA-loop ei perustu mihinkään tieteelliseen julkaisuun, vaan Boydin alun perin 1970-luvulla pitämiin luentoihin.

OODA-loopin vaiheet ovat seuraavat: havainnointi (observation), tilanteenarviointi (orientation), päätös (decision) ja toiminta (action). OODA-loopista esitetään usein sen yksinkertaisempi versio, jossa edellä mainitut vaiheet toistuvat ympyrän omaisessa kehässä. Boydin esittelemä kattavampi malli on kuitenkin huomattavasti monimuotoisempi (kuvio 9).



KUVIO 9 OODA-loop (Brehmer, 2005, alunperin John Boydin luentomateriaali)

Kuvion 9 mukainen versio OODA-loopista on Boydin myöhemmin kehittelemä malli, jonka avulla hän on pyrkinyt luomaan siitä yleisemmän mallin voittamisesta ja häviämisestä. (Brehmer, 2005). Tämä yleisempi versio OODA-loopista ei ole enää varsinaisesti silmukka, kuten yleensä käytetty neljän kohdan ympyrämalli. Tähän mallin uudempaan versioon on lisätty myös vaiheita yhdistäviä nuolia kuvaamaan eri vaiheiden liittymistä toisiinsa.

OODA-loop tarjoaa menetelmän nopealle päätöksenteolle, jossa toimintaa pyritään muokkaamaan saatujen havaintojen ja saavutetun ymmärryksen kautta tehokkaammaksi ja päämääriä palveleviksi. OODA-loopin mukaan menestys saavutetaan sillä, että oma päätöksentekosykli kyetään muodostamaan vastustajan sykliä nopeammaksi. Tehdyt päätökset tai toiminta palautuvat aina oppimisen kautta tulevien havaintojen pohjaksi.

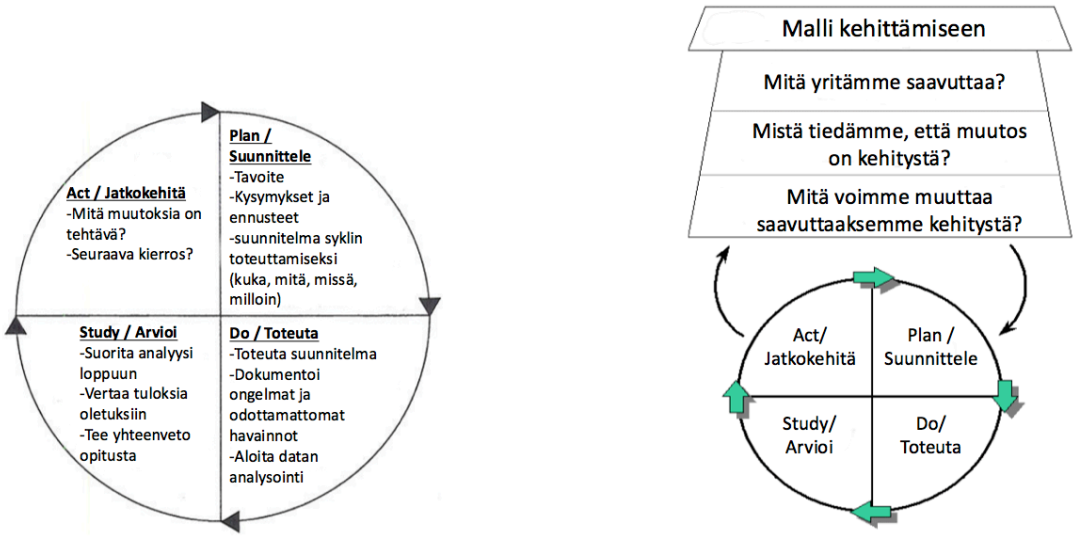
4.3.2 PDSA –sykli

PDSA-syklistä käytetään myös nimitystä Demingin laatuympyrä, Demingin sykli ja PDCA -kehityssykli. (Deming, 2016; Moen & Norman, 2006). PDSA on kehitetty malli 1950 luvun Japanissa esitetystä PDCA -syklistä. Sykli pohjautuu tohtori W. Edward Demingin luentoihin aiheesta. Prosessin juuret ovat tieteellisissä menetelmissä ja tieteen filosofiassa, joka on kehittynyt 400 vuoden ajan. Moenin ja Normanin (2006) mukaan sykli toimii viitekehyksenä yksityiskohtaisille menetelmille ja toimii kaikissa organisaatioissa sekä organisaation eri tasoilla. Helposti opittava ja käytettävä menetelmä tukee oppimista ja kehittymistä. Sykli lisäksi osallistaa pragmaattisen mallin kautta organisaation henkilöstöä ryhmätyöhön yhteisen kehityksen takaamiseksi. (Moen & Norman, 2006).

Syklin vaiheet olivat aiemmin ovat PLAN - DO - CHECK - ACT, mutta sykliä on kehitetty edelleen vaihtamalla kolmas vaihe alkuperäisestä CHECK -vaiheesta STUDY:n, jolloin mallia sovelletaan nykyisin vaiheilla PLAN - DO - STUDY - ACT. Sykli kulkee suunnittelun ja suunnitelman toteutuksen kautta oppimiseen ja toteutuksen valvontaan ja viimein itse toimintaan. Deming vaihtoi CHECK -vaiheen, koska se kuvaa pidättyneisyyttä prosessissa. Deming pyr-

ki kehittämään prosessia kohti tiedon virtausta vaiheesta toiseen. (Deming, 2016; Moen & Norman, 2006).

Kuviossa 10 on kaksi PDSA -syklin kehitysvaihetta vasemmalla vuonna 1994 esitelty PDSA -sykli (Moen & Norman, 2006; Langley, Nolan & Nolan, 1994) ja oikealla "Model for Improvement" -malli, joka laadittiin alun perin vuonna 1996 (Moen & Norman, 2006; Langley, Moen, Nolan, Nolan, Norman & Provost, 1996) ja paranneltiin edelleen vuonna 2009. Kolme kysymystä vuoden 2009 mallissa määrittivät tavoitetta, keinoja ja mahdollisia muutoksia prosessissa (Moen & Norman, 2006).



KUVIO 10 PDSA -sykli (Moen & Norman, 2006)

5 TUTKIMUKSEN TOTEUTTAMINEN

Tutkimuksen suunnitteluprosessi alkoi syksyllä 2015. Tutkimuksen tutkimuskysymystä määriteltiin lähinnä yleisellä tasolla, koska oli selvää, että kysymystä tullaan säätämään ja tarkentamaan tutkimusprosessin edetessä, kuten Eisenhardt (1989) kuvaa. Aiheen pohdinnan yhteydessä kävi ilmi, että tutkielman aiheen moniulotteisuuden vuoksi on ensinnäkin tarve pitää päiväkirjaa ja toiseksi tallentaa materiaalin lähdeaineistoa tietokantaan. Tietokanta ja lähdemateriaali tuli olla tutkimukseen osallistuvien tutkijoiden käytettävissä koko prosessin ajan ja fyysisestä olinpaikasta riippumatta. Tutkimuksen aikana kerätty data kerättiin tutkimuksen alussa laadittuun tietokantaan, koska Darke, Shanks & Broadbent (1998) mukaan tutkimuksen tiedonkeruun tehokkuuden kannalta dokumentointi koko tutkimuksen elinkaaren ajan on erittäin tärkeää. Tutkimuksen elinkaarella tarkoitetaan tässä tutkimuksessa jatkumoa tutkimuksen suunnittelusta aina pro gradu -tutkielmaprosessin päättämiseen ja arvioinnin antamiseen asti. Tämän jälkeen pro gradu -tutkielmaa voidaan edelleen käyttää apuna jatkotutkimuksessa ja riskien arvioinnin menetelmien kehittämisessä, mutta tähän nimenomaiseen tutkielmaan liittyvän tietokannan päivittäminen lopetetaan. Tietokanta laadittiin Google Drive -palveluun, joka on suojattu pilvitallennuspalvelu tiedostojen tallentamiseen ja jakamiseen muiden käyttäjien kanssa (Google, 1.11.2015). Raportit tapaamisista, päiväkirja prosessinaikaisista tapahtumista, pro gradu -tutkielman suunnitelma, pro gradu -tutkielman vaiheet, tietopankki mahdollisista lähteistä ja prosessia ohjaava aikataulu olivat Google -Drive palvelun kautta sekä tutkimuksen tekijöiden, että tutkielman ohjaajien saatavissa koko tutkimuksen ajan. Tietokannasta otettiin varmuuskopioita säännöllisin väliajoin mahdollisten vahinkojen välttämiseksi. Google Drive valikoitui useiden palveluntarjoajien joukosta aikaisempien käyttökokemusten ja hyvin rakennetun kokonaisuuden vuoksi.

5.1 Tutkimusmenetelmä

Seuraavassa luvussa kuvataan tutkimusmenetelmä ja se, millä perusteilla päädyttiin juuri kuvattuun menetelmään. Niiniluodon (1997) mukaan tutkimuksen lähtökohta on aina jokin tutkimuskohdetta koskeva kysymys tai ongelma. Käy-

täntöön orientoituneen tutkimusongelman kaksi tyyppiä ovat 1) deskriptiivinen - ja 2) generalisoiva tutkimusasetelma. Deskriptiivinen tutkimusasetelma pyrkii kuvaamaan nykyistä tilaa tai historiaa, kun taas generalisoiva tutkimusasetelma kartoittaa systeemiä koskevia säännönmukaisuuksia, jotta voidaan tehdä luotettavia ennustuksia ja jotta löydettäisiin tai parannettaisiin annettuun tavoitteeseen johtavia keinoja. (Niiniluoto, 1997). Riskien arviointiin on aikaisemmin laadittu runsaasti erilaisia malleja, menetelmiä ja standardeja. Tässä tutkimuksessa pyrittiin löytämään yhdenmukaisuuksia ja ristiriitoja käytössä olevien riskien arvioinnin mallien, teorian ja käytännön suhteen. Tutkijoiden perimmäisenä tarkoituksena oli tuottaa organisaatioiden riskien arvioinnin toteuttamiseksi käytännön tason ratkaisu uuden riskien arvioinnin mallin muodossa. Tällöin voidaan sanoa, että tämä tutkimus sijoittuu selkeästi generalisoivan tutkimusasetelman puolelle, koska tarkoitus oli nykytilan tai historian kuvailun sijaan tuottaa keinoja laadukkaamman riskien arvioinnin toteuttamiseen.
Tutkimusongelmat ovat Niiniluodon (1997) mukaan usein väljästi muodostettuja, mutta Puusan ja Juutin (2011) mukaan tutkijalla on toisaalta esiymmärrys aiheesta. Tästä syystä tutkimusongelman täsmentäminen ja jakaminen osiin on tutkimuksen onnistumisen kannalta ratkaiseva tekijä. Tutkimusmenetelmän valinnassa pyrittiin huomioimaan tutkijoiden tietoisuuden kasvu ja mahdollisuus ongelman ratkaisemiseksi tarvittavien muutosten tekemiseen. Tutkimusongelman monitahoisuuden vuoksi muutoksille jätettiin riittävästi tilaa. Keskeinen ajatus tutkimusmenetelmän muodostumisessa on, että sen tulee tukea tulevaisuuteen kohdistuvaa ajattelua kokonaisvaltaisen, holistisen, näkemyksen saamiseksi (Puusa & Juuti, 2011) eikä niinkään pyrkiä kuvaamaan historiaa ja aiempia käytänteitä. Tavoitteena on kokonaisvaltaisen ymmärryksen kautta tuottaa tutkimuksen kohteena olevasta ilmiöstä tulkinta, joka johtaa ilmiön uudelleen tarkasteluun ja tätä kautta ymmärryksen syventymiseen ja lopulta uuden tulkinnan tekemiseen. (Puusa & Juuti, 2011). Puusan ja Juutin (2011) mukaan tutkimusprosessi elää, kunnes tutkija pystyy rakentamaan johtopäätöksensä aineistosta ja kriittisesti arvioimaan omaa työtään.

Tapaustutkimus on nähty hyvänä menetelmänä silloin, kun tutkittavan alueen tutkimus ja teoria ovat vielä varhaisessa vaiheessa (Darke ym., 1998). Darke ym. (1998) mukaan tietojärjestelmiin liittyvässä tutkimuksessa on vielä paljon alueita, joihin tämä pätee. Tässä suhteessa tutkijat näkivät tarpeen myös tälle tutkimukselle. Tutkijat näkivät laadukkaan riskien arvioinnin olennaisena osana organisaatioiden menestyksekästä toimintaa. Aiheeseen liittyvä aiempi tutkimus vaikutti melko vähäiseltä. Tämän vuoksi tämän tutkimuksen nähtiin vastaavan todelliseen tarpeeseen. Ilmiöitä pyrittiin tutkimaan sen omassa luonnollisessa ympäristössä, finanssialan organisaatioissa.

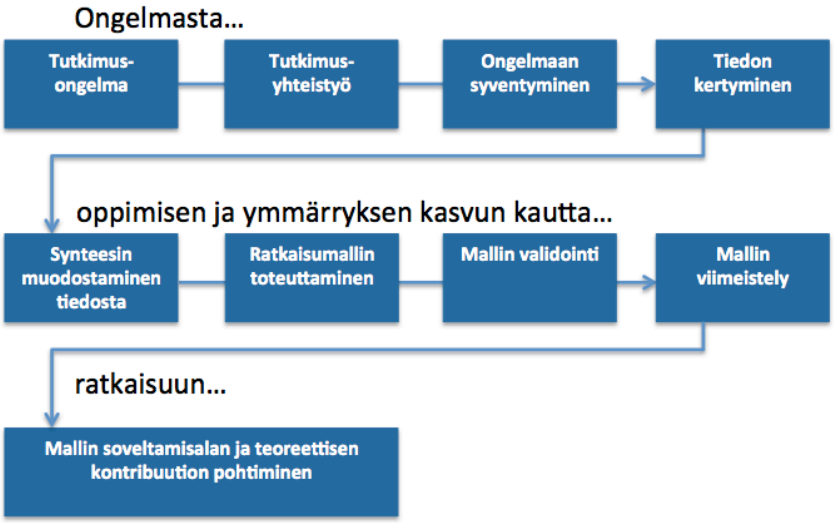
Tuomen ja Sarajärven (2009) mukaan haluttaessa tietää, mitä ihminen ajattelee tai miksi hän toimii niin kuin toimii, on järkevää kysyä asiaa häneltä itseltään. Tutkimusta tehtiin tutkimuskysymyksen dynamiikan selvittämiseksi omassa ympäristössään haastattelemalla finanssialan organisaatioiden asiantuntijoita ja tutkimalla olemassa olevaa teoriaa. Tutkimuskysymyksen monitieteellisen ja kompleksisen luonteen vuoksi vastauksia pyrittiin löytämään haastatteluiden avulla kvalitatiivisin keinoin. Haastattelut myös ohjasivat tutkimusongelman kannalta keskeisimmän teorian löytämisessä. Eisenhardtin ja

Graebnerin (2007) mukaan todennäköisyys uusien teorioiden löytymiselle kasvaa, koska uudet teoriat testataan olemassa olevien teorioiden suhteen. Teoria on todennäköisesti empiirisesti kelvollinen, koska teorian rakennusprosessi on erittäin tiukasti sidoksissa todisteisiin ja teoria on yhteneväinen empiiristen havaintojen kanssa. (Eisenhardt & Graebner, 2007). Teoria on syntynyt läheisessä kanssakäymisessä selkeän näytön kanssa, mikä tekee siitä todellisuutta peilaavan (Eisenhardt & Graebner, 2007). Kvalitatiivisessa, eli laadullisessa tutkimuksessa on tavoitteena kuvata todellista elämää (Hirsjärvi, Remes & Sajavaara 2002). Laadullisessa tutkimuksessa on lähtökohtana kuvata jokin ilmiö tai tapahtuma, ymmärtää toimintaa tai tulkita teoreettisesti mielekkäästi jotakin ilmiötä. Riskien arvioinnin prosessin toteuttamisen tavat ja yhteys organisaation liiketoimintastrategiaan ovat ilmiöinä hyvin kiinnostavia. Eisenhardtin ja Graebnerin (2007) mukaan teorian oikeutuksen perustelu liittyy tutkimuskysymyksen luonteeseen. Nykyisiä teorioita voidaan pyrkiä laajentamaan. Toisaalta ilmiöitä voidaan pyrkiä perustelemaan niiden tärkeydellä sekä teorioiden ja empiiristen havaintojen puutteella. (Eisenhardt & Graebner, 2007).

Olemme ottaneet tutkimuksessa huomioon, että kvalitatiivinen tutkimus voidaan ymmärtää monella eri tavalla (Eisenhardt & Graebner, 2007; Puusa & Juuti, 2011). Laadullista tutkimusta tehdessä on perusteltua joka kerta määrittää mitä on tekemässä. Von Wrightin (1970) mukaan tutkimuksessa tehdyt menetelmät tulee pystyä perustelemaan, mutta tehtyjä valintoja ei voi avata rationaalisesti loputtomiin, koska jossain vaiheessa tulee kuitenkin perustelematon usko tai asenne. Tuomen ja Sarajärven (2009) mukaan edes tutkimusongelman muotoilua ei voi pitää teoria- tai arvovapaana, vaan siihen vaikuttavat tutkijan omat päämäärät.

Tutkimuksessa tehtiin kaksivaiheinen kvalitatiivinen tutkimus, jossa kerättiin tietoja teemahaastatteluin, tieteellisestä kirjallisuudesta, julkaisuista ja standardeista. Tutkimuksen tulosten perusteella laadittiin riskien arvioinnin prosessimalli tietoturvajohtajien näkökulmasta. Tutkimuksen tavoitteena ei ole pyrkiä tilastollisiin yleistyksiin (Tuomi & Sarajärvi 2009). Tutkimus laaditaan kvalitatiivisena, koska kvantitatiivisen tutkimuksen kautta ei ole saatavissa tutkimuksen kannalta keskeisiä tietoja, joita vain tutkimuksen tärkein tiedon lähde, haastateltavat henkilöt, tuottavat (Darke ym., 1998; Eisenhardt & Graebner, 2007; Puusa & Juuti, 2011). Laadullisen tutkimuksen etuna on todennäköisyys uusien teorioiden kehittymiselle. Tutkimuksen aikana teoriaa testataan koko ajan sillä tutkimus on läheistä kanssakäymistä tutkimuksen kohteen kanssa. (Eisenhardt & Graebner, 2007; Puusa & Juuti, 2011). Niiniluodon (1997) mukaan tutkimuksen vaiheet eivät aina seuraa toisiaan yksinkertaisesti ajallisessa järjestyksessä. Tutkimuksessa joudutaan usein palaamaan taaksepäin ja korjaamaan aikaisemmissa vaiheissa tehtyjä oletuksia ja ratkaisuja. (Niiniluoto, 1997).

Tutkimusprosessi noudatti sovellettuna Eisenhardin (1989) kuvaamaa tapaustutkimuksen teorian laadinnan prosessia. Ensimmäisessä vaiheessa määriteltiin tutkimuskysymys yleisellä tasolla, jotta voitiin valita tutkimuksen kannalta soveltuvia kohdeorganisaatioita. Tutkimusmenetelmän valinnassa painotus oli reaalimaailman ja organisaatioiden käytännön tutkimuksessa. Tutkimuksen tarkoitus oli auttaa reaalimaailman ongelmien ratkaisussa tuottamalla uusi innovatiivinen malli riskien arviointiin. Tavanomaisen tilastollisen valintaperusteen sijaan painotettiin soveltuvuutta olemassa olevien teorioiden toistamiselle tai laajentamiselle. Seuraavaksi selvitettiin mahdolliset yhteistyömahdollisuudet ja alkavat sekä meneillään olevat tutkimukset aiheeseen liittyen. Tutkimusongelmaan syvennyttiin ja kerättiin tietoa tutkittavasta aiheesta. Kerätyn tiedon perusteella muodostettiin synteesi ja laadittiin ratkaisumalli ongelmaan. Muodostettu malli validoitiin asiantuntijoilla ja viimeisteltiin saadun palautteen perusteella. Tutkimuksen lopuksi pohdittiin mallin soveltamisalaa ja tunnistettiin tutkimuksen kontribuutio myös mallin ulkopuolelta esimerkiksi jatkotutkimusaiheiden muodossa. Tutkimuksen vaiheet on kuvattu tarkemmin vaiheita koskevissa luvuissa. Kuviossa 11 on esitetty tutkimuksen vaiheet.



KUVIO 11 Tutkimusprosessin vaiheet

5.2 Aineiston keruu ja käsittely

Luvussa 5.2 kuvataan miten, tutkimuksen aineisto kerättiin ja miten sitä käsiteltiin. Tieteellisen kirjallisuuden tutkiminen ja mahdollisten tutkimuskysymykseen liittyvien artikkelien kerääminen tutkimuksen alussa laadittuun tietokantaan aloitettiin syksyllä 2015. Aineiston keruu alkoi jo ennen varsinaista pro gradu -tutkielmaprosessia tutkijoiden oman kiinnostuksen vuoksi. Tutkimuskysymyksen arveltiin muuttuvan tutkimuksen aikana, joten materiaalia kerättiin myös tutkimuskysymyksen ulkopuolelta mahdollista tavoitetilaa, mallin luomista, ajatellen. Tutkimuksen tieteellisen kirjallisuuden etsiminen jatkui koko prosessin ajan. Haastattelujen jälkeen oli mahdollista etsiä tietoa haastatteluissa esille tulleisiin asioihin liittyen. Eisenhardtin (1989) mukaan oppimisen,

tuntemusten ja ajatusten heräämisen kautta voidaan prosessin kulkua muuttaa, jotta lopputulos olisi paras mahdollinen. Aineiston analyysin ja materiaalin vertailun kautta on mahdollista löytää ristiriitaisuuksia, joita tutkimalla on mahdollista löytää uutta tietoa, jolla teoriaa kyetään toistamaan tai kyseenalaistamaan (Eisenhardt, 1989).

Tutkimuksen aineisto koostuu aihealueen aiemmasta tieteellisestä tutkimuksesta, valituista riskien hallinnan standardeista, kirjallisuudesta. Tieteellisen tutkimuksen kautta muodostettava teoreettinen tausta pyrittiin muodostamaan laajasti pyrkimättä tietoisesti pitäytymään nimenomaan esimerkiksi tietojärjestelmien turvallisuuteen liittyvässä tutkimuksessa. Tätä kautta pyrittiin saamaan tutkimukselle mahdollisimman laaja ja eri aloille yleistettävissä oleva tieteellinen perusta. Tutkimuksen, ja mallin muodostamisen ensisijaisena lähteenä käytettiin organisaatioista kerättävää empiiristä aineistoa. Organisaatioista kerättyä tietoa täydennettiin ja sille haettiin vahvistusta edellä mainitun täydentävän aineiston avulla.

Empiirisen aineiston kerääminen päätettiin kohdistaa Suomen finanssialalla toimiviin organisaatioihin. Finanssialan organisaatioiden toimintaympäristö on vahvasti riippuvainen digitaalisten järjestelmien toimivuudesta ja niillä on vahva toimintakulttuuri liittyen riskienhallintaan. Lisäksi finanssiala on vahvasti reguloitu myös riskienhallintaan liittyen. Näin ollen voitiin olettaa, että finanssialan organisaatiosta saataisiin mallin muodostamisen perustaksi vahvaa empiiristä aineistoa liittyen riskienhallintaan ja –arviointiin.

Haastatteluun osallistuville lähetettiin ennen varsinaista haastattelua saatekirje. Saatekirjeessä kerrottiin tutkimuksen tavoite ja käytiin tutkimuksen vaiheet lyhyesti läpi. Saatekirjeessä (liite 1) kerrottiin tutkimuksen tekijöiden nykyisestä koulutusohjelmasta Jyväskylän yliopistossa, yleisesti aikaisemmasta koulutuksesta, tekijöiden työtaustasta sekä tutkimuksen tarpeesta kyberturvallisuuden alalla ja tarkemmin riskien arvioinnin osalta. Haastateltaville kerrottiin mahdollisuudesta olla osa tutkimusta, joka käsittelee yritysten toimintaympäristön muutoksen kannalta keskeistä toimintaa. Tutkimuksen tulosten hyödynnettävyyttä kuvataan saatekirjeessä organisaatioiden näkökulmasta (Darke ym., 1998). Saatekirjeen lopussa mainittiin yritysten mahdollisuudesta olla yhteydessä tutkimuksen tekijöihin koko tutkimuksen ajan ja saada tutkimuksen tulokset lopulta omaan käyttöönsä. Saatekirjeen liitteenä toimitettiin haastattelun teemat kysymyksineen, jotta ensinnäkin pystyttiin varmistamaan henkilön soveltuvuus haastatteluun ja toiseksi valmistautumisen osalta haastateltavalle annettiin mahdollisuus hankkia itselleen tarvittavat taustatiedot. Kysymykset lähetettiin ennakkoon, jotta oikea henkilö saataisiin haastatteluun ja toisaalta siksi, että haastattelussa oli tarkoitus saada mahdollisimman paljon tietoa tutkittavasta asiasta. Tuomen ja Sarajärven (2009) mukaan haastattelun onnistumisen kannalta on suositeltavaa toimittaa haastateltaville kysymykset ennalta. Saatekirjeen ja ennakkoon lähetettyjen kysymysten kautta pyritään omaaloitteisesti osoittamaan haastateltaville, että tutkijat ovat luottamuksen arvoisia. Tämä tarkoittaa suunnitelmallisuutta, valmistautumista ja tutkimukseen sitoutumista. (Darke ym., 1998).

Haastateltaville kerrottiin ennen varsinaisen haastattelun aloittamista haastattelun tallentamisesta ja kysyttiin lupa tallentamiseen. Ehdotimme haas-

tateltaville haastattelun tallentamista. Kaikki haastateltavat suostuivat tallennukseen. Olimme valmistautuneet myös tallennuksesta kieltäytymiseen varaamalla haastatteluun tarvittavat muistiinpanovälineet. Myös kahden haastattelijan käyttö antoi osaltaan mahdollisuuden tälle toimintatavalle.

5.3 Haastatteluiden toteuttaminen

Tässä luvussa kuvataan, miten haastattelut ensimmäisessä ja toisessa vaiheessa toteutettiin. Tutkimus on kvalitatiivinen tutkimus, jossa haastatteluja tehtiin kahdessa vaiheessa. Ensimmäisessä vaiheessa haastateltiin suomalaisten finanssialan organisaatioiden edustajien joukkoa. Toisessa vaiheessa haastateltiin keskeisiä kyberturvallisuuden ja riskien arvioinnin asiantuntijoita sekä tarkasteltiin ensimmäisen vaiheen jälkeen muodostetun riskien arvioinnin mallin käytettävyyttä. Tutkimuksen molemmissa vaiheessa haastattelut toteutettiin puolistrukturoiduilla haastatteluilla. Puolistrukturoitu haastattelu, teemahaastattelu, etenee tiettyjen etukäteen valittujen teemojen ja tarkentavien kysymysten kautta varassa. (Tuomi & Sarajärvi, 2009). Kysymyksiä ei välttämättä esitetä samassa järjestyksessä vaan pyritään mahdollisimman paljon saamaan tietoa haastateltavan vapaalla kerronnalla. Tutkimuksessa vapaa kerronta tarkoittaa haastateltavan omien ajatusten jäsentämistä haastateltavalle itselle omalla tavalla. Tarvittaessa haastattelua viedään eteenpäin saatekirjeen mukaisilla teemoilla ja niiden alakysymyksillä. Teemahaastattelussa ei voi kysyä ihan mitä tahansa. Teemahaastattelussa pyritään löytämään vastauksia tutkimuksen tarkoituksen ja ongelmanasettelun kannalta keskeisiin kysymyksiin. Teemat perustuvat tutkimuksen viitekehykseen. (Tuomi & Sarajärvi, 2009).

Ensimmäisen vaiheen haastatteluiden runko ja teemat löytyvät liitteestä 4. Tutkijat olivat muodostaneet ennen haastatteluiden toteuttamista käsityksen riskien hallinnan ja –arvioinnin prosessin suorittamisesta perehtymällä valittuihin standardeihin ja muodostamalla niistä synteesin. Lisäksi tutkijat olivat tutkineet nykyajan digitaalisen toimintaympäristön asettamia haasteita liittyen organisaatioiden toimintaan ja riskien arvioinnin suorittamiseen. Näiden tekijöiden avulla muodostettiin ensimmäisen vaiheen haastatteluiden runko ja teemat. Kysymysten asettelun kautta tutkijoiden tarkoituksena oli selvittää organisaatioiden käytännön tavat suorittaa riskienhallinta ja riskien arviointi. Lisäksi tarkoituksena oli kartoittaa sitä, miten riskien arvioinnin tulokset käytännössä vaikuttavat organisaatioiden toimintaan. Tämä tapahtui selvittämällä organisaatioiden tapoja muodostaa tietoturvapolitiikkaa ja sitä, miten riskien arvioinnin tulokset vaikuttavat sen muodostumiseen. Haastattelun teemassa 4 (parhaat käytänteet) pyrittiin selvittämään organisaatioiden havaintoja siitä, mikä riskien arvioinnissa ja tietoturvapolitiikan laadinnassa on koettu toimivaksi ja mikä on koettu huonosti toimivaksi.

Kysymykset valmisteltiin etukäteen, jotta kaikilta osallistuvilta organisaatioiden edustajilta ja asiantuntijoilta oltaisiin saatu vastaukset tutkimuksen kannalta keskeisiin seikkoihin, joita ei muualta kuin alan organisaatioista ole saatavilla. Organisaatioiden taustatiedot selvitetään muun muassa organisaati-

on julkaisuista ja internetistä. Haastateltavilta kysytään ainoastaan tiedot joita ei muualta ole saatavissa (Darke ym., 1998). Etukäteen valmisteltujen kysymyksien kautta pyritään suuntaamaan haastattelujen kulkua oikeaan suuntaan (Eisenhardt, 1989). Kysymysten kautta pyritään lisäksi selvittämään vastauksia sellaisiin kysymyksiin, joihin ei ole saatavissa vastausta muilla keinoilla (Darke ym., 1998). Kysymysten laadinnassa ja aineistonkeruun perustana käytetään teoriaa. Teoriaa käytetään ohjaamaan haastatteluja oikeaan suuntaan, poistamaan sattumanvaraisuuksia ja tutkijan oman subjektiivisen näkemyksen vaikutusta. Laadullinen tutkimus perustuu aina jossain määrin tutkijan tekemiin valintoihin, mutta tieteelliselle tutkimukselle ominaiseen vuoropuheluun aiemman teorian kanssa on kiinnitettävä huomiota. Tulosten vertailu aiemman teorian, tutkimuksen teoreettisen, viitekehyksen kanssa on yksi keskeisimmistä asioista. (Puusa & Juuti, 2011).

Tutkimuksen molemmissa vaiheissa ja kaikissa haastatteluissa käytettiin kahta haastattelijaa. Kaikki haastattelut tehtiin henkilökohtaisesti. Ennalta määritelty ja haastatteluun valmistautunut päähaastattelija vastasi haastattelun toteuttamisesta. Päähaastattelija vastaa, että kaikki tarvittavat kysymykset sekä teemat esitettiin haastateltaville ja haastatteluaika käytetään tehokkaasti. (Myers & Newman, 2007). Toinen haastattelija vastasi haastattelun tallentamisesta tallentimelle ja keskeisten löydösten kirjaamisesta tietokoneelle muistiinpanoiksi. Toisen haastattelijan tehtävään kuului lisäksi ennalta määritellyn päähaastattelijan tukeminen haastattelun lopussa avoimen keskustelun vaiheessa. Kahden haastattelijan käyttö on perusteltavissa kattavammalla dokumentoinnilla ja toisen haastattelijan, tässä tapauksessa päähaastattelijan, paremmalla osallistumisella itse keskusteluun haastateltavan kanssa (Darke ym., 1998). Darke ym. (1998) kuvaavat haastateltavaa tapaustutkimuksen pääasialliseksi tiedon lähteeksi. Haastattelujen tulos on tutkimuksen tuloksen kannalta erityisen merkittävä, koska kattavaa tilastollista tietoa riskien arvioinnin tuloksista organisaatioissa ei ole saatavilla. Baskervillen (1991) ja Siposen (2015) mukaan tilastollisesta tutkimuksesta tietojärjestelmätieteessä puuttuu tutkimuksellinen tarkkuus, koska riskien arvioinnin menetelmät tietoturvallisuuden osalta on määritetty muilta tieteenaloilta lainattujen menetelmien avulla.

Myersin ja Newmanin (2007) mukaan haastatteluissa ja niihin valmistautumisessa on otettava huomioon mahdolliset haastatteluissa eteen tulevat ongelmat:

- haastateltavat voivat kokea haastattelun keinotekoisena
- haastateltavan ja haastattelijan välillä ei ole luottamusta
- haastatteluun ei ole aikaa
- tutkimuskysymykseen haetaan vastauksia organisaation alatasolta jolloin siirtyminen ylemmälle tasolle ei ole aina mahdollista
- haastatteluilla saavutetaan vain tutkimusongelman kannalta kapea näkemys (elite bias) haastattelemalla organisaation johtohenkilöitä
- haastattelija vaikuttaa haastateltavan käyttäytymiseen (sosiaaliset tekijät Hawthorne -ilmiö)

- haastattelun aikana haastateltavan tietoisuuden rakentuminen tutkittavasta aiheesta
- kielen epäselvyys ja väärinkäsitykset
- haastattelu ei onnistu, koska haastateltava esimerkiksi pahoittaa mielensä. (Myers & Newman, 2007).

Edellä mainittujen ongelmien esiintymistä tarkasteltiin haastattelujen jälkeen tutkimuksen luotettavuuden pohdinnan yhteydessä. Myersin ja Newmanin (2007) kuvaamat ongelmat antavat mahdollisuuden tarkastella omaa suoriutumista haastatteluissa ja tätä kautta tutkimusten luotettavuutta.

Haastateltaville annettiin mahdollisuus tarkastaa antamansa vastaukset. Tutkimus lähetettiin ennen arvosteltavaksi vientiä siihen osallistuneille henkilöille tarkastettavaksi. Haastattelun etu on, että haastateltavat henkilöt harvoin kieltävät haastattelun käytön tutkimusaineistona (Tuomi & Sarajärvi, 2009). Palautteen antamiselle annettiin määräaika, jonka jälkeen tutkimus korjausten jälkeen toimitettiin pro gradu -tutkielman tarkastajille.

Tuomi ja Sarajärvi (2009) kuvaavat haastattelun olevan kallis ja aikaa vievä aineistonkeruumuoto. Tutkimuksen laatimisesta ja aineiston keräämisestä aiheutuneet kustannukset jaettiin tutkimuksen tekijöiden kesken. Aineiston keräämiseen käytettiin tutkimuksen tekijöiden henkilökohtaisia työvälineitä ja tarpeen mukaan Jyväskylän yliopiston tarjoamia teknisiä apuvälineitä. Tutkimus raportoitiin sähköisesti Jyväskylän yliopiston julkaisujärjestelmässä. Tutkimus on Opetus- ja kulttuuriministeriön antaman ohjeen (3/500/2004) mukaisesti kokonaisuudessaan julkinen.

Kummatkin tutkijat osallistuivat kaikkiin haastatteluihin. Haastattelut pidettiin pääosin pääkaupunkiseudulla ja ne olivat kestoltaan keskimäärin tunnin mittaisia.

5.4 Haastattelukierrokset

Tutkimuksen ensimmäisen vaiheen haastateltavat henkilöt toimivat Suomessa finanssialan organisaatioiden tietohallinnon, turvallisuuden tai liiketoiminnan johtotehtävissä. Organisaatioiden rakenteiden eroista johtuen tietyn nimikkeen alla toimivaa henkilöä ei voinut määritellä ennalta, vaan kuvasimme haastattelun saatekirjeessä mahdollisimman tarkasti tutkimukseen toivomaamme henkilöä. Henkilöiden valinnassa painotettiin osallistumista organisaation riskien arvioinnin suunnitteluun, toteuttamiseen ja toimintaan osana organisaation johtoryhmää tai vastaavaa ylemmän johdon tasoa. Painotus oli liiketoiminnan ja turvallisuuden osa-alueiden tuntemuksella ja yhteensovittamisella. Tarkoituksemme oli haastatella henkilöitä, joilla on laaja näkemys ja mahdollisuus kertoa tutkimuskysymykseen liittyvistä ilmiöistä eri näkökulmasta. Laaja tietämys ja näkökulman laajuus näkyvät myös mahdollisuutena yhdistellä sekä reaaliaikaisia että menneitä tapahtumia. (Eisenhardt & Graebner, 2007; Puusa & Juuti, 2011). Haastateltavien henkilöiden valinta tehdään suunnitelmallisesti välttäen sattumanvaraisuutta (Eisenhardt, 1989). Haastateltavien määrää oli

ennen tutkimuksen aloittamista hankala määrittää. Tuomi ja Sarajärvi (2009) eivät näe väitöskirjaa alempien opinnäytetöiden aineistojen kokoa merkittävänä perustaen näkökulmansa siihen, että opinnäytetyö on harjoitustyö ja pyrkii osoittaa oppineisuutta omalta alalta. Tässä kyseisessä tutkimuksessa pyrittiin näkökulmasta huolimatta kattavaan näkemykseen suurista finanssialan organisaatioista. Eskolan ja Suorannan (1996) mukaan tutkimuksessa ei pyritä määrällisen tutkimuksen laajuiseen näytteen kokoon vaan tulkintojen kestävyyteen ja syvyyteen. (Eskola & Suoranta, 1996). Saatekirje lähetettiin ensimmäisessä vaiheessa kattavasti finanssialan organisaatioihin sekä yksityiselle että julkiselle sektorille. Pyrimme aluksi noin kymmeneen haastateltavaan ensimmäiselle kierrokselle. Laadullisessa tutkimuksessa laatu on näytteiden määrää tärkeämpää. (Puusa & Juuti, 2011). Tutkimusekonomisista syistä haastateltavien henkilöiden määrä rajattiin noin kymmeneen.

Toisen vaiheen haastateltavien valinnassa painotettiin laaja-alaista osaamista niin turvallisuuden, liiketoiminnan kuin informaatioteknologian aloilla. Haastateltaviksi saatiin yhteiskunnan kannalta merkittäviä henkilöitä, jotka pystyvät näkemään riskien arvioinnin osana turvallisuutta ja liiketoimintaa, mutta toisaalta myös osana vielä suurempaa yhteiskunnallista merkitystä ja yhteistoimintaa. Toiseen vaiheen asiantuntijahaastattelut ja mallin validointi suoritettiin henkilökohtaisesti kolmelle suomalaiselle asiantuntijalle. Tutkimuksen toisen vaiheen asiantuntijoina toimivat:

- **Jarno Limnéll**, Insta Defsec Oy:n kyberliiketoiminnan johtaja ja Aalto-yliopiston professori
- **Mikko Siponen**, Jyväskylän yliopiston professori, tietojenkäsittelytieteen laitoksen johtaja
- **Kimmo Rousku**, Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) pääsihteeri sekä Tietoturva ry:n valitsema vuoden tietoturvapäällikkö 2015

Laadittavaa riskien arvioinnin prosessimallia ei räätälöity yksittäiselle toimialalla tai organisaatiolle, joten asiantuntijoiden valinnassa painotettiin henkilöiden laajaa näkemystä turvallisuudesta osana organisaatioiden tavoitteiden toteuttamista. Seuraavaksi kerrotaan tarkemmin millä perusteilla mainittuihin asiantuntijoihin päädyttiin. **Jarno Limnéll** on suomalaisen Insta Defsec Oy:n kyberliiketoiminnan johtaja ja Aalto -yliopiston professori kyberturvallisuuden alalla. Limnéll on yksi tunnetuimmista suomalaisista turvallisuuspolitiikan ja kyberturvallisuuden asiantuntijoista. Limnéll on ottanut merkittävästi osaa keskusteluun digitaalisesta turvallisuudesta ja Suomen tulevaisuudesta. Limnéll on osallistunut niin kansallisen kuin kansainvälisen tason yhteistyöhön kyberturvallisuuden alalla. (Insta, 2015). Limnéll tuo tutkimukseen näkemystä erittäin laaja-alaisesti niin koulutuksen, liiketoiminnan kuin turvallisuuspolitiikan osa-alueilta. Limnéll on aiemmin työskennellyt puolustusvoimissa upseerina. **Mikko Siponen** toimii Jyväskylän yliopiston tietojenkäsittelytieteiden professorina ja laitoksen johtajana. (Jyväskylän yliopisto, 2016a). Siponen sijoitettiin vuonna 2013 maailmanlaajuisella top 100 -listalle sijalle 29 ollen paras eurooppalainen tietojärjestelmätieteilijä. (Hartio, 2013). Siponen valittiin vuonna 2015

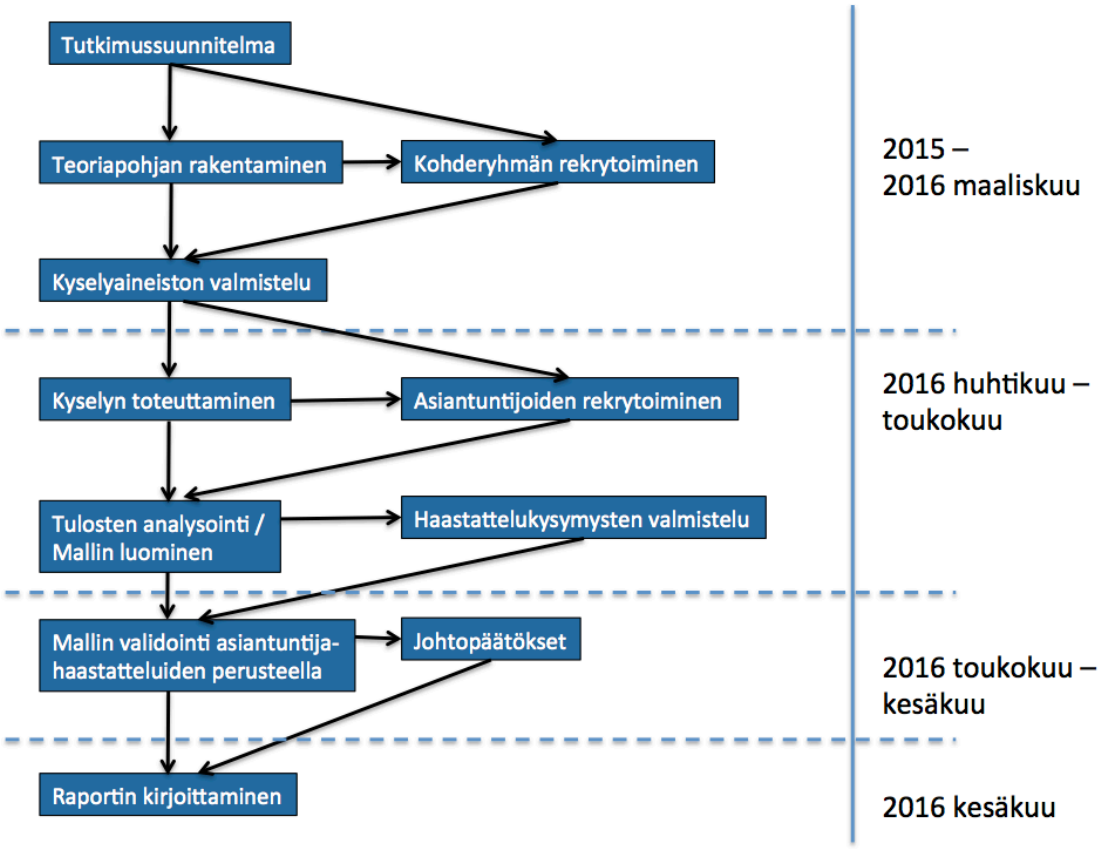
vuoden tietoturvatutkijaksi ja hän on yksi alan siteeratuimpia tutkijoita maailmassa. Siposen johtama tutkimuskonsortio sai lisäksi Tekesiltä 956000 euron rahoituksen uuden tietoturvan hallintamenetelmän kehittämiseen. (Jyväskylän yliopisto, 2016b). **Kimmo Rousku** toimii valtiovarainministeriön asettaman valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) pääsihteerinä. Rousku on toiminut ICT-alalla lukuisissa valtionhallinnon tehtävissä viimeisen 20 vuoden ajan. (IT2015, 2015). Tietoturva ry valitsi Kimmo Rouskun vuoden tietoturvapäälliköksi 2015. Valintaa perusteltiin esimerkillisellä tietoturvan toimintatapojen ja edellytysten kehittämisellä sekä tietoturva-ammattilaisten verkostoitumisen edistämisellä ja puolueettoman tiedon jakamisella vuoden 2014 aikana. Rousku on kirjoittanut lukuisia tietoturvatietoisuutta lisääviä blogeja ja ollut ahkera puhuja erilaisissa tapahtumissa. (Karkimo, 2015).

Asiantuntijahaastatteluiden lisäksi malli toimitettiin ensimmäiseen vaiheeseen osallistuneiden organisaatioiden edustajille kommentoitavaksi. Ensimmäisen vaiheen haastatelluista henkilöistä kukaan ei kommentoinut mallia määräaikaan mennessä.

Luvussa 6.2 kuvataan, miten tutkielman aikaisempien vaiheiden perusteella laadittu riskien arvioinnin prosessi malli validoitiin haastattelujen toisessa vaiheessa. Mallin validointi tarkoittaa tässä tutkimuksessa ensimmäisen vaiheen haastattelujen ja teorian pohjalta laaditun mallin esittelemistä asiantuntijoille ja ensimmäisen vaiheen haastatelluille sekä palautteen ja kehitysehdotusten keräämistä mallista. Mallin validointi voitaisiin asettaa kysymyksen muotoon: “Olisitko valmis ottamaan mallin käyttöön organisaatiossasi tai ottaisitko mallin käyttöön kuvitteellisessa organisaatiossa, jota johdat?” Mallin validoinnin kautta kerättiin palautteet ja kehitysehdotukset. Kerätystä materiaalista muodostettiin synteesi. Synteesi toimii pohjana mallin kriittiselle tarkastelulle ja lopullisen mallin luomiselle.

Malli toimitettiin tutkimukseen osallistuneiden organisaatioiden käyttöön ja julkaistiin kesällä 2016 osana pro gradu -tutkielmaa. Malli julkaistiin avoimesti julkaisujärjestelmässä sekä posterin muodossa. Posteria käytetään yleisesti muun muassa tieteellisissä konferensseissa (Tuomi & Sarajärvi, 2009) havainnollistamaan tutkimustuloksia selkeässä muodossa. Tutkimuksen posterissa kuvataan laadittu mallin yhdellä sivulla. Posteri esiteltiin ensimmäisen kerran tutkimusprosessiin liittyvässä seminaarissa Jyväskylän yliopistolla 8.6.2016. Muodostettu riskien arvioinnin malli löytyy tutkimusraportin liitteestä 10.

Kuviossa 12 on kuvattu tutkimuksen aikataulu. Tutkimuksen teoriapohja muodostettiin vuoden 2016 alussa tammi- ja helmikuun aikana. Samaan aikaan suoritettiin tutkimuksen ensimmäisen vaiheen kohdeorganisaatioiden rekrytointi ja valmisteltiin haastatteluaineisto. Haastattelut toteutettiin vuoden 2016 maalis- ja huhtikuun aikana siten, että tuloksia analysoitiin huhtikuussa 2016. Teoriapohjan ja haastattelujen tulosten synteesinä luotiin malli, joka validoitiin asiantuntijahaastatteluilla toukokuussa 2016. Toisen vaiheen asiantuntijahaastatteluiden jälkeen tehtiin johtopäätökset sekä kirjoitettiin tutkimuksen raportti. Tutkimus valmistui kesällä 2016.



KUVIO 12 Tutkimuksen aikataulu

5.5 Ensimmäisen vaiheen haastattelut ja aineiston analysointi

Kvalen (1996) ja Tuomen ja Sarajärven (2009) mukaan analysointia on liian myöhäistä miettiä haastattelujen jälkeen. Tässä aineiston analysointi -kappaleessa kuvataan analysoinnissa käytetyt menetelmät sekä teemat, joiden mukaisesti analysointia kohdennettiin päämäärätietoisesti ja tutkimuksen tavoitteen mukaisesti (Tuomi & Sarajärvi, 2009). Ensimmäisen haastattelukierroksen jälkeen kerätty haastattelumateriaali litteroitiin. Litterointi on aineiston koodaamista, jossa materiaalin tärkeitä kohtia osoitetaan, materiaalia jäsennetään ja keskeisiä kohtia kuvaillaan (Tuomi & Sarajärvi, 2009). Tutkimuksen resurssien tehokkaan kohdentamisen vuoksi litterointityö jaettiin tutkijoiden kesken. Litteroinnin raakamateriaali tallennettiin tutkimuksen tietokantaan analysointia varten. Analyysiin osallistuivat molemmat tutkijat, jolloin materiaalista oli mahdollista tehdä kattavammin havaintoja. Tutkijat analysoivat materiaalin ensin itse ja tekivät tämän jälkeen yhdessä synteesin havainnoistaan teemoina ja poimimalla keskeisiä haastateltavien lainauksia materiaalista. Kuvatun analyysimenetelmän etuina voidaan pitää analyysin kattavuutta, koska analyysin teki kaksi eri henkilöä verraten materiaalia aiempiin kokemuksiinsa ja koottuun teoriaan. Analyysimenetelmä huomioi kahden eri henkilön näkemyksen, jolloin löydöksiin suhtauduttiin todennäköisesti kriittisemmin kuin yhden henkilön löydöksiin. Keskeisimmät asiat tulee todennäköisesti myös kattavammin suo-

datettua, koska kaksi henkilöä luokittelee, teemoittelee ja tyypittelee aineistoa sekä kirjoittaa yhteenvedon. Aineiston analyysin tarkoituksena oli tuottaa tutkittavasta aiheesta uutta tietoa. Tähän pyrittiin selkeyttämällä ja tiivistämällä empiiristä aineistoa. Muodostetun mallin pohjana käytettiin kohdeorganisaatioista kerättyä empiiristä tietoa, jolla kartoitettiin organisaatioiden käytännön menetelmiä ja näkemyksiä riskien arviointiin ja tietoturvapolitiikan muodostamiseen liittyen. Tämä tavoite on yhtenevä Eskolan ja Suorannan (1996) esittämän näkemyksen mukaan siitä, mihin laadullisen aineiston analysoinnilla tulisi pyrkiä.

Aineiston analysoinnin lähtökohtana oli aineistolähtöinen sisällönanalyysi, jossa on tavoitteena edetä yksittäisistä havainnoista kohti yleisempiä väitteitä. (Eskola & Suoranta, 1996). Aineiston analysoinnin kautta tutkijat pyrkivät muodostamaan haastatteluaineiston kokonaisuudesta yksittäisten havaintojen ja yksityiskohtien kautta laajempia teemoja ja kokonaisuuksia, jotka lopulta konkretisoituvat muodostettavan riskien arvioinnin mallin kautta.

Analyysivaiheessa tutkijat jakoivat haastattelumateriaalin neljän teeman alle. Neljä teemaa on tiedon luokittelun kannalta mielekästä, koska mukaan teemoittelun tai tyypittelyn tulee olla tiivistävää (Tuomi & Sarajärvi, 2009). Neljän teeman perusteella oli myöhemmässä vaiheessa tarkoitus laatia riskien arvioinnin prosessimalli, joten teemojen tuli tukea mallin vaiheittaista rakentumista ja soveltuvuutta liiketoimintastrategiasta aina konkreettisiin organisaation tekemiin toimenpiteisiin.

Tutkijat olivat muodostaneet haastatteluiden rungon ja teemat tutkimuksen muusta taustamateriaalista muodostetun käsityksen perusteella. Lisäksi haastattelurungon muodostamiseen vaikutti se, mitä tutkijat halusivat haastatteluiden kautta selvittää. Eskolan ja Suorannan (1996) mukaan koodauksen kautta aineistoa tulisi jakaa pienempiin osiin, joita on helpompi tulkita. Eskolan ja Suorannan mukaan koodauksen voi suorittaa joko aineistoon tai aikaisempaan teoriaan perustuen ja koodauksen perusteena ja apuna voi käyttää aiemmin muodostettua haastattelun runkoa.

Tässä tutkimuksessa tutkijat käyttivät koodauksessa ja teemoittelussa molempia lähestymistapoja. Tutkijat olivat muodostaneet alustavan käsityksen muodostettavan riskien arvioinnin mallin tarpeista aiemman tutkimuksen ja muun tausta-aineiston perusteella. Tätä kautta koodausta ohjasi aikaisempi teoria. Empiirinen materiaali taas ohjasi koodausta organisaatioiden käytännön toiminnan osoittamaan suuntaan. Suuremmassa roolissa on kuitenkin ollut empiirinen aineisto, koska finanssialan organisaatioiden toiminta pohjautuu enemmän hyviksi havaittuihin käytänteisiin ja käyttöön valittuihin standardeihin, kuin tieteelliseen teoriaan.

Aineiston analysoinnin ja mallin muodostumisen pohjana käytettiin empiirisestä aineistosta löydettyjä samankaltaisuuksia, joille haettiin tukea ja vahvistusta aiemmasta tutkimuksesta ja tutkimuksen muusta tausta-aineistosta. Tämän teemoittelun pohjana käytettiin haastattelun rungon teemoja, mutta aineistoa analysoitiin avoimesti antaen mahdollisuus myös muiden teemojen esiin nousemiselle.

Hirsjärvi ja Suoranta (1996) sanovat, että onnistunut teemoittelu vaatii teorian ja empiirisen aineiston vuoropuhelun. Tässä tutkijat pyrkivät tähän vuoro-

puheluun etenkin luvussa 6.3, jossa esitellään muodostettu riskien arvioinnin prosessimalli. Teorian ja empirian linkittämisellä pyritään osoittamaan perustelut mallin muodostumiseen vaikuttaneille tekijöille.

Tutkijoiden muodostamat teemat toimivat finanssialan organisaatioiden haastattelujen runkona. Tutkimuksen ensimmäisen vaiheen haastattelujen teemat olivat seuraavat:

Teema 1: Riskien arviointi organisaation strategian toteuttamisen välineenä
Teema 2: Riskien arvioinnin prosessi
Teema 3: Riskien arvioinnin perusteena käytettävä tieto
Teema 4: Riskien arvioinnin tulosten vaikutus tietoturvapolitiikan laadinnassa

Teemojen valinnan taustalla oli tutkimuksen teorian kautta syntynyt kuva organisaation liiketoimintastrategian ja yksittäisten turvallisuustoimenpiteiden suhteesta. Jos tarkastellaan asiaa käänteisessä järjestyksessä, niin tietoturvapolitiikan tulisi perustua tehtyyn riskien arviointiin, joka perustuu edelleen organisaation keräämään tietoon. Organisaatio kerää tietoa omasta toimintaympäristöstään tavoitteena tukea omaa liiketoimintastrategiaansa. Organisaatiolla on näin ollen yksi strategia, jota kaiken muun toiminnan tulee tukea. Teema 4:n olisi voitu valita mikä tahansa organisaation liiketoimintastrategian toteuttamisen väline, mutta valitsimme tietoturvapolitiikan, koska:

- tietoturvapolitiikka löytyy konkreettisesti organisaatioista
- teorian perusteella tietoturvapolitiikka laaditaan riskien arvioinnin perusteella
- tietoturvapolitiikka laaditaan pääsääntöisesti tutkimukseen haastateltavien henkilöiden, tietoturvajohtajien, johtamissa yksiköissä

Teemojen rajaaminen mainittuihin neljään tuki ajatusta mallin ketteryyden kehittämisessä ja relevantin riskien arvioinnin perustana olevan tiedon löytämisestä. Teorian perusteella riskien arvioinnin prosessi ei välttämättä tue organisaation liiketoimintastrategian toteutumista ja johdon sekä turvallisuushenkilöstön välistä kanssakäymistä. Riskien arviointi tehdään jopa saman organisaation sisällä eri tavoilla, jolloin riskien arvioinnin tulosten vertailu on mahdotonta, koska tulokset eivät ole määrämuotoisia. Teemojen kautta oli mahdollista selvittää, miten riskien arviointi tehdään tutkittavissa organisaatioissa, miten prosessi etenee, mihin riskien arviointi kohteeksi valitut riskit perustuvat ja miten riskien arviointi konkreettisesti vaikuttaa organisaation toimintaan.

Toisen vaiheen asiantuntijahaastattelujen aineiston analysoitiin samoilla periaatteilla, kuin ensimmäinen vaihe. Teemat ja riskien arvioinnin prosessimalli oli muodostettu ensimmäisen haastattelukierroksen jälkeen. Tästä syystä aineiston analysointi oli luonteeltaan erilaista. Toisessa vaiheessa haastateltavia asiantuntijoita oli yhteensä kolme kappaletta. Haastatteluiden materiaalista etsittiin yhteisiä nimittäjiä ja kommentteja, mutta myös yksittäisen asiantuntijan kehitysehdotuksille annettiin painoarvoa mallin lopullista muodostusta tehtä-

essä. Muodostettua mallia muokattiin asiantuntijoiden kommenttien perusteella. Muokkaamiseen vaikuttaneita tekijöitä on pyritty tuomaan esiin omassa alaluvussaan (6.2 Toisen vaiheen haastattelut: mallin validointi).

Seuraavassa vaiheessa käydään teemoittain läpi ensimmäisen haastattelukierroksen aikana kertynyttä materiaalia. Teemoissa on kuvattu havaintoja yleisellä tasolla. Tutkimuksen tavoite on kuitenkin lopulta muodostaa riskien arvioinnin prosessimalli, jonka osalta on hyvin tärkeää huomioida organisaatiokulttuuriin liittyvät tekijät. Tästä syystä teemoissa on käytetty runsaasti lainauksia, jotta tutkijoiden oma tulkinta ei vaikuta lukijan saamaan käsitykseen organisaatioiden näkemyksestä. Organisaatiot jakoivat tietoa prosesseistaan varsin avoimesti. Tästä syystä teemojen käsittelyssä halutaan tuoda esille haastatteluissa esille nousseet eroavaisuudet. Luvun 5.5 alaluvut käsittelevät empiiristä aineistoa teemoihin pohjautuen. Merkittävin tutkimustulos, eli muodostettu riskien arvioinnin prosessimalli on erotettu omaan lukuunsa (6 Tutkimustulokset) siitä syystä, että se saisi tutkimusraportin kokonaisuudessa riittävän painoarvon.

5.5.1 Teema 1: Riskien arviointi organisaation strategian toteuttamisen välineenä

Ensimmäisen haastattelukierroksen teema 1 käsitteli riskien arviointia organisaation strategian toteuttamisen välineenä. Alla olevaan taulukkoon 3 on koottu organisaatioittain haastateltavien keskeisin näkemys organisaation antamaan strategiseen ohjaukseen riskien arvioinnin suorittamisessa. Teemassa 1 organisaatiot jaettiin kahteen luokkaan sen perusteella, että koetaanko organisaation strateginen ohjaus riittäväksi riskienhallinnan ja -arvioinnin toteuttamisen kannalta.

Taulukko 3 Organisaation strategian ohjaus riskien arvioinnin suorittamiseen

Organisaatio	Organisaation strategian ohjaus riskien arvioinnin suorittamiseen
A	Ei riittävää ohjausta. Osastot toimivat erillään.
B	Riittävä ohjaus on olemassa. Strategian kautta linjataan käytännön tekeminen, myös riskien arvioinnin osalta.
C	Antaa yleiset periaatteet. Turvallisuusorganisaatiolle on annettu laaja valta ja vastuu riskien arvioinnin suorittamiseen.
D	Riskienhallinta (ja -arviointi) on strategiasta irrallaan. Strategia ei suoraan vaikuta riskienhallinnan periaatteisiin (tai tietoturvaperiaatteisiin).
E	Riskienhallinta (ja -arviointi) on strategiasta irrallaan. Strategia ei suoraan vaikuta riskienhallinnan periaatteisiin (tai tietoturvaperiaatteisiin).
F	Organisaation strategia antaa laajat, yleiset perusteet, joiden mukaan on suuri vapaus toteuttaa riskien arviointi.

Strategian sekä riskienhallinnan ja -arvioinnin suhde vaihtelee suuresti eri organisaatioissa. Joissain organisaatiossa ne eivät ole millään tavalla yhteydessä. Osassa organisaatioista strategia antaa riittäväksi koetun ohjauksen. Yleisesti tutkimukseen osallistuneista organisaatioista voidaan todeta, että strategia antaa yleiset periaatteet ja suuntaviivat, mutta käytännössä riskienhallinnan ja -arvioinnin toteuttamiseen annetaan melko suuri vapaus strategian näkökulmasta.

Organisaatioissa B, C, E ja F strategia ohjasi riskien arvioinnin suorittamista yleisellä tasolla. Organisaatioissa C ja F strategia antoi yleiset perusteet, mutta vastuutaho, kuten turvallisuusorganisaatio, toteutti strategiaa parhaaksi katsomallaan tavalla. Organisaatiossa B strategian yhteys riskien arviointiin ja organisaation toteuttamiin toimenpiteisiin kuten tietoturvapolitiikkaan oli viety hyvin pitkälle:

> Elikkä meillä on niinku hyvinkin selvästi strategian kautta linjattu että mitä me tehdään. Et meillä se strategia on linjassa sen käytännön tekemisen kanssa. Siihen me ollaan näitten viime aikaisten muutosten kautta enemmän keskitytty et ne on niinku linjassa, mikä on ihan hyvä asia. Ja tota kun riittävän ohjauksen riskien arvioinnin suorittamiseen, niin ainoa mikä on, tai mihin ei ole näissä niin kun strategisissa linjauksissa keskitytty on enemmänkin ne työkalut.

Tietoturvapolitiikka rakentuu organisaatiossa B riskikarttojen perusteella, jotka taas perustuvat strategiaan. Organisaatiossa riskien arviointia tehdään kolmella eri tasolla: strategisella, taktisella ja operatiivisella "three lands of defence" -mallin mukaisesti:

> "First line of defence" on operatiiviset yksiköt, jotka käytännössä tekee asioita ja käytännössä 90% organisaatiosta kuuluu "first lineen". "Second line of defence" sitten määrittää ne vaatimukset joiden mukaan organisaation pitää toimia. Ja sit meillä on "third line of defence" joka on sisäinen tarkastus.

Käytännössä organisaation B:n käyttämä malli toimii seuraavalla tavalla strategiselta tasolta kohti operatiivista tasoa:

> Strategisella tasolla, se on enemmänkin semmonen "top down approach"... Riskienhallinta on määrittänyt semmosia isoja riskikokonaisuuksia. Otetaan nyt vaikka tosta IT:stä esimerkiksi se että meidän järjestelmät on.... Se stability mikä tossa mun kalvoilla näkyi, elikkä ne järjestelmät on käytettävissä. Elikkä ne järjestelmät ei ole käytettävissä on strateginen riski meille. Niin me määritetään se täällä ylätasolla, sen jälkeen me keskustellaan siitä strategisesta riskistä esimerkiksi liiketoimintayksikön kanssa, mikä sen riskin vaikutus toimintaan on. Ja sit se niinku pikkuhiljaa valuu tänne alaspäin tänne taktiselle tasolle, operatiiviselle tasolle.

Organisaation B käyttämä malli toimii seuraavalla tavalla operatiiviselta tasolta kohti strategista tasoa:

> Tää on sitten niinku bottom up, elikkä täällä tunnistetaan pikkusia riskejä sitten mietitään et miten niistä muodostuu isompi riskikokonaisuus. Esimerkiksi täällä ne voi olla näistä esimerkinmukaisesti voidaan tunnistaa riskejä jotka liittyy tietoliikenteeseen tai tiedon välittämiseen ulkopuolisille.... Ja sitten täällä kun meillä on järjestel-

> mien alhaalla olo niin okei tää network- yhteyden toimivuus vaikuttaa meidän järjestelmien käytettävyyteen elikkä siihen strategiseen riskiin mikä täällä ylhäällä oli määritetty.

Organisaatiossa B turvallisuusstrategia linjaa miten turvallisuus on linjassa organisaation liiketoimintastrategian kanssa. Strategia määrittää operatiivisia toimintoja, mutta prosessi toimii myös toisin päin. Turvallisuusstrategian muun muassa määrittää osaltaan tietoturvayksikkö:

> He (tietoturvayksikkö) käytännössä toteuttaa kaikki ne aktiviteetit tietoturvan varmistamiseen liittyen. He myös määrittää sen strategian, jos ajatellaan vaikka jotakin tietoturva tämmösien loukkausten selvittämiseen tai valvontaan tai monitorointiin liittyviä juttuja. Eihän riskienhallinta sano mitään muuta kuin, että semmosia voi olla. Ja sitten tää infosec-yksikkö miettii että miten ne käytännössä sen toteuttaa ja sitten heidän strategiassa linjataan että halutaan niinku painottaa vaikka lokitietojen analyysiä jotta me vastataan liiketoiminnan strategisiin tavoitteisiin.

Organisaatiossa C strateginen ohjaus ymmärretään haastatellun edustajan mukaan uudella tavalla, eli turvallisuusorganisaatiolle annettuna laajana mandaattina:

> ...No meil on niinku niinpäin ajateltu tää homma et meille on annettu johtokunnassa nimenomaan meille tämmönen mandaatti ja vastuu organisaation turvallisuusasioista. Ja silloin me annetaan suoraan organisaation turvallisuutta koskevat linjaukset eli tämmöiset soveltamisohjeet joiden kautta määritellään et mitä se turvallisuus organisaatiossamme tarkoittaa.

Organisaatiossa C kyseinen menettely nähdään nykyaikaisena versiona johdon sitouttamisesta:

> Ja tää on sitä tän päivän johdon sitouttamista eikä niin päin et me joka ******* (kirosana korvattu ****- merkeillä), anteeksi, lippulappu viedään sinne tota johtokuntaan tai johtoryhmään ikään kuin hyväksyttäväksi, vaan nimenomaan toisinpäin. Et annetaan se vastuu, annetaan se mandaatti, annetaan se mahdollisuus toimia ja reagoida nopeasti muuttuvaan turvallisuustilanteeseen antamalla ikään kuin sille turvallisuusorganisaatiolle iso vastuu ja mahdollisuus sit antaa näitä ohjeita ja linjauksia.

Tärkeimpänä asiana strategisessa ohjauksessa organisaatiossa C nähdään johdon kanta riskien sietokykyyn:

> Ja nyt se että mikä on sen johdon näkökulmasta se meidän riskinsietokyky tai riskinkantokyky turvallisuudessa on semmonen asia mikä on tärkee aina saada ikään kuin leimattua sieltä ylimmästä johdosta. Eli minä kun esitän meidän turvallisuuden näkökulmasta niinku sopivat mittarit esimerkiksi kokonaisturvallisuuden osalta, niin mun esimies sitten omalla näkemyksellään sanoo että onks tää hyvä tai ei oo ja tarvittaessa me sit käydään johtokunnassa se keskustelu että onko tämä taso nyt se mihin me tähdätään näillä turvallisuustoimenpiteillä.

Organisaatiossa C tiivistetään heidän näkemyksensä johdon sitoutumisesta, strategisesta ohjauksesta ja niiden vaikutuksesta operatiiviseen toimintaan:

> Se kauneus tässä kun mä puhuin siitä et ku jaetaan ikään kuin sitä vastuuta oikein organisaatiossa. Ja kun sä puhut turvallisuuden soveltamisohjeista ja nyt jos meillä olis se tilanne et mun pitäis jokaikinen lippulappunen viedä meidän johtokuntaan hyväksyttäväksi niin se ei olis kauheen nopeeta… sehän johtaa suoraan sit siihen et jos tarve on niin mä saan vaikka samana päivänä tai tunti sen jälkeen, kun joku tieto tulee, niin voin päivittää sitä meidän turvallisuuden soveltamisohjetta, voin nostaa rimaa, voin laskee sitä, voin ohjata turvallisuutta oikeelle tasolle valitsemalla niinku tavallaan uuden tyyppisen kontrolliluettelon tai uuden tyyppisen tavan tehdä asioita jotta ne niinku uhkat ei tuu läpi.

Organisaation C mukaan nykyinen maailma ei mahdollista niin sanottuja vanhoja menettelytapoja organisaation turvallisuuden varmistamisessa:

> Nää on nää tietoturvapolitiikat sun muut jutut niin ne on vähän, hyvät herrat, niin sellasta niinku staattista maailmaa, mikä vähän niinku meni jo.

Nykyaikainen malli pohjautuu organisaation C mukaan teknisiin valintoihin ja päätöksentekoon hetkessä:

> Kyl sun pitää niinku ohjata niillä teknisillä valinnoilla sitä niinku ja niillä prosesseilla sitä toimintaa niin hyvin kuin vaan mahdollista siihen suuntaan et tavallaan jossain vaiheessa niiden ohjeiden merkitys vähenee… sun pitää tehdä ne päätökset tässä ja heti, just sen muuttuvan ympäristön mukaan ja ne kontrollit pitäis rakentaa niin.

Organisaatio E kokee, että strategia antaa viitekehystensä kautta riittävät perusteet myös riskienhallinnalle.

> ...kyllä se meidän tota noin niin strategia niin kyllä se tähän ohjaukseen antaa sen riittävän ohjauksen siinä mielessä että nämähän tota noin niin ohjeistukset ja framworkit sisältää ne metodit ja menetelmät ja frekvenssit ja laajuudet missä suhteessa meidän pitää niinku riskejä arvioida, seurata ja monitoroida ja raportoida.

Organisaatiossa E strategia koetaan liiketoiminnan tahtotilaa kuvaavana linjauksena. Riskienhallinnan ja tietoturvan tulee tukea strategian toteutumista.

> ...strategiahan lähtee kuvaamaan niinku sitä liiketoiminnan tahtotilaa ja tota noin niin halukkuutta siellä ja silloinhan tään niinku riskienhallinnan ja tietoturvan pitää sitä peilata sillä tavalla että me huolehditaan ensinnäkin siitä että se perälauta ei vuoda…

Organisaation E näkemyksen mukaan liiketoimintastrategia edellyttää aina mahdollisuuksien mukaan kaikkien riskien saattamista numeraaliseen muotoon.

> Et tota se on niinku yks mikä tulee tällä tota riskienhallinnan puolella tulee on nimenomaan se että siellä määritetään se tota ruokahalu tota riskin suhteen. Ja se on tietysti se ongelma jos puhutaan tota operational riskistä, taikka tietoturvariskistä, millä sen saa kvantifioitua niin et tota noin niin kun liiketoimintastrategia kuitenkin päätyy johonkin numeroihin sun muuhun…

Organisaation F strategia antaa melko laajat vapaudet riskienhallinnan ja -arvioinnin toteuttamiselle. Tätä ei kyseisessä organisaatiossa kuitenkaan koettu millään tavalla ongelmaksi.

> ...organisaatiomme strategiassa lukee, että meidän tehtävä on tuottaa turvallista laatua ja siinä meillä on aika paljon vapauksia miten me se tulkitaan.

> Se menee siihen jatkuvuuteen, jatkuvuus on meidän suurin, suurin tämmöinen yksittäinen asia, asiakasvaatimus ja strategiassa lukee, että meidän pitää sitä toteuttaa. Vastaus kysymykseen: Me tulkitsemme itse sitä hyvin vapaasti niinkuin firmat yleensäkin tekee omistuspohjasta riippumatta, itse tuntevat oman ympäristönsä kaikkein parhaiten... ainakin pitäisi tuntea...

Organisaatioissa A ja D koettiin, että strategia ja riskien arviointi ovat erillään eikä strategia näin ollen vaikuta suoranaisesti riskien arvioinnin suorittamiseen. Organisaatiossa A kuvattiin, että organisaation eri osastot toimivat omalla tavallaan tulkiten organisaation strategiaa:

> ...Tää on viel meillä vähän niinkun hajallaan ja niinkun se kytkös et meillä oikeestaan niinkun tulevaisuuden, tämän päivän, tämmönen havainnointi, et toiminnasta tulevat havainnot ohjais siihen et se vaikuttais meidän riskien arviointiin niin ei toimi vielä riittävästi et me ollaan voisko sanoo vähän vielä vanhojen mallien vankeja.

Organisaatiossa A kuvattiin organisaation eri osastojen pitävän tiukasti kiinni osastojen välisistä rajoista:

> Noi mitkä tehdään noilla "osastoilla" (haastateltavan käyttämä ilmaus korvattu) prosesseittain, järjestelmittäin niin ne menee niinkuin siiloissa niillä "osastoilla" niitä ei silleesti käsitellä kuin siellä "osastoilla", meillä nämä "osastorajat" ovat aika tiukat ja ne haluukin pitää vähän mustasukkaisesti kiinni.

Organisaatiossa A koettiin lisäksi, että riskien arviointi on liian järjestelmäkohtaista, vaikka riskien arvioinnin tulisi keskittyä prosessien toimivuuteen. Organisaation turvallisuussuunnittelu keskittyy organisaation A mukaan liiaksi järjestelmien jatkuvuuden turvaamiseen ja kunnossapitoon.

Organisaation D mukaan organisaatiolla voi olla vain yksi strategia, josta kaikki muu ohjeistus ja toimenpiteet johdetaan:

> Mun kanta on se, että organisaatiossa voi olla yks strategia ja se on konsernin strategia, liiketoimintastrategia ja sen jälkeen tietoturvaperiaatteet, tietoturvaohjeet, tietoturvatoimenpiteet johdetaan siitä konsernin strategiasta.

Organisaatio D koki kuitenkin, että strategia ja riskienhallinta ovat toisistaan irrallisia asioita:

> Mä luulen et riskienhallinta on aikalailla siitä strategiasta irrallaan sillä tavalla et ei niitä oo formaalisti mietitty.

Riskienhallinnan tulisi pystyä johtamaan oma osuutensa strategian kautta. Organisaatiossa D tätä tapahtui lähinnä johtoryhmätasolla:

> Konsernin johtoryhmä miettii niitä strategisia riskejä, et siinä semmoinen linkitys on olemassa, mutta ei silleen ehkä tietoisesti rakennettu.

Organisaatio D ei kokenut, että muutokset strategiassa vaikuttaisivat oleellisesti tarpeeseen uudistaa esimerkiksi riskienhallinnan periaatteita.

> Sanotaan et nyt kun meidän strategia uudistu vuos sitten niin siinä vaiheessa riskienhallintaperiaatteita eikä myöskään tietoturvaperiaatteita ei otettu käsittelyyn.

Riskienhallinnan ja strategian yhteys koettiin organisaatioissa vaihtelevasti. Osa organisaatioista sai strategian kautta mielestään riittävän ohjauksen riskienhallinnan toteuttamiseen, kun taas osassa organisaatioissa ne koettiin siinä määrin toisistaan erillisiksi asioiksi, että ohjausta strategian kautta ei välttämättä edes odotettu annettavan.

Riskienhallinnan ja -arvioinnin merkitys organisaation liiketoiminnassa kuitenkin ymmärrettiin kaikissa organisaatiossa. Riskienhallinnan ollessa yksi merkityksellinen osa organisaation liiketoimintaa, tulisi organisaation strategisten linjausten pyrkiä huomioimaan se jollain tasolla.

5.5.2 Teema 2: Riskien arvioinnin prosessi

Teema 2 käsitteli yleisesti riskien arvioinnin prosessia sekä keinoja riskitiedon jakamiseen organisaatiossa. Alla oleva taulukko 4 antaa kuvauksen haastateltujen organisaatioiden riskien arvioinnin prosessista.

Taulukko 4 Kuvaus organisaatioiden riskien arvioinnin prosessista

Organisaatio	Kuvaus organisaatioiden riskien arvioinnin prosessista
A	Tietoturvariskien kartoittaminen vuosikellon mukaisesti → päivittäminen valmiiden pohjien mukaisesti (järjestelmävastaavat) → raportointi johdon riskiraportoinnissa. Tietoturvallisuuden riskien arviointi on tekniseen puoleen painottuva prosessi.
B	Kolme tasoa: strateginen, taktinen, operatiivinen. Arviointi lisäksi kahdessa kategoriassa: business- ja group unit. Riskikarttojen ylläpitäminen. Strategiset linjaukset ylhäältä alaspäin, riskien tunnistaminen alhaalta ylöspäin. Turvallisuusriskikartoitus vuosittain.
C	Riskienhallinta (ja -arviointi) tehdään turvallisuuden näkökulmasta operatiivisten riskien arvioinnin yhteydessä. Riskien arviointi on jatkuva prosessi. Koordinoitu riskien arvioinnin prosessi viedään läpi vähintään kerran vuodessa.
D	Kaksi kertaa vuodessa ohjattu riskienhallintakierros (sisältää arvioinnin suorittamisen). Riskit haetaan erilliseen työkaluun → johtoryhmä käsittelee tulokset → tiedoksi hallitukselle.
E	Vuosittainen riskien ja kontrollien arviointiprosessi → liiketoimintayksiköiden työpajat etukäteen määritettyjen skenaarioiden pohjalta → merkittävimpien riskien koostaminen → toimenpiteiden suunnittelu. Keskeisten riskien osalta arviointi tehdään kerran kvartaalissa ja lisäksi arvioidaan kuukausittain merkittävimmät riskit.
F	Vuosittain organisaation määrämuotoinen riskienhallinnan prosessi ja riskikartoitus. Arvioinnin päivittäminen ja ylläpitäminen on periaatteessa jatkuvaa, ei varsinaisesti koordinoitua prosessia. Toimintaympäristön muutoksia havaittaessa tarvittaessa asiantuntijaryhmien toiminnan kautta.

Kaikissa organisaatioissa järjestettiin ohjattu riskienhallintakierros vuosikellon mukaisesti. Vaihtelua syntyi muun muassa siitä, miten useasti kierros järjestettiin. Joissain organisaatiossa riskejä kartoitettiin kerran vuodessa, kun taas toisissa organisaatioissa riskien arvioinnin koettiin olevan jatkuva prosessi.

Merkittävimmät erot riskien arvioinnin prosessissa tulevat siitä, miten koordinoitu prosessi on ja miten aktiivisesti riskejä arvioidaan ohjattujen kierrosten välillä. Esimerkiksi organisaatio B toteutti riskien arvioinnin perehtyneiden ammattilaisten vetämissä työpajoissa. Organisaatio A ei ollut määrittänyt arvioinnin suorittamiseksi mitään tiettyä tapaa tai muotoa. Organisaatioissa

koettiin myös, että tietoturvallisuuden riskien arviointi on keskittynyt liikaa järjestelmien tekniseen puoleen.

> Organisaatio A: ...tääkin on vähän se perisynti näissä asioissa et kun me lähdetään tietoturvallisuutta tämmösten riskien arviointien kanssa tekemään niin nää aika pitkälle on, on täällä niinkun jonkin verran niinkun (toteaa itsekseen), nää liittyy enempi niinkun järjestelmiin, meilläkin nää mennään enempi niin kuin järjestelmäkohtaisesti.

> Organisaatio B: Meillä on tälläinen kvartaalikierto tällä hetkellä elikä noi strategiset riskit päivitetään kerran kvartaalissa ja sitten nää operatiivisen tason riskit päivitetään vähintään kerran vuodessa sillee että meillä on siihen työpaja, mut tottakai siinä päivittäisessä toiminnassa ne riskit on tunnistettu ja niihin liittyen esimerkiksi kehitystoimenpiteet on laadittu ja kehitystoimenpiteitä seurataan…

> Organisaatio D: Puolivuosittain tehtävät etenee siten, että meillä on henkilö joka vastaa siitä työkalusta ja siitä käytännön toimenpiteiden käynnistämisestä. Kaikille joille on merkitty joku vastuualue siellä riskienhallinnassa lähtee sähköposti ja ohjeet eli muistutus siitä miten se työkalu toimii…

> Organisaatio D: ...jos mä vastaan turvallisuusriskeistä niin sit se on minun vastuulla, minun asiani miettiä kuinka paljon käytän tällä kierroksella siihen aikaa, että katsonko vaan läpi nytten, että mikäs tää nykytilanne olikaan ja eipä tuu mitään mieleen ja ”done” vai kerääks mä jonkun porukan kasaan ja ”hei että mietitääs nyt että onks jotain riskejä jota ei ole huomattu tähän mennessä ja mikä tää tilanne nytten on”. Et tää saattaa vaihdella hyvin paljon organisaatiossa sen henkilön halun ja kyvyn ja aikataulun suhteen.

Organisaatiossa B kuvattiin organisaatioiden eri yksiköiden välistä merkitystä koko prosessin kannalta:

> ...meillä on kolme tasoa. Tää on “top down”, tää on “bottom up” (näyttää piirtämäänsä kuvaa). Tää “bottom up” on nimenomaan sitä että me... Tiettyyn tarpeeseen arvioidaan riskejä, se on enemmän semmosta “brainstorming” –asiaa, missä istutaan pöydän ääreen ja mietitään mitä riskejä tähän voi liittyä. Mutta syy miksi me ollaan otettu käyttöön tämmönen hyvin formaali malli on se että me pystytään vertailemaan meidän organisaation eri osia keskenään, tekemään niinku sisäistä “benchmarkkia” ja että me arvioidaan samalla tavalla riskejä. Koska silloin kun se on tämmönen pöydän ääreen koottu ryhmä joka rupee pohtimaan että mitä riskejä meillä on ja että onks nää nyt isoja vai pieniä riskejä. Ja silloin tässä huoneessa meidän riskit on isoja tos viereises huonees ne on tosi pieniä, vaikka me puhutaan samasta asiasta. Niin sen takia meillä on hyvin formaali malli tähän riskianalyysiin…

Organisaatiossa C otettiin esille organisaation kypsyystasot ja keinot riskien arvioinnin tekemiseen. Aikaisemmat Microsoft Excel -taulukkotyökaluilla tehtävät arvioinnit koettiin ongelmallisiksi, koska ne vievät huomion itse prosessista muun muassa epäolennaisiin seikkoihin:

> ...se maailma mihin ollaan menossa, että siinä mielessä se perinteinen että kaivetaan se Excel-luettelo esiin ja ruvetaan niinku arvioimaan et mitenhän nää ja sit se menee helposti sellaseen että mites tää muistitikku että mitäs tähän liittyy ja... Et se on vähän sellasta niinku... Sillä on paikkansa, aikansa se riippuu. Mennään taas siihen että

> mikä on sen organisaation kypsyys et jos sä vasta oot opettelemassa niin sillä on pirun iso merkitys että tehdään edes sitä jotta ymmärrys kasvaa.

Organisaatiossa C kuvataan näkemys myös siitä, miten riskien arvioinnin prosessin suoritus tulisi nykyisin tehdä:

> ...enemmän mennä siihen tavallaan maailmaan missä muutenkin eletään eli pyrkiä mahdollisimman dynaamisesti tuomaan asioita esille. Ja nyt sitten, kun me mietitään sitä perinteistä riskien arviointia, niin se on ehkä vähän staattista usein. Ja sitä just nimenomaan mietitään, no tehdään vaik se nyt kerran vuodessa tai tehdään näin. Se ehkä tuo niitä ratkaisuja sellaisiin isompiin asioihin, isompiin ehkä toimintamalleihin, kun valitaan jotain tapaa tehdä asiaa niin sieltä ehkä löytyy niitä ratkaisuja. Mut semmosta niinku operatiivista tavallaan niinku tietoa, operatiivista kontrollia, operatiivista vastetta koko ajan, niin eihän se synny sillä lailla, että me joka päivä vaan niinku istuttais alas ja mietittäis et mikäs meidän riskihomma täs nyt on, kun se menee kaikki aika siihen istumiseen, miettimiseen. Et sun pitäis saada se automatisoituu, et kyllähän se tottakai kyberturvallisuuden puolella niin on että et sul pitää olla ne tilannekuvajärjestelmät, sun pitää saada se prosessi niinku mahdollisimman automaattiseksi ja mielellään sen tyyppiseksi, että automaattisesti myös se sun hallintajärjestelmä kykenee tekemään päätöksiä, kykenee torjumaan niitä ulkoisia uhkia.

Organisaatiossa C tunnistettiin riskien arvioinnin prosessin ketteryyden tarpeet:

> ...Mut niinku idea siinä on se että katot tätä niinku molempiin suuntiin, sun pitää ymmärtää se koko ajan et nyt mitä mä teen päätöksenä niin se saattaakin olla huono ja mä sallin itselleni sen että mä voin kattoo taaksepäin ja palata askeleen taakse, kattoo uudestaan ja sit mennä eteenpäin.

Kaikki organisaatiot tiedostivat riskien arvioinnin tärkeyden ja sitä toteutettiin jossain määrin kontrolloidusti. Arvioinnin suorittamisen käytännön tavat ja etenkin arviointiprosessin kokonaisuuden koordinointi vaihteli suuresti organisaatioiden välillä. Niissäkin organisaatioissa, joissa prosessi ei perustunut esimerkiksi johdettuihin työpajoihin tiedostettiin riski siitä, että koordinoimattomuus saattaa johtaa subjektiiviseen ja organisaation sisällä huonosti vertailukelpoiseen riskitietoon.

Teemassa 2 käsiteltiin yleisen riskien arvioinnin prosessin kuvauksen lisäksi riskien arvioinnin tulosten jakamista organisaatiossa. Taulukossa 5 on kuvattu organisaatioiden keinot riskien arvioinnin tulosten jakamiseksi.

Taulukko 5 Riskien arvioinnin tulosten jakaminen organisaatiossa

Organisaatio	Riskien arvioinnin tulosten jakaminen organisaatiossa
A	Jakaminen toimialoittain. Toimialat päättävät erikseen laajuudesta. Johdolle yhteenveto 2krt / vuosi.
B	Tulokset jaetaan laajasti. Huolehditaan, että riskillä on aina operatiivisen tason omistaja, joka voi tehdä siihen liittyvät käytännön toimenpiteet.
C	*Asiaa ei käsitelty haastattelussa*
D	Kaksi kertaa vuodessa ohjattu riskienhallintakierros (sisältää arvioinnin suorittamisen). Riskit haetaan erilliseen työkaluun → johtoryhmä käsittelee tulokset → tiedoksi hallitukselle.
E	Liiketoimintayksiköillä on omat "riskimapit", johtoryhmällä laajempi kuva
F	Hallitukselle kerran vuodessa. Merkittävistä muutoksista tarvitsijoille lyhyelläkin aikajänteellä.

Teeman 2 taulukossa 5 käsitellään riskitiedon tulosten jakaminen organisaatiossa. Haastattelujen perusteella riskien arvioinnin tulosten jakaminen ei ollut pääsääntöisesti koordinoitua ja toisaalta tiedon jakaminen rajoittui hyvin pienelle osaa henkilöstöä, yleensä ainoastaan organisaation johdolle. Haastattelujen aikana joissain organisaatioissa havahduttiin siihen, että riskien arvioinnin tulokset pysyvät melko pienen ryhmän sisällä. Organisaatioissa todettiin suoraan, että tämä on selkeä puute tai jäätiin pohtimaan pitäisikö asialle tehdä jotain. Teemassa 3 asiaa on lähestytty myös prosessin kannalta toisesta suunnasta. Teemassa 3 havaittiin, että osassa organisaatioista henkilöstöllä ei ollut mahdollista antaa syötteitä analyysiä tekeville henkilöille. Tiedon kulkeminen organisaation sisällä toimijalta toiselle oli merkittävä puute niin teemassa 2 kuin teemassa 3.

Organisaatiossa A:ssa tunnistettiin ongelmat riskien arvioinnin tulosten jakamisessa:

> ...tää on viel meillä vähän niinkun hajallaan ja niinkun se kytkös et meillä oikeestaan niinkun tulevaisuuden, tämän päivän, tämmönen havainnointi, et toiminnasta tulevat havainnot ohjais siihen et se vaikuttais meidän riskien arviointiin niin ei toimi vielä riittävästi et me ollaan voisko sanoo vähän vielä vanhojen mallien vankeja.

Organisaatiossa A tunnistetaan muun muassa ennaltaehkäisy ja yhteistyö tulevaisuuden kehityskohteiksi:

> ...Kun jossain jotain tapahtuu, niin miten se sitten siinä ketjussa sitten hoidetaan, jos siellä sitten jotain, mut nyt tietoturvaongelmia tai muita sitten niinkuin, saatais se yhteensovittaminen tehtyä et kaikki niinkuin puhaltais yhteen hiileen siinä vaiheessa kun ruvetaan ongelmia selvittelemään. Parantamaan sitten... ennenkaikkea jos päästäis siihen ennaltaehkäisyyn.

Organisaatiossa B on riskien arviointi otettu osaksi organisaation päivittäistä toimintaa:

> ...Eli meillä on oikeastaan kolmen tasoisia... Kolmella tasolla riskien arviointia ja tota kartottamista ja myös hallintaa. Eli meillä on strateginen taso, sit meillä on taktinen taso ja operatiivinen taso… käytännössä se "first line" on vastuussa näistä operatiivisen tason riskien tunnistamisesta ja arvioinnista.

Organisaatiossa B kuvattiin riskienhallinnan ja liiketoimintayksiköiden välistä yhteistyötä riskien arvioinnin tulosten jakamisessa:

> Riskienhallinta on määrittänyt semmosia isoja riskikokonaisuuksia. Otetaan nyt vaikka tosta IT:stä esimerkiksi se että meidän järjestelmät on.... Elikkä ne järjestelmät ei ole käytettävissä on strateginen riski meille. Niin me määritetään se täällä ylätasolla, sen jälkeen me keskustellaan siitä strategisesta riskistä esimerkiksi liiketoimintayksikön kanssa, mikä sen riskin vaikutus toimintaan on. Ja sit se niinku pikkuhiljaa valuu tänne alaspäin tänne taktiselle tasolle, operatiiviselle tasolle.

Riskien arviointia kuvataan koko organisaation ja myös organisaation ulkopuolisten toimijoiden yhteistyöksi. Trendien tunnistamisen kautta data normalisoidaan, luokitellaan ja lopuksi keskustellaan asianomaisen tahon kanssa asiasta:

> ...Me haetaan enemmän niitä trendejä mitä maailmalla nähdään ja sitten sen pohjalta... Sitten mitä me sitten tehdään sille tiedolle niin me tietysti luokitellaan se ja muutetaan se dataksi tavalla tai toisella ja sen jälkeen me hyödynnetään sitä dataa. Meillä on aikamoinen tämmönen laskentamalli taustalla jolla me normalisoidaan se tietomäärä mikä meillä on ja kategorioidaan se yhdestä neljään. Ja sitä kautta me saadaa tietty "riski-indikaattori" tai riskiluku tietylle osa-alueelle. Ja sit me keskustellaan, eli riskienhallintayksikkö kokoo tän ja tekee tän analyysin ja yhteenvedon. Ja sitten kun meillä on jonkinnäköinen lopputulos niin me keskustellaan siitä lopputuloksesta sellasen tahon kanssa joka ymmärtää sitä.

Organisaation C osalta haastattelussa ei käsitelty riskien arvioinnin tulosten jakamista. Organisaation C prosessissa valta ja vastuu turvallisuuteen liittyvässä päätöksenteossa oli annettu turvallisuusorganisaation johdolle. Turvallisuusorganisaation johtaja pyrkii jakamaan riskien arvioinnin tulokset johdolle rahassa mitattuna:

> ...Kun me puhutaan euroista niin organisaation johto, varsinkin finanssimaailmassa, ymmärtää sitä paremmin...laadullinen homma, se on aina semmosta, siin jää aina se tulkintavara.

Organisaatiossa C nostetaan tiedon jakamisen osalta esille määrällinen ajattelu kyberturvallisuuteen liittyen. Määrällisen esityksen pohjana voi käyttää esimerkiksi vakavien kyberturvallisuustilanteiden määrää vuodessa:

> ...jos ajatellaan vaikka kyberturvallisuutta voitais todeta niin että vakavien kyberturvallisuustilanteiden määrä vuodessa. Se kuvaa sitä että kuinka hyvin sä oot arvioinut

> riskejä, kuinka hyvin sä ymmärrät muuttuvan toimintaympäristön aiheuttamat ongelmat tai haasteet sulle. Kuinka hyvin sä osaat ymmärtää sun bisnestä.

Organisaatiossa C turvallisuutta arvioidaan yhdessä liiketoiminnan kanssa, jolloin voidaan nähdä mihin suuntaan liiketoiminta on kehittymässä:

> ...me peilataan sitten ikään kuin tulevaisuuteen ja siihen näkemykseen, että missä vaiheessa eteenpäin tää liiketoiminta ikään kuin niinä omina "steppeinään" etenee ja me ikään kuin mennään ja duunataan itsemme siihen vuoteen, niin riskeihin, siihen muuttuvaan toimintaympäristöön, siihen muuttuvaan regulaatioon ja yritetään sitten siinä miettiä yhdessä mitkä ne riskit on nimenomaan siinä maailmassa.

Organisaatiossa B pyritään käyttämään riskien arvioinnin tulosten jakamisessa strategisen tason riskeistä termejä, joita johto ymmärtää kuten:

> ...kun me puhutaan strategisen tason riskeistä me puhutaan enemmän termeillä joita johto ymmärtää. Eli todennäköisyys ja meidän kyky torjua se uhka. Mikä on siis "impact" mutta ne ymmärtää sen "ability to manage" paljon paremmin.

Haastattelun aikana organisaatiossa D tunnistettiin mahdolliset puutteet riskien arvioinnin tulosten jakamisessa:

> ...Itse asiassa hyvä pointti, että tota se pysyy aika pienessä piirissä, että yksiköiden johtoryhmät näkee ne riskit, konsernin johtoryhmä, hallitus, asiakkaat (yksilöivä tarkenne poistettu)... tota ei laajemmin. Ei esitellä esimies infoissa, ei ole henkilökunnalle näkyvissä. En tiedä pitäiskö olla... Ei näytetä mun tietääkseni edes yleistä karttakuvaa, jossa näkyy eri osa-alueet: "tos on riskejä, tääl ei ole", ei laajemmin ole jakelussa. Asiakkaille näytetään sitten asiakastilaisuuksissa, että meil on esimerkiksi erään asiakkaan kanssa tämmöinen puoli vuosittainen "information security and compliance" -tapaaminen, jossa me kerrotaan meidän riskienhallinnan tilanne, jatkuvuussuunnittelusta, tietoturva "incidenteistä", mahdollisista muista poikkeamista... tämmöisissä tilaisuuksissa asiakkaille kyllä kerrotaan.

Organisaatiossa D tunnistettiin nykyisen riskien arvioinnin prosessin puutteellisuudet tuotettavan tuloksen suhteen:

> ...Yks sellainen huolenaihe mulla on tietysti tää yleinen suhtautuminen riskienhallintaan, käytetäänkö siihen aikaa ja onko siihen kytketty riittävästi ihmisiä. Mä en tiedä välttämättä, mutta mulla on sellainen tuntuma, että monessa tapauksessa riskienhallinta jää siihen, että henkilö joka vastaa tietystä sovellus- tai palvelualueesta huomaa, että "voi hitto nyt tulee deadline, mun täytyy kattoo nää riskit ja se on enemmänkin se riskin päivitys... et tota musta oikeempi tapa olis se, että otettais sitten jonkinnäköinen asiantuntija porukka ja käytettäis vähän enemmän aikaa ja käytettäis pari tuntia mitä täällä, onks nää nyt "valideja" riskejä, pitäiskö nää nostaa, tuleeks teillä jotain mieleen, sit saattaa usein olla se, että se johtoryhmä sitten miettii mitäs täs on tapahtunut ja mitä kuultu asiakkailta, mitäs nähty, että pitäiskö meidän nostaa esille vaikkei se ole tullut sieltä muualta. Se mun pelko on et se riskinäkymä on liian suppea et se tulee vaan tietyiltä henkilöiltä.

Organisaatiossa D kuvattiin heikkoudeksi riskien arvioinnin tulosten esittämisessä käytettävät asteikot:

> ...Riskienhallinnasta mä olen huolissani sikäli, että mä en ole lainkaan vaikuttunut, että nämä nykyiset riskienhallintamenetelmät toimii, että tästä on tehty pseudotiedettä, tehdään niinkun asteikkoja yhdestä viiteen ja ihmiset sitten jollain tavalla mukamas arvioi niitä jollain tavalla. Hämärtyy se, että joku sanoo et vakavuus kolme ja todennäköisyys neljä niin tota mihin perustuu.

Lisäksi organisaatio D kuvasi riskien arvioinnin käyttöä turvallisuuden ohjaustyökaluna, eli käytännössä riskien arvioinnin tulosten muokkaamisena halutun toiminnan aikaansaamiseksi:

> ...riskienhallinnasta tulee turvallisuuden ohjaustyökalu... että ja oon käyttänyt sillee et tiettyjä asioita oon yrittänyt saada organisaatiossa läpi, ei ole löytynyt resursseja, ei ole tehty, kunnes mä nostan sen riskien arvioinnissa näkyviin. Sit ku tiedetään... se menee tiettyyn prosessiin, se menee näkyviin asiakkaille, se menee näkyviin hallitukselle, jolloin siihen on pakko tarttua. Se on mulla ikäänkuin sellainen yks sellainen viimeinen keino, että jos asiat ei muuten... toki jos mä huomaan selkeesti riskejä ne nostetaan, mut jos on joku asia et mä kuvittelen et saan organisaatiossa käyntiin muutenkin ja se ei vaan lähde jostain syystä niin mä voin sit miettiä et arvioin tän isommaks riskiksi, vähintään keskimääräiseksi.

Organisaatiossa D mukaan organisaation prosessissa on puutteita tapahtuneista "inceidenteistä", loukkauksista, oppimisessa ja tiedon kertymisessä:

> Semmoinen heikkous tässä meidän riskienhallinnan prosessissa on, että ei ole sitä looppia takaisin päin, kun esim. tulee joku incidentti niin missään vaiheessa ei katsota, että miksei me ole havaittu tätä riskienhallinnassa, koska tää olis semmoinen, et tää olis pitänyt huomata... pitäiskö meidän nostaa tää myöhemmin riskiksi, et se riskin hallinta on ikään kuin irrallaan siitä tulevasta ja ikäänkuin ei arvioida sitä oliko se riskienhallinta toimiva.

Organisaatiossa E liiketoimintayksiköt järjestävät työpajat, workshopit, joissa käytetään apuna organisaation riskienhallinnan asiantuntijoita. Organisaation yksiköiden riskikansioista kerätään merkittävimmät riskit ja siirretään aina ylemmäksi kohti koko organisaation tasoa. Organisaation E mukaan osaaminen ja avoimuus riskien esille tuomiseen on parantunut. Kehittämisalueiksi nähdään vuosittaisten riskien arviointien pohjamateriaalin ja työpajojen kehittäminen.

> Et se osaaminen ylipäänsä on parantunut ja sanotaan tota avoimuus niinku riskien esille tuomiseen niin se on parantunut. Edelleenkin, sanotaan se niinku pohjamateriaali erinäköisiin, sanotaan varsinkin näihin vuosittaisiin riskiarviointeihin, se pitää vielä parantua. Tai sanotaan niinku siellä on vielä varaa parantaa. Ja sitten ehkä se tota toinen on se osaaminen sen keskustelun ja sen workshopin fasilitoinnissa niin se on varmaan semmonen missä meidän pitää tehdä töitä että me saadaan se tässä organisaatiossa paremmaks.

Pohjamateriaali riskien arviointien suorittamiseksi nähtiin organisaatiossa E erittäin olennaisena asiana:

> No sanotaan se mikä mikä mun mielestä tänä vuonna tuo organisaatio on sen valmistelussa onnistunut on nimenomaan se pohjamateriaalin luominen ja mukaan

saaminen koska se on... Jos sä otat tota kuudesta kymmeneen ihmistä keskustelemaan siitä että mitkä meidän riskit on, ja niillä on puuttellinen pohjamateriaali niin kyllähän se keskustelu nyt... Se ei oo sitä samaa ollenkaan ku että jos sulla on hyvä pohjamateriaali ja tota noin niin ja hyvä fasilitaattori joka pystyy sen keskustelun viemään läpi, kertoon mikä merkitys milläkin asialla siihen prosessiin on niin tota onhan siinä selvä ero. Ja sitten toinen on se että materiaalia on riittävän ajoissa käytettävissä jotta ihmiset pystyy siihen myöskin tutustuun

Organisaatiossa F riskitieto pyritään jakamaan laajasti sidosryhmille, jotta omaa toimintaa voitaisiin kehittää:

...keskeiset seikat, olkoon ne realisoituneita tai havaittuja asioita, joihin me ollaan valmistauduttu tai huomioitu turvallisuusuhkia niin ne menee meidän omistajille ja tietyiltä osin meidän asiakaspankeille. Se näkymä siirretään sinne koko ajan. Me pyrimme valmistamaan sen, että kun meidän asiantuntemus on luokitella, arvioida asioita ja me arvotamme niitä ykkösestä kolmoseen. Jos siellä on tällaisia kolmos riskejä niin kyl se eskalointi menee sitten eteenpäin. Jotta osapuolet, jotka tässä tapauksessa on asiakkaat ja omistajat pystyvät mahdollisesti itse arvioimaan mitä se heille tarkoittaa jos me ollaan tehty virhearvio, niin ne voi sanoa, et ”hei nyt pakkia et tää on niin tärkeä juttu et teidän pitää hoitaa tää”. Tällaista ei ole mun tietääkseni koskaan tapahtunut et me ollaan ilmeisesti aika hyvin osattu arvioida niitä riskejä.

Organisaatio F kertoi esimerkin avulla, miten riskien arvioinnin tuloksia pyritään jakamaan:

Esimerkki: meille tuli viime viikolla X (ilmoittaja poistettu) varoitus, että ”heipä hei, tän tyyppistä X (ongelman luonne poistettu) on nyt todettu käytettävän jossain päin maailmaa ja he antoivat suosituksen et miten voi estää tän X (ongelman luonne poistettu) vaikutukset. Ja me kokoonnuimme... tästä nimenomaisesta me sovimme erillisen palaverin, mutta normaalisti se menee meidän normaali istuntojen kautta. Me käydään se läpi, haetaan asiantuntijoilta näkemystä,...”onko tämä mahdollista meidän ympäristössä?”. Vastaus on et ei ole. Me todetaan et tällainen on tullut ja se on ”ykkönen”. Jos katsotaan et tää vois toimii meillä niin siinä tulee arvoksi kaks tai kolme todennäköisyyden pohjalta, et kuinka helppo se olis loppupeleis toteuttaa. Lyhyesti se menee noin, ei mitään rakettitiedettä…

Organisaatio F kertoi riskien arvioinnin tulosten jakamisen olevan erittäin hyvä viestinnän väline:

...Mun mielestä se, että riski- ideoiden kerääminen, se on koko organisaation tietämä toimintapa. Niitä riski-ideoita pitää saada esille sieltä. Se, että meillä on osaamisyhteisöt, meillä on viranomaisyhteisöt niin se on vähän eri asia, että me ollaan kuitenkin ammattilaisia niin itte jos me ei sitä hallita niin me ollaan ihan paskoja. Se, että otetaan se organisaatio mukaan siihen niin se, että löydetään ne keinot saada ihmiset avaamaan suu, että riski-ideoita tulisi. Tulee tuhat turhaa, ei mitää väliä, mutta siellä saattaa olla yksi helmi mukana, joka onkin merkittävä, niin se on tärkee ja hyväksi havaittu tapa. Sit me saadaan siitä hirveen hyvää viestinnän välinettä, että ”nyt on yks löytynyt, upee juttu”. Vaikeeta on juuri hyväksymiskriteerit, että me tuotetaan aina yhdenmukaisia tuloksia, se on tosi vaikeeta.

Organisaatio F kertoi, että riskien arvioinnin tulosten jakaminen on keino saada henkilöstö sitoutumaan yhteiseen toimintaan. Riskien arvioinnin suunnittelun, markkinoinnin ja ajan varaamisen kautta saadaan paras tulos:

> Riittävä aika pitää varata sille. Se on osa sitä suunnitelmaa, mutta se suunnitelma ei voi olla, että pitäis olla huomenna valmis... ei siitä tule... pitää olla järjestelmällinen... riittävä aika kun on varattu niin osallistaminen on paljon suurempaa. Perspektiivi on tällöin erilainen. Lisäksi tiedon ryhmittely ja tiettyihin asioihin keskittyminen siellä. Jos me on käytetty muiden ihmisten aikaa siihen niin on kohteliasta, että heidän havainnot on tullut käsitellyksi. Se on läpinäkyvää, että vaikka tuntui tyhmältä kirjoittaa listaa itsestään selvyyksistä niin se ei mennyt hukkaan. Se on osa sitä markkinointia. Ja kun sitä työstää sitä listaa, esimerkiksi työjärjestystä, varsinkin korjaava toimenpide niin ei aseteta sitä tavoitetta, että meidän pitäisi ratkaista se.

Arvioitaessa organisaatioiden riskien arvioinnin prosessia yleisesti ja riskitiedon jakamisen näkökulmasta, esiin nousi monia huomionarvoisia asioita. Tutkimukseen osallistuneiden organisaatioiden osalta käytännön tavat suorittaa riskien arviointia vaihtelivat suuresti. Osassa organisaatiossa riskien arviointi oli huomattavasti koordinoidumpi ja määrämuotoisempi prosessi, kun taas osa organisaatioista jätti enemmän vapauksia arvioinnin käytännön toteuttajalle. Ne organisaatiot, jotka pyrkivät määrämuotoiseen ja formaaleja tuloksia tuottavaan arviointiprosessiin tiedostivat lähtökohtaisesti nykyajan nopeasti muuttuvan toimintaympäristön asettamat vaatimukset joustavalle ja dynaamiselle riskien arvioinnin prosessille. Ketterämmän prosessin kautta niillä oli pyrkimys suurempaan ennaltaehkäisyyn ja ennakointiin sen sijaan, että tyydyttäisiin havainnoimaan parhaillaan meneillään olevia tapahtumia. Äärimmäisessä tilanteessa tämä johtaa jopa siihen, että organisaatio ei edes kykene havainnoimaan vain meneillään olevia tapahtumia, vaan organisaation toiminta keskittyy jo tapahtuneiden asioiden vaikutuksiin reagointiin.

Haastattelujen aineistossa organisaatioissa pääsääntöisesti arvostettiin riskien arvioinnin prosessia, joka on riittävän hyvin valmisteltu ja koordinoitu. Tätä kautta arvioinnin tuloksista saadaan huomattavasti luotettavammat ja vertailukelpoiset. Näihin tavoitteisiin pääsemiseksi esimerkiksi valmistellut työpajat ja laadukas pohjamateriaali koettiin tärkeäksi.

Riskien arvioinnin prosessin tulisi olla riittävän joustava, että henkilöstö saadaan sitoutettua sen suorittamiseen riittävällä tasolla. Riittävän joustava prosessi mahdollistaa myös helpomman riskitiedon ilmoittamisen, mikä saattaa tarjota organisaatiolle tärkeää tietoa yllättävistäkin lähteistä.

Arvioinnin tulosten esittämisen muodosta organisaatioilla oli monenlaisia näkemyksiä. Osa pyrki aina numeraaliseen muotoon. Yksi organisaatioista oli ehdottomasti sitä mieltä, että tähän tulee pyrkiä aina kaikkeen riskien arviointiin liittyen, myös kyberturvallisuudessa. Jotkin organisaatioista olisivat halunneet muodostaa riskien arvioinnin tuloksista mitattavia numeraalisia arvoja, mutta olivat sitä mieltä, että kyberturvallisuuden liittyen riskien arvioinnin perustana käytettävän datan määrä ei ole riittävä.

Riskitiedon jakamiseen liittyvät käytänteet vaihtelivat organisaatioiden välille. Poikkeuksetta kaikki organisaatiot kuitenkin kokivat, että analysoitu riskitieto ei saa jäädä liian pienen jakelun piiriin. Organisaatioiden tulisikin

miettiä, mikä on se vaikutus, mitä analysoidulla riskitiedolla halutaan saada aikaiseksi. Riskien arvioinnin tulokset antavat organisaatiolle arvokasta tietoa sen heikkouksista ja vahvuuksista. Tiedon riittävällä jakamiselle voidaan esimerkiksi nostaa henkilöstön tietoisuutta uhkista tai nostaa esiin sellaisia asioita, joita organisaatiossa voitaisiin tehdä paremmin.

Teeman 2 käsittelyn yhteydessä nousi esille riskien arvioinnin kannalta mielenkiintoinen ilmiö. Organisaatio C:ssä kuvattiin riskien arvioinnin käyttöä turvallisuuden ohjaustyökaluna. Lyhyesti kuvattuna ilmiö tarkoittaa, että riskien arvioinnin suorittava toimija nostaa tarkoituksellisesti riskien arvioinnin tuloksena olevia numeerisia arvoja (kuten asteikon 1-5 arvoja), jotta toimijan näkökulmasta merkityksellinen toimenpide saadaan hyväksytettyä organisaation johdossa. Tällöin riskien arvioinnin tulokset eivät ole vertailtavia alkuperäisessä merkityksessään, koska arvioihin vaikuttaa myös arvioitsijan henkilökohtainen näkemys aiempaa enemmän.

5.5.3 Teema 3: Riskien arvioinnin perusteena käytettävä tieto

Taulukossa 6 on kuvattu tietolähteitä, joita organisaatiot käyttävät riskien arvioinnin perusteena.

Taulukko 6 Organisaatioiden riskien arvioinnin perusteena käyttämät tiedon lähteet

Organisaatio	Organisaatioiden riskien arvioinnin perusteena käyttämät tiedon lähteet
A	Prosessiin osallistuvien "omasta päästä" ja valmiin pohjan kautta.
B	Laajamittainen tausta-aineiston kerääminen: organisaation sisäinen data, historiadata, analyysiraportit, auditointi, erilaiset riskiluettelot, kypsyysarvioinnit, erilaiset raportit. Tarkan tapauskohtaisen tiedon kerääminen sekä trendien tunnistaminen. Pyrkimys "data driven" -prosessiin.
C	Aktiivinen oma seuranta, kontaktit viranomaisiin, kontaktit muihin alan toimijoihin, kyberturvallisuukeskus, poliisi, KRP, erilaiset jakelulistat, tietoturvallisuuden tilannekuvajärjestelmät.
D	Asiantuntijoilta saatava tieto, kertynyt tietoturvatieto omista järjestelmistä, toimialan sisäiset ryhmät, kollegat, konferenssit, kyberturvallisuuskeskus, erilaiset julkaisut.
E	Konsulttitalot, organisaation oma data, ulkopuolelta kerättävä tieto, informaation vaihto alan sisällä.
F	Kansainväliset yhteydet, vertaisryhmät, alihankkijat, asiakkaat, viranomaiset, osaamisyhteisöt, keskustelupalstat, riskiideoiden kerääminen koko organisaatiosta.

Pääsääntöisesti organisaatiot pyrkivät hankkimaan riskien arvioinnin perusteena käytettävän uhkatiedon monipuolisesti eri lähteistä. Yhteistyön merkitystä korostettiin monessa organisaatiossa. Yhteistyön muodoiksi mainittiin esimerkiksi viranomaisten kanssa tehtävä yhteistyö ja erilaiset oman alan yhteistyöryhmät. Organisaation tulee itse tunnistaa tarvitsemansa tietolähteet. Parhaimmillaan riskien arvioinnin perusteena käytettävän uhkatiedon kerääminen oli erittäin kattavaa ja monipuolista. Tiedon keräämiseen pyrittiin esimerkiksi yhteistyön, julkisista lähteistä kerättävän tiedon, tapauskohtaisen tiedon ja tietoturvallisuuden tilannekuvajärjestelmien kautta. Niillä organisaatioilla, joilla tiedon kerääminen oli aktiivisinta ja monipuolisinta, voitiin todeta olevan erittäin hyvät valmiudet tunnistaa heidän toimintaansa uhkaavia riskejä ajoissa. Organisaatiossa A tunnistettiin organisaation puutteet riskien arvioinnin perusteena olevan tiedon lähteissä:

> ...meidän pitäisi alkaa enemmän tekemään tälle kun vaan, mä luulen et siel (viittaa organisaation johtoon) on helposti vastaus et onhan Viestintävirasto kattonut näitä juttuja, mut ne kattoo vähän niinkuin teknisesti ja vähän sen vanhan tietoturvamallin mukaisesti ja sillon ollaan auttamatta jäljessä, että muodollisesti, hallinnollisesti joitakin vanhoja ohjeita, standardeja vastaan hommat voi olla ihan hyvin, mut ku ne ei oikeen päde enää tän päivän maailmaan niin siinä meillä pitäis päästä sitten pidemmälle ja vähän niinkuin semmoiseen uuteen "moodiin".

Organisaatiossa A koettiin tilannekuvan muodostaminen ongelmalliseksi olemassa olevien menetelmin:

> ...ei ole oikeen semmosta voisko sanoa just tämmöstä niinkun tilannekuvan muodostamista/semmoista ympäristöanalyysiä, meillä tehdään sellainen tietty ympäristöraportti mitä niin kun yleisesti maailmalla tapahtuu, mutta ei se ole mitenkään riskiperustainen, se on enemmän sellainen "nice-to-know" et mitä ympärillä tapahtuu ja se käydään silloin tällöin johtoryhmässä läpi mut vielä ei ole mitään sellaista riskilähtöistä.

Organisaatiossa A koettiin taulukkotyökalu -pohjaiset riskien arvioinnin menetelmät toimintaa ohjaaviksi, vaikka nykyisin toiminnan tulisi perustua toimintaympäristön tarkasteluun:

> ...yks jatkuva keskustelun aihe, että tämmöset valmiit listat, ohjaako ne pelkästään niihin et pysytään niissä vanhoissa listojen mukaisissa riskeissä eikä mietitä et jotain uutta, rikolliset hyökkää finanssilaitosten järjestelmiin suoraan eikä mitään tämmösiä et tilat ei ole vaatimuksenmukaisia sillä ei ne hyökkääjät tule enää välttämättä konkreettisesti sisään, sisään, että mut kyl mä luulen et tänä päivänä enemmän ne tulee täältä valmiista malleista ja sitten jos mä saan jotain tuotua esille, et nyt on tällainen uus ilmiö päällä tälle pitäisi alkaa tekemään jotain, et miten mä saan sitten johtoryhmän innostumaan siitä... Niin lähinnä sitä kautta.

Organisaatio A:n edustaja nosti esille, että henkilöstö on suoraan yhteydessä häneen mahdollisten riskien osalta. Päivittäinen yhteistyö on tärkeää. Organisaatio B käyttää riskien arvioinnissa formaalia, määrämuotoista, esitystapaa, jotta eri osastojen välinen riskitasojen vertaaminen on mahdollista:

> ...silloin kun se on tämmönen pöydän ääreen koottu ryhmä, joka rupee pohtimaan että mitä riskejä meillä on ja että onks nää nyt isoja vai pieniä riskejä. Ja silloin tässä huoneessa meidän riskit on isoja, tos viereises huonees ne on tosi pieniä, vaikka me puhutaan samasta asiasta. Niin sen takia meillä on hyvin formaali malli tähän riskianalyysiin.

Organisaatio B:n toiminta perustuu kaikkeen organisaatiosta ja sen ulkopuolelta saatavaan tietoon.

> ...kun toi meidän tieturvapolitiikka perustuu tähän meidän "landscapeen", riskikuvaan, niin se riskikuva muodostuu meidän operatiivisista riskiestä, taktisista riskeistä, kaikesta siitä datasta mitä me organisaatiosta saadaan irti, niihin tulevaisuuden näkymiin mitä me odotetaan. Eli käytännössä niin kaikki ne käytännön toimenpiteet joita vuoden aikana on tehty sen tietoturvapolitiikan niinku toteuttamiseksi, niin ne tavalla tai toisella työntää tietoa siihen uhkakarttaan, "threat landscapeen", riskikart-

taan, jota käytetään sitten seuraavan vuoden analyysin, tai ton politiikan päivittämiseen.

Organisaatio C:ssä kuvattiin yhteistyötä muiden toimijoiden kanssa merkittäväksi tiedon lähteeksi:

> Me ite tottakai seurataan (riskejä), meillä on aika hyvä resursointi turvallisuuden osalta ja nimenomaan kyberturvallisuuden osalta ja on todella hyvät kontaktit viranomaisiin, on hyvät kontaktit muihin pankkitoimijoihin, muihin toimijoihin tällä alueella eli meillä on tämmöistä niin sanotusti eri toimijoiden välistä yhteistyötä josta sitten ikään kuin nousevaa uhkatietoa tai olemassa olevien järjestelmien uhkatietoa saadaan.

Organisaatio C täsmensi yhteistyökumppaneita:

> ...jos ajattelee viranomaispuolta niin esimerkiksi kyberturvallisuuskeskuksen kanssa ... hyvin tarkkaan ja hyvää yhteistyötä tehdään ja tota tietysti poliisi on myös, KRP ja paikallispoliisi on myös tahoja. Ne ei ehkä oo sellasia mistä sitä niinku tavallaan tulevaisuuden haltuunottoon liittyvää niinku tietoa tulee mutta et sitten on tietysti kaikennäköset "vendorit", tietyntyyppiset jakelulistat, "threadit", missä tätä tietoa niinku koko ajan liikkuu. Kyl me niitä niinku seurataan koko ajan aktiivisesti. Ja meillä on tietysti tietoturvallisuuden tilannekuvajärjestelmät ja muut jotka myös sitten tuottaa meille ymmärrystä paremmin asioista.

Organisaatio C kuvaa ulkopuolisen avun käyttöä riskien arvioinnissa tapauskohtaiseksi:

> ...ulkopuolista apua niin sen niinku oman analyysin tekemiseen ei lähtökohtaisesti käytetä koska me vähän lähdetään siitä liikkeelle et jos me ei ite ymmärretä tätä omaa bisnestämme niin vähän huono happi, ikäänkuin sit arvioida. Mut et sit jos meillä on tälläsiä uusia hankkeita tai tän tyyppisiä et nyt pitäis johonkin uuteen tilanteeseen niinku arvioida alustavia uhkia tai mitenhän tän homman ottais haltuun tai mikähän tätä uhkais niis me käytetään ehkä tämmösis niinku tavallaan jos tarvitaan jonkinnäköinen snapshotti jostain niinku jostain osa-alueesta niin niis me ollaan sit käytetty muunmuassa niinku konsultteja apuna arvioimaan niinku siihen tilanteeseen tai vaikka niinku uuteen liiketoiminta-avaukseen liittyviä mahdollisia riskejä...Tääkin on vähän silleen niiinku paisuntasäiliön käyttö et jos omat resurssit on niinku tukossa niin sit on hyvä ottaa vähän apua muualtakin.

Organisaatiossa C pidettiin tärkeänä päätöksentekokykyä. Kontrollien ja päätöksentekokyvyn suhde nostettiin erityisesti esille:

> ...sun pitää tehdä ne päätökset tässä ja heti, just sen muuttuvan ympäristön mukaan ja ne kontrollit pitäis rakentaa niin.

Organisaatio C:n näkemyksen mukaan turvallisuusorganisaatiolle delegoitu laaja päätöksenteko-oikeus antoi sille mahdollisuuden reagoida nopeasti havaittuihin toimintaympäristön muutoksiin. Organisaatio D saa tietoa laajasti yhteistyökumppaneita:

> Asiantuntijoilta, vuoden aikana tapahtuneista "incidenteistä" esimerkiksi, tietoturvapuolella sitten tietysti, tietoturvatietoahan tulee koko ajan, sitä me saadaan monesta lähteestä. Erilaisista finanssitoimialan sisäisistä ryhmistä, kollegoilta, kyberturvallisuuskeskuksesta, konferensseista, julkaisuista eli se on tietoturvapuolihan on sitä et se ymmärrys kerääntyy siinä pikkuhiljaa että tulee kaikenlaista tietoa ja se tilannekuva rakentuu ja sitten asiantuntijoiden kautta tietysti, että Windows-asiantuntija, tietoturva-arkkitehti, tietoturvatestaaja saattaa tuoda jotain esille. Öö, sitten mulla on tällainen tietoturvan virtuaalitiimi, eli mä tapaan kvartaaleittain nimetyt about 15 henkilöä ympäri organisaation eli mä kerron miltä tietoturva näyttää mun näkökulmasta ja he kertoo onko he nähnyt jotain mielenkiintoista organisaatiossa ja mikä toimii mikä ei toimi, onks jotain uutta tulossa niin tätä kautta niitä saattaa myös tulla.

Organisaatio E kuvaa riskien arvioinnin perusteena käytettäviä tiedon tuottajia yleisesti:

> …No tota jos me katsotaan koko tätä materiaalia niin toki yks lähde on erinäköiset informaation tuottajat ja eri näköiset konsulttitalot joista tulee osa tästä materiaalista. Osa tulee tota noin niin meidän omasta datasta ja mitä meillä käytännössä on insidenttitietoa olemassa siitä mitä meille on tapahtunut ja sitä käytetään. Ja sitten se missä ehkä eniten käytetään ulkopuolista tietoa, kerätään niinku koko ajan sitä tietoa ulkopuolelta, eri näköisiltä toimijoilta sun muilta on tietysti tietoturvan alue. Et se on niinku siinä mielessä se alue jossa kaikkein eniten kerätään ulkopuolelta koska tota, koska se on niinku relevanttia ja tota noin niin se on myöskin alue jossa niinku selkeesti nähdään se että pitää myöskin pystyä entistä enemmän alan sisällä vaihtamaan informaatiota.

Ja tämän jälkeen oman henkilöstön osalta:

> ...tota noin niin kyllähän he (henkilöstö) vaikuttavat lähinnä niiden omien liiketoimintayksikköjensä "workshoppien" kautta. Mut sitten kun puhutaan näistä erikoisyksiköistä niin kyllähän täällä henkilöstö nimenomaan on se joka, asiantuntijat jotka pitää itsensä ajan tasalla siitä mitä maailmalla tapahtuu sun muuta ja tuo aktiivisesti sitä tietoa käsittelyyn. Mut tota noin niin jos me ajatellaan niinku pankkiakin niin meillä on kuitenkin merkittävä osuus meidän henkilöstöstä... niin nehän on konttoreissa ja eihän heillä ole sellasta mahdollisuutta tuoda mitään kontribuutiota täämmöiseen prosessiin ulkoisista uhista. Korkeintaan ne tietää että jos tota niin jossain lähiössä alkaa oleen entistä enemmän rauhattomuutta niin onko sitten jotain fyysistä uhkaa. Mut ku ei niissä konttoreissa oo kohta enää rahaakaan niin ei siellä oo enää hirveesti sitä ryöstön uhkaakaan.

Organisaatio E nostaa esille riskien arviointityökalujen kehityksen ja riskien esille tuomisen:

> ...kyllähän tää jatkuva riskin arviointi… niin täytyy myöntää että onhan tässä tapahtunut melkoinen kehitys viimeisen reilun kymmenen vuoden aikana. Et se osaaminen ylipäänsä on parantunut ja sanotaan tota avoimuus niinku riskien esille tuomiseen niin se on parantunut.

Organisaatio F kuvaa, että tietoa tulee laajasti toimialalta, viranomaisilta, vertaisryhmiltä, osaamisyhteisöistä, alihankkijoilta ja jopa organisaation ulkopuolisilta kansalaisilta. Organisaatio haluaa myös pystyä osoittamaan, mihin kaikkiin ryhmiin se kuuluu, dokumentoida sen tarkasti ja kertoa sidosryhmille:

> ….me ollaan tarkasti dokumentoitu se, että mihin osaamisyhteisöihin me kuulutaanmistä kanavista me vastaanotamme tiedot... et meil on sopimus et meille toimitetaan tietoa et mihin erilaisiin osaamisyhteisöihin me kuulutaan ja mikä sen tarkoitus on ja mitkä ne muut osallistujat on. Se on yks tapa osoittaa sitä, että me toimimme huolellisesti... me olemme miettineet mitä kumppaneita me tarvitaan... kuka voi tarjota meille sitä ennakkovaroitusta tai muuta informaatiota, jota me sitten pystymme käyttämään ja varautumaan ennalta. Et se preventiivisyys tulee ja tää on ihan hirveen tärkee asia, et kun me, pitää pystyä osoittamaan sitä et me tehdään asioita hyvin ja huolellisesti ja tää on yks ilmentymä siitä... millä foorumeilla meidän pitää olla paikalla, me vaikka maksetaan siitä (painottaa sanomaansa), jos tiedetään et toi on se foorumi ja me halutaan sinne paikalle niin meidän tulee miettiä miten me sinne päästään. Meillä on semmoinen kymmenen keskeistä osaamisyhteisöä, foorumia mihin me kuulutaan plus sit tietenkin palvelut "US-cert", "cert.fi" tällaiset ja muutama tällainen ei kaupallinen toimija, ei viranomainen eikä kaupallinen toimija, mut on virtuaalisia osaamisyhteisöjä eri keskustelupalstoilla, joista tulee myöskin tietoa sitten, et nää on ne asiat...mut se on sellainen, et pystytään osoittamaan et missä me ollaan, miksi me ollaan, ketä muita siellä on ja mitä hyötyä siitä on... mitä me halutaan heiltä.

Organisaation F:n kuvaama tiedonhankinnan kanavien lähestyminen organisaation omista lähtökohdista toistui kaikissa organisaatioissa jossain muodossa. Keskeistä on tunnistaa tarvittava tieto ja pyrkiä osaksi tietoa jakavia ryhmiä.

5.5.4 Teema 4: Riskien arvioinnin tulosten vaikutus tietoturvapolitiikan laadinnassa

Taulukko 7 kuvaa tietoturvapolitiikan roolia organisaatiossa.

Taulukko 7 Tietoturvapolitiikan rooli organisaatiossa

Organisaatio	Tietoturvapolitiikan rooli organisaatiossa
A	Strategisen ohjauksen antava asiakirja.
B	Vuosittain luotava asiakirja, jonka kautta pyritään luomaan toiminnalle painopisteitä. Politiikkaa täydentää organisaation oma tietoturvastandardi.
C	Ylätason asiakirja, jossa määritellään turvallisuusorganisaation valta ja vastuu. Alemman tason asiakirjoilla pyritään vaikuttamaan käytännön toimintaan.
D	Tietoturvapolitiikka on ylätason ohjaava asiakirja.
E	Tietoturvapolitiikka on konsernin hallituksen päättämä peruslinjaus toimenpiteistä. Politiikkaa täydentää yksityiskohtaisempi ohjekokoelma ja sitä tarkemmat ohjeistukset.
F	"Organisaation tahdon ilmaisu". Asettaa suuntaviivat ja vaatimukset organisaation toiminnan alla oleville muille organisaatioille.

Tietoturvapolitiikka voidaan ymmärtää monen eri tason asiakirjaksi aina strategiselta tasolta järjestelmäkohtaisiin ohjeisiin. (Whitman & Mattord, 2010). Kaikki tutkimukseen osallistuneet organisaatiot pitivät tietoturvapolitiikka (tai tietoturvaperiaatteita) ohjaavana ylätason strategisena asiakirjana. Tietoturvaperiaatteiden koettiin antavan organisaation tietoturvallisuudelle yleiset linjaukset ja suuntaviivat, joita täydennettiin yksityiskohtaisemmilla ohjeilla. Yksi organisaatioista käytti tietoturvapolitiikkaa siten, että se päivitettiin vuosittain ja sen avulla luotiin painopisteitä organisaation tietoturvallisuuden kehittämiseen.

Organisaatio A toimintamalleja kutsutaan tietoturvaperiaatteiksi, joita ei muokata kovin usein. Viimeiseen kolmeen vuoteen periaatteisiin ei ole tehty muutoksia. Tietoturvaperiaatteita ohjaa taas organisaation ylemmän tason ohjeistus.

Organisaatio B kuvaa tietoturvapolitiikan roolia organisaatiossa painopistealueiden luojana:

> …mietitään että mikä, miten me nähdään sen kyseisen riskin muutokset tai vaikutukset meidän organisaatioon seuraavan vuoden aikana...me päivitetään kerran vuodessa tuo tietoturvapolitiikka. Ja sen riskikartan perusteella me otetaan fokusalueet meidän politiikkaan.

Organisaatio B korostaa henkilöstön tietoisuutta ja sen yhteyttä politiikkaan. Organisaation tietoturvapolitiikka antaa henkilöstölle kuvan muun muassa keskeisistä tietoturvariskeistä:

> ...se tarkoittaa et meidän (jokin riskien arvioinnissa havaittu asia) on heikentynyt ja sitten meidän pitää politiikassa keskittyä siihen että joka ikisen henkilön pitää ymmärtää perus tietoturvariskit. Ja se on sitten meidän painopistealue politiikassa sille.

Organisaatio C kuvaa organisaatioiden asemointia omaan toimintaympäristöön ja tätä kautta syntyviä turvallisuuden linjauksia, joita muun muassa tietoturvapolitiikat edustavat:

> …Ja tota tää on niinku se juttu eli sen lisäksi että sä arvioit uhkaympäristöä, sä ymmärrät että minkälaisia vaatimuksia siihen liittyy, miten sä asemoidut siihen itse siihen uhkaympäristöön. Sun pitää myös sitte kattoa koko ajan sitä et mitä tapahtuu, eli paljon osuu tuulettimeen, minkälaisia yrityksiä, mitkä meni ehkä vähän niinku läpi, missä meidän pitää ikään kuin korottaa kontrollitasoa, missä me ollaan riittävällä tasolla, koska se vaikuttaa siihen et miten me linjataan sitä turvallisuutta ja miten sitä pitää tehdä.

Organisaatio C:n toimenpiteet omassa toimintaympäristössä siirtyvät tarpeen mukaan myös tietoturvapolitiikkaan:

> …Ja nyt kun me saadaan (...) sitä reaaliaikaista tilannekuvaa, sitä tavallaan et nyt tällästä tapahtuu meille, niin sehän johtaa suoraan sit siihen et jos tarve on niin mä saan vaikka samana päivänä tai tunti sen jälkeen kun joku tieto tulee niin voin päivittää sitä meidän turvallisuuden soveltamisohjetta, voin nostaa rimaa, voin laskee sitä, voin ohjata turvallisuutta oikeelle tasolle valitsemalla niinku tavallaan uuden tyyppisen kontrolliluettelon tai uuden tyyppisen tavan tehdä asioita jotta ne niinku uhkat ei tuu läpi.

Tietoturvapolitiikka tai -periaatteet voidaan mieltää yhdeksi keinoksi, jolla organisaatio pyrkii vaikuttamaan riskien arvioinnissa havaittuihin riskeihin. Taulukko 8 kuvaa organisaatioiden käytäntöjä siinä, että vaikuttavatko riskien arvioinnin tulokset käytännössä tietoturvapolitiikan muodostumiseen.

Taulukko 8 Riskien arvioinnin tulosten vaikutus tietoturvapolitiikan muodostumiseen

Organisaatio	Riskien arvioinnin vaikutus tietoturvapolitiikkaan
A	Ei merkittävää vaikutusta. Periaatteet olleet viimeiset kolme vuotta muuttumattomat.
B	Tietoturvapolitiikka perustuu laadittuun riskikarttaan. Vuoden aikana kertyvä data vaikuttaa käytännössä seuraavalle vuodelle laadittavaan tietoturvapolitiikkaan.
C	Vaikuttaa. Arvioinnin tulokset menevät "turvallisuuden soveltamisohjeisiin". Merkittävät muutokset tilannekuvassa saadaan tarvittaessa nopeastikin vietyä käytännön tason ohjeistuksiin ja toimintaan.
D	Ei vaikutusta.
E	Riskien arvioinnin tulosten muuttuessa olennaisesti arvioidaan myös politiikoiden / periaatteiden päivittämisen tarve uudelleen.
F	Vaikuttaa paljon. Tietoturvapolitiikalla pyritään vastaamaan riskien arvioinnissa havaittuihin riskeihin.

Tarkasteltaessa riskien arvioinnin tulosten vaikutusta tietoturvapolitiikan muodostumiseen huomattiin, että kaikki organisaatiot eivät kokeneet arvioinnin tulosten vaikuttavan siihen mitenkään. Vastauksissa oli kuitenkin huomattavia eroja. Suurin osa organisaatioista koki, että riskien arvioinnin tulokset vaikuttavat siihen, millaiseksi tietoturvapolitiikka muodostuu. Tietoturvapolitiikkaa esimerkiksi käytettiin selkeästi keinona vastata havaittuihin riskeihin. Jotkin organisaatiot kokivat tarpeen tietoturvapolitiikan päivittämiselle vasta silloin, jos riskikentässä huomattiin ilmenneen merkittävitä muutoksia. Organisaatio A kuvaa tietoturvaperiaatteiden muodostamista:

> Voisko sanoa, että periaatteiden muodostaminen on sitä, että minä katon niitä läpi ja havannoin maailmaa ja keskustelen jos tuolta toimialoilta tulee jotain jota tarvii tehdä ja sitten muutetaan sitä, mutta et miten viedään sit riskiarvioinnin muut havainnot sinne käytäntöön sitä kuvattiin enemmän nyt on sitä politiikan toteuttamista tai jotkut puhuu riskiarvioinnin suunnitelmasta mitä me tehdään tietoturvassa tänä vuonna.

Organisaatio B kuvaa riskikuvan vaikutusta tietoturvapolitiikkaan:

> Meidän tieturvapolitiikka perustuu tähän meidän "landscapeen", riskikuvaan, niin se riskikuva muodostuu meidän operatiivisista riskiestä, taktisista riskeistä, kaikesta siitä datasta mitä me organisaatiosta saadaan irti, niihin tulevaisuuden näkymiin mi-

tä me odotetaan. Eli käytännössä niin kaikki ne käytännön toimenpiteet joita vuoden aikana on tehty sen tietoturvapolitiikan niinku toteuttamiseksi, niin ne tavalla tai toisella työntää tietoa siihen uhkakarttaan, "threat landscapeen", riskikarttaan, jota käytetään sitten seuraavan vuoden analyysin, tai ton politiikan päivittämiseen. Elikä se on semmonen sykli. Ja se toimii ihan käytännössä.

Organisaatiossa C uhkien arvioiminen vaikuttaa siihen, miten organisaatio asemoituu:

Niin kyllähän se vaikuttaa, koska lähtökohtahan on tottakai se sitten kun me ymmärretään, arvioidaan riskejä, ymmärretään, että mikä se meidän tavallaan niinku asema siinä regulaatioympäristössä, siinä uhkaympäristössä on, niin kyllähän se sitten vaikuttaa siihen kun me tehdään sitä tietoturvapolitiikkaa. Ja täs mä nyt puhun siis näistä meidän turvallisuuden soveltamisohjeista, joissa me määritellään se nyt normaali turvallisuuspolitiikan taso , niin tottakai se vaikuttaa, et se menee suoraan sinne...

...ja tota tää on niinku se juttu eli sen lisäksi että sä arvioit uhkaympäristöä, sä ymmärrät että minkälaisia vaatimuksia siihen liittyy, miten sä asemoidut siihen itse siihen uhkaympäristöön. Sun pitää myös sitte kattoa koko ajan sitä et mitä tapahtuu, eli paljon osuu tuulettimeen, minkälaisia yrityksiä, mitkä meni ehkä vähän niinku läpi, missä meidän pitää ikään kuin korottaa kontrollitasoa, missä me ollaan riittävällä tasolla, koska se vaikuttaa siihen et miten me linjataan sitä turvallisuutta ja miten sitä pitää tehdä.

Organisaatiossa C reaaliaikainen tilannekuva vaikuttaa lähes välittömästi organisaation turvallisuuden soveltamisohjeisiin:

...Ja nyt kun me saadaan (...) sitä reaaliaikaista tilannekuvaa, sitä tavallaan et nyt tällästä tapahtuu meille, niin sehän johtaa suoraan sit siihen et jos tarve on niin mä saan vaikka samana päivänä tai tunti sen jälkeen kun joku tieto tulee niin voin päivittää sitä meidän turvallisuuden soveltamisohjetta, voin nostaa rimaa, voin laskee sitä, voin ohjata turvallisuutta oikeelle tasolle valitsemalla niinku tavallaan uuden tyyppisen kontrolliluettelon tai uuden tyyppisen tavan tehdä asioita jotta ne niinku uhkat ei tuu läpi.

Haastateltu henkilö laatii organisaatio D:n tietoturvaperiaatteet:

...Muodostumisen periaatteet yksinkertaisimmillaan ovat sitä, että minä arvioin vuosittain tietoturvaperiaatteet ja arvioin, että tarviiko tehdä muutoksia. Jos siinä on tämmöisiä pieniä muutoksia esimerkiksi organisaatio on muuttunut ja vastuut on muuttunut, termistön muutokset niin tämmöisethän päivitetään aina... mut sit käytännössä se iso päivitys ruljanssi eli et "nyt olisi syytä katsoa tietoturvaperiaatteet aivan uudelta kantilta" niin se on mun päätös. Eli ja... oikeastaan se... sanotaan et kukaan ei tähän mennessä ole tullut sanomaan et pitäisikö tietoturvaperiaatteet päivittää.

Organisaatiossa D on tarkoitus päivittää tietoturvaperiaatteet. Sinällään ei koeta, että tietoturvaperiaatteiden sisältö muuttuisi, mutta tarkoituksena on päivittää ne organisaation nykymuodon ja strategian näköisiksi. Organisaatiossa D riskien arvioinnin tulokset eivät vaikuta tietoturvapolitiikan muodostumiseen. Tietoturvaperiaatteita ei koeta ongelmallisiksi eikä organisaatiossa uskota,

että tietoturvaperiaatteita muokkaamalla vaikutettaisiin hirveästi organisaation toimintaan.

Organisaatiossa E koettiin, että suurin virhe olisi laittaa riskien arvioinnin tulokset "hyllyyn", jolloin ne eivät vaikuttaisi millään tavalla tietoturvapolitiikan laadinnassa. Muutoksiin reagoidaan tarvittaessa:

> ...Kyllä tietysti jos tota noin jos sanotaan niin riskiarvioinnin tulokset lähtee muuttumaan radikaalisti niin kyllähän sitten on myöskin pakko käydä katsomassa et onks meidän niinku politiikat kunnossa, eli ollaanko me joko avattu liikaa tai ollaanko me suljettu liikaa.

Organisaatiossa F vastaukset olivat organisaatio E:n kaltaisia:

> ...Vaikuttaa paljon, se tota, riskiperusteinen... me teemme riskienhallintaa ja jos me toteamme siellä, että nyt tulee merkittäviä havaintoja niin kyl meidän pitää pystyä se viestimään ja siel on ylätasolla tietoturvapolitiikka on aina.

Haastatteluissa kartoitettiin myös organisaatioiden parhaiksi koettuja käytänteitä liittyen riskien arviointiin ja tietoturvapolitiikan muodostamiseen. Edellä mainitun avulla pyrittiin saamaan organisaatioiden käytännön kokemuksia tukemaan tutkimuksessa muodostettavaa riskien arvioinnin mallia. Taulukko 9 kuvaa poimintoja organisaatioiden parhaista käytänteistä liittyen riskien arviointiin ja tietoturvapolitiikan muodostumiseen. Taulukon 9 parhaat käytänteet ovat organisaatioiden omia näkemyksiä eivät tutkijoiden päätelmiä kerätystä materiaalista.

Taulukko 9 Riskien arvioinnin ja tietoturvapolitiikan muodostamisen parhaat käytänteet

Organisaatio	Parhaat käytänteet
A	Turvallisuushenkilö johtoryhmän jäsenenä, johdon sitoutuminen turvallisuustoimintaan, päivittäisen yhteistyön toimivuus
B	Työpajat, riskeihin liittyvissä toimenpiteissä riittävä keskustelu asianomaisen tahon kanssa.
C	Pyrkimys rakentaa ICT-ympäristö siihen suuntaan, että käyttäjillä olisi mahdollisimman vähän mahdollisuuksia toimia väärin. Pyrkimys tuoda asioita esiin mahdollisimman joustavasti ja dynaamisesti → pyrkimys pois "staattisesta" riskien arvioinnista.
D	Asiantuntijaryhmien käyttö riskejä arvioitaessa.
E	Avoimuus riskien esille tuomiseen, arvioinnin pohjamateriaalin laatu, työpajojen toteuttaminen.
F	Riski-ideoiden kerääminen organisaatiosta, riskien arvioinnin suunnitelmallisuus ja "markkinointi" henkilöstölle

Kaikissa tutkimukseen osallistuneissa organisaatioissa oli tunnistettu hyviä riskien arviointiin ja / tai tietoturvapolitiikan laatimiseen liittyviä käytänteitä. Monessa organisaatiossa toistui näkemys siitä, että riittävän hyvin suunnitellut, johdetut ja toteutetut henkilöstöä osallistavat työpajat tarjoavat arvokasta tietoa riskien arviointiin liittyen. Onnistuneen työpajatyöskentelyn edellytyksenä pidettiin sitä, että työpajoissa käytettävä pohjamateriaali on riittävän korkeatasoista ja että työpajojen vetäjät omaavat riittävän ammattitaidon.

6 TUTKIMUSTULOKSET

Tässä luvussa kuvataan riskien arvioinnin mallin muodostuminen ja tutkimuksen tulosten vaikutus riskien arvioinnin prosessimallin muodostamisessa. Tutkimuksen lopputuloksena muodostunut Heräte -malli esitellään myöhemmin alaluvussa 6.3, joten tämän luvun tarkoitus on kuvata mallin muodostumista teemojen tarkastelun kautta.

6.1 Mallin muodostaminen

Mallin muodostamisessa käytettiin apuna jo olemassa olevia tieteellisiä artikkeleita, kirjallisuutta, tutkimusraportteja, standardeja sekä ensimmäisen vaiheen haastatteluja, jotka tehtiin huhtikuussa 2016 suomalaisissa finanssialan organisaatioissa. Muodostettu malli on näin ollen synteesi tutkimustiedosta ja käytännöstä. Mallissa käytettiin apuna tutkimuksen aikana muodostettuja teemoja, joiden kautta organisaation strategiaa jalostetaan edelleen konkreettisiksi toimenpiteiksi. Perusteet teemojen taustalla on kuvattu ensimmäisen vaiheen haastattelujen yhteydessä.

Tavoitteemme oli luoda holistinen malli, joka luo riskien arvioinnille uutta arvoa organisaation menestystekijänä. Holismilla tarkoitetaan, että jonkin kokonaisuuden ominaisuudet ovat enemmän kuin sen osien ominaisuuksien summa (Oxford Dictionaries, 2016d). Tutkimuksessa tehtyjen haastattelujen perusteella riskien arvioinnin pohjana olevan tiedon tulee olla kerätty laajasti organisaation eri tasoilta, mutta tämän lisäksi myös yli organisaation rajojen ympäröivästä maailmasta. Kerätty tieto analysoidaan, jolloin oppimisen ja ymmärryksen pohjaksi saadaan enemmän kuin tiedot yksittäin pystyvät tuottamaan.

Mannermaan (1991) ja alun perin Roy Amaran (1981) kolmen perusperiaatteen mukaan:

1. Tulevaisuus ei ole ennakoitavissa.
2. Tulevaisuus ei ole ennalta määrätty.
3. Tulevaisuuteen voidaan vaikuttaa valinnoilla.

Mannermaan (1991) ja Amaran (1981) ajattelusta on tehtyjen haastattelujen perusteella mahdollista ottaa oppia myös organisaation riskien arvioinnin osalta. Vaikka tulevaisuutta ei voi ennustaa on kuitenkin huomioitava se, että tulevaisuus ei ole ennalta määrätty. Organisaatioiden on mahdollista omilla valinnoillaan vaikuttaa tapahtumien kulkuun niin positiivisessa kuin negatiivisessa mielessä. Oleellista on huomata, että toimintaympäristössä on varmasti muita toimijoita ja nämä toimijat pyrkivät vaikuttamaan tulevaisuuden tapahtumiin. Tulevaisuuden tapahtumien ja mahdollisten tapahtumakulkujen arvioimiseksi organisaatioiden tulee kerätä aktiivisesti ympäröivästä maailmasta dataa ja käsiteltyä tietoa. Kerätyn materiaalin perusteella tapahtumien arvioiminen muuttuu arvaamisesta vähitellen kohti tarkempia arvioita. Tulevaisuus ei ole ennakoitavissa, mutta tapahtumakulkuja arvioimalla ja vertaamalla kerättyä tietoa aiempiin tapahtumiin arvioinnin tarkkuus paranee.
Mallin muodostamisessa käytimme ohjaavina tekijöinä tutkimuksen aikana muodostettuja teemoja 1-4, jotka ovat:

Teema 1: Riskien arviointi organisaation strategian toteuttamisen välineenä
Teema 2: Riskien arvioinnin prosessi
Teema 3: Riskien arvioinnin perusteena käytettävä tieto
Teema 4: Riskien arvioinnin tulosten vaikutus tietoturvapolitiikan laadinnassa

Teema 4:n osalta tietoturvapolitiikan sijassa voisi olla myös jokin muu organisaation lopputuote, johon riskien arvioinnin tulokset vaikuttavat. Tämän vuoksi teema 4 on jatkossa kehyksenä toimenpiteille otsikolla "**riskien arvioinnin tulosten vaikutus organisaation toimintaan**". Jatkossa teemat ovat:

Teema 1: Riskien arviointi organisaation strategian toteuttamisen välineenä
Teema 2: Riskien arvioinnin prosessi
Teema 3: Riskien arvioinnin perusteena käytettävä tieto
Teema 4: Riskien arvioinnin tulosten vaikutus organisaation toimintaan

Teemoilla 1-4 on kaikilla oma tarkoituksensa pyrittäessä ketteröittämään uutta mallia. Yleinen huomio haastatteluissa oli nykyisten riskien arvioinnin menetelmien hankala käytettävyys ja toisaalta riskien arvioinnin näkeminen perusteettomana menetelmänä. Tutkimustulosten ja aikaisemman teorian perusteella mallista ja riskien arvioinnin prosessista tulee tehdä koko organisaation yhteinen ja organisaation arvoja tukeva työkalu.

Teema 1 - Riskien arviointi organisaation strategian toteuttamisen välineenä:
Organisaation toimintaa ohjaa strategia, jota varsinkin yksityisen sektorin yri-

tyksissä kutsutaan liiketoimintastrategiaksi. Tässä tutkimuksessa käytämme käsitettä "strategia", jotta haastatteluun osallistuneet julkisen sektorin toimijat käsitellään saman käsitteen alla. Koska organisaatiolla on yksi strategia, tulee organisaation riskien arvioinnin tapahtua yhdenmukaisella ja vertailukelpoisella tavalla. Varsinkin projektien osalta on tehtyjen haastattelujen perusteella koettu ongelmalliseksi havaittujen riskien tuominen osaksi organisaation laajempaa riskien arviointia. Projekteissa havaitut riskit eivät haastattelujen perusteella usein siirry organisaation riskien arviointiin, vaan ne jäävät projektiin. Organisaation johdon kannalta on ongelmallista, mikäli tuotetut riskien arvioinnin tulokset eivät ole vertailukelpoisia ensinnäkin organisaation eri toimintojen välillä, mutta toisaalta verrattaessa kuluvaan aikaan. Jos periaatteet riskien arvioinnin suorittamisessa ja mittaamisessa muuttuvat vuosittain, riskien arvioinnin taustalla kerääntyvä aineisto ei ole vertailukelpoista.

Laadittu malli on riskien arvioinnin malli, mutta on paikallaan lainata Mikko Hyppösen (2016) sanoja tietoturvasta: "Ei pidä unohtaa sitä, että monimutkaisuus on tietoturvan vihollinen. Koitetaan siis pyrkiä tekemään mahdollisimman yksinkertaisia ja turvallisia järjestelmiä". Tämä pätee muuhunkin kuin ainoastaan tietoturvaan. Organisaation, ja laajemmin koko yhteiskunnan jäsenten tulee ymmärtää roolinsa ja tekemiensä asioiden seuraukset. Laadittavan mallin tulee näin ollen olla omaksuttavissa kaikilla organisaation tasoilla, jotta kaikilla organisaation toimintaan osallistuvilla henkilöillä on yhteinen näkemys riskien arvioinnin tavoitteesta. Turvallisuus ja jatkuvuus tulevat mallissa esille kaikille yhteisen viitekehyksen kautta. Organisaation eri tasoilla tulee olla tarkempia menetelmiä riskien arvioinnin toteuttamiseksi, mutta viitekehyksen on pysyttävä muuttumattomana. Viitekehyksen tulee näin ollen soveltua niin strategiselle, operatiiviselle kuin teknis-taktisille tasoille.

Organisaatioissa ei ole olemassa soveltuvia välineitä henkilöstöltä saatavan tiedon keräämiseen ja käsittelyyn. Henkilöstö tuottaa tällä hetkellä hyvin vähän tietoa organisaation riskien arvioinnin perustaksi. Riskien arviointi tehdään asiantuntijatasolla, jolloin analysoitu tieto ei siirry organisaatioissa varsinkaan henkilöstölle. Organisaatioiden henkilöstö muodostaa kuitenkin valtaosan organisaatioiden käytettävissä olevasta tietopääomasta jo ainoastaan henkilömäärän perusteella arvioituna.

Teema 2 - Riskien arvioinnin prosessi: Teemassa 1: Riskien arviointi organisaation strategian toteuttamisen välineenä sivuttiin osittain organisaation riskien arvioinnin prosessin yhdenmukaisuutta itse prosessina sekä tuotetun riskitiedon osalta. Riskien arvioinnin prosessin tulee yhdenmukaisuuden lisäksi olla yksinkertainen, eli helppo toteuttaa. Yksinkertaisuus riskien arvioinnin prosessissa tarkoittaa sitä, että se voidaan toteuttaa vähäisellä koulutuksella niin, että riskien arvioinnin suorittaja pystyy tuottamaan yhdenmukaista tietoa muun organisaation kanssa. Riskien arviointi on aina arvio, johon liittyy epävarmuustekijöitä. Oleellista on kuitenkin tuotettava yhdenmukainen riskitieto, jota voidaan jälkikäteen arvioida.

Riskien arvioinnissa käytetään nykyisin asiantuntijoita, joiden siirtyminen toisiin tehtäviin tai muu poissaolo aiheuttavat prosessin laadun heikentymisen. Haastatteluissa nähtiin hyväksi vaihtaa arvioinnin suorittajia toisinaan, ettei

riskien arvioinnista ei tulisi rutiinia. Osassa organisaatioista käytettiin apuna myös ulkopuolisia asiantuntijoita, mutta ei niinkään suorittamassa itse riskien arviointi prosessia, vaan esimerkiksi haastamaan nykyisiä näkemyksiä ja tuomaan uutta tietoa riskien arviointi prosessin tueksi.

Riskien arvioinnin prosessin tulee olla ketterä. Ketteryydellä tarkoitetaan sitä, että riskien arvioinnin vaiheet voivat mennä osittain päällekkäin ja niihin voidaan palata prosessin edetessä. Organisaatioissa, joissa oli vielä käytössä vaiheittain etenevä riskien arviointiprosessi, pohdittiin tulevaisuutta ja muuttuvaa toimintaympäristöä ajatellen siirtyä aktiivisempaan ja ketterämpään riskien arviointimalliin. Organisaatioissa oli käytössä edelleen riskien arvioinnin prosesseja, joissa riskit arvioitiin joko kvartaaleittain, puolivuosittain tai vuosittain. Jatkuva toimintaympäristön muutoksiin reagoiva ja trendejä tunnistava riskien arviointi nähtiin kuitenkin tulevaisuuden mallina.

Teema 3 - Riskien arvioinnin perusteena käytettävä tieto: Tietoa riskien arviointiin kerättiin varsin laajasti. Organisaatiot keräävät tietoa niin oman organisaation sisäisistä lähteistä, kuin ulkopuolisistakin lähteistä. Tiedon keräämisen osalta tulee tunnistaa organisaation kannalta merkittävät tiedon lähteet ja pyrkiä oma-aloitteisesti jäseneksi muun muassa erilaisiin asiantuntijaryhmiin. Toimiala ja käytettävissä olevat resurssit vaikuttavat olennaisena pidettävän tiedon keräämiseen, mutta yhdessäkään organisaatiossa ei todettu, että tietoa tulee liikaa. Riskien arvioinnin perusteena olevan keskeisimmän tiedon tunnistaminen ennalta on hyvin hankalaa, jolloin tietoa pyritään keräämään kaikista mahdollisista keskeisinä pidetyistä lähteistä.

Haastatteluissa käytettiin toistuvasti käsitettä “kehitysaste” liittyen organisaation tiedon keräämiseen liittyen. Tässä vaiheessa on todettava, että haastattelut tehtiin organisaatioissa, joiden oletetaan jo toimintaympäristön ja regulaation kautta tekevän riskien arviointia keskimääräistä yritystä tai organisaatiota haastavammassa ympäristössä. Varhaisessa kehitysvaiheessa olevat organisaatiot keräävät tietoa Microsoft Excel -pohjaisilla taulukkotyökaluilla, joihin on etukäteen kerätty aiheittain mahdollisia riskitekijöitä. Työkalut tuottavat annetun pisteytyksen, tavanomaisesti asteikolla 1-5, perusteella tietoa organisaation riskeistä. Kyseinen malli koettiin osittain hankalaksi käyttää ja pisteyttämällä tehtävän arvioinnin luotettavuutta arvosteltiin. Toisaalta todettiin, että tällä hetkellä ei ole olemassa parempaa työkalua, vaikka aikomus riskien arvioinnin työkalun kehittämiseen on olemassa. Taulukko-ohjelmapohjaisten arviointityökalujen koettiin ohjaavan riskien arviointia niin, että oletusarvoisesti annettujen riskitekijöiden ulkopuolelta ei riskien arvioinnissa mainita muita riskejä. Kehittyneissä organisaatioissa koettiin, että Excel -pohjaiset arviointityökalut eivät ole enää tätä päivää. Excel -työkalujen koettiin ajavan asiansa varhaisessa vaiheessa olevissa yrityksissä, joissa riskien arviointia ja riskitiedon keräämistä vasta harjoitellaan. Riskitietojen ilmoittaminen koettiin osittain ongelmalliseksi, koska riskitiedon ilmoittanut saattaa joutua keksimään ratkaisun ilmoittamaansa riskiin.

Teema 4 - Riskien arvioinnin tulosten vaikutus organisaation toimintaan: Haastatteluissa tuotiin esille, että ainoastaan lopputuloksella on merkitystä.

Näin ollen kaiken toiminnan tulee perustua organisaation strategiaan. Haastatteluissa organisaation strategian siirtäminen käytännön toimintaan kuvattiin tietoturvapolitiikan muodostumisen kautta. Aiemman teoreettisen tutkimuksen mukaan riskien arvioinnin tulosten tulisi vaikuttaa tietoturvapolitiikan muodostumiseen. (mm. Knapp, 2009). Haastattelujen perusteella yhteys riskien arvioinnin ja tietoturvapolitiikan välillä on osassa organisaatioista hyvin löyhää tai yhteyttä ei ole ollenkaan. Organisaatioissa, joissa riskien arvioinnin menetelmiä oli kehitetty pitkälle, oli rakennettu tietoisesti yhteyttä riskien arvioinnin ja muun toiminnan välille.

Kaikissa yrityksissä ymmärrettiin, että turvallisuuspolitiikat rakentuvat organisaation ominaisuuksien mukaan, mutta osa organisaatioista loi omat politiikkansa muiden organisaatioiden malleja kopioiden sekä kaupallisista tai avoimista lähteistä saatavilla olevien mallien perusteella, kuten Höne ja Eloff (2002a) kuvaavat tutkimuksessaan. Mallien lainaaminen johtuu usein puutteellisista taidoista. Hönen ja Eloffin (2002a) mukaan leikkaa ja liitä -mallilla (cut & paste) rakennetut politiikat kuvaavat harvoin organisaation kulttuuria ja eivät johda todelliseen tehokkaaseen ohjeistukseen.

6.2 Toisen vaiheen haastattelut: mallin validointi

Tässä luvussa kuvataan ensin yleisellä tasolla toisen haastattelukierroksen kulkua sekä haastatteluiden tuloksia. Luvussa kuvataan myös asiantuntijoiden kommentteja mallin käytettävyydestä ja mahdollisuuksista. Luvun keskeisin teema kiteytyy kysymykseen siitä, olisivatko asiantuntijat valmiita ottamaan käyttöön muodostetun mallin joko omassa organisaatiossaan tai mahdollisessa kuvitteellisessa organisaatiossa.

6.2.1 Asiantuntijahaastattelut

Tutkimuksen toinen haastattelukierros toteutettiin toukokuussa 2016 aikataulun mukaisesti. Asiantuntijahaastatteluiden aikana kertynyt materiaali tallennettiin suunnitelman mukaisesti, jonka jälkeen materiaali analysoitiin haastattelu kerrallaan. Aineiston analysointi on kuvattu menetelmäluvussa 5.5. Haastatteluja käsiteltiin yksitellen ja kaikkien asiantuntijoiden kommentteihin otettiin kantaa.

Tutkimuksen toisen vaiheen asiantuntijahaastatteluiden haastateltavien henkilöiden rekrytointiin käytetty saatekirje on kuvattu liitteessä 2. Haastattelut toteutettiin keskustelemalla muodostetusta riskien arvioinnin mallista. Haastatteluiden runkona käytetyt teemat on kuvattu liitteessä 5. Liitteessä 3 on kirje, jolla asiantuntijoita muistutettiin meneillään olevasta tutkimuksesta ja sen aiheesta.

Ensimmäisen asiantuntijahaastattelun haastateltavana toimi **Kimmo Rousku**. Rousku kuvasi ensimmäiseksi omia havaintojaan riskienhallinnasta yleisemmällä tasolla viitaten kuitenkin myös tutkimuksessa muodostettuun

malliin. Riskienhallinta on Rouskun mukaan yllättävän vanha tieteenala, jonka heikkoutena on se, että riskienhallinta ei ole toisaalta myöskään kehittynyt merkittävästi. Esitelty malli tulee osaltaan auttamaan tässä ongelmassa. Riskienhallinnassa on puutteita päivittäisen toiminnan osalta ja hänen mukaansa riskienhallinta koetaan liian erillisenä prosessina. Riskienhallinta keskittyy nykyisin yleensä strategiselle tasolle ja johdon näkemykseen tai projektien ja hankkeiden yhteydessä tehtävään riskienhallintaan. Riskienhallinta on Rouskun mukaan pahimmillaan liian määrämuotoista ja määräajoin tapahtuvaa toimintaa. Riskienhallinta tulisi Rouskun mukaan nähdä koko ajan toimintaan liittyvänä aktiviteettina. Rousku nosti esille mallin "herätteen" käsitteen ja antoi tälle positiivista palautetta kuvaavasta määritelmästä. Riskienhallinta tulisi nähdä ennen kaikkea apuna mahdollisuuksien tunnistamisessa ja menestymisen turvaamisessa, koska Rouskun mukaan "pelolla on hankala myydä".

Rousku ehdotti malliin strategian, uhan ja riskin määritelmien kuvaamista, koska kyseiset määritelmät eroavat lähteestä riippuen. Rousku nosti esille myös mallissa kuvattujen trendien tunnistamisen, kilpailukyvyn, ketteryyden ja dynaamisuuden tärkeyden. Rousku ehdotti, että mallissa korostettaisiin digitalisaation merkitystä. Digitalisaatio tuo Rouskun mukaan mahdollisuuksia muun muassa uhista ja riskeistä ilmoittamiseen. Rousku myös ehdotti koko prosessin vastuutahon muuttamista prosessin omistajaksi. Riskien arvioinnin tulosten esittäminen on Rouskun mukaan kokonaisuudessaan haastavaa. Rouskun mukaan todennäköisyyksien esittämiseksi tulisi esittää tarkentavia kysymyksiä. Haastattelun aikana keskusteltiin riskien arvioinnin perusteella tehtyjen toimenpiteiden toteutumisen valvonnasta, mutta päädyttiin siihen, että valvonta ei sinällään kuulu riskien arviointi prosessiin vaan laajempaan riskienhallinnan kokonaisprosessiin. Rouskun mukaan mallissa korostuva menestyminen on tärkeää ja Rousku ehdotti, että mallissa korostetaan myös organisaation luottamuksen kasvattamista enemmän.

Rouskun mukaan on positiivista, että mallista ei ole lähdetty tekemään liian konkreettista. Kysyttäessä Kimmo Rouskulta olisiko hän valmis ottamaan mallin käyttöön omassa tai kuvitellussa organisaatiossa Rousku kommentoi seuraavasti:

> Sanotaan et kyllä, nimenomaan se et kyllä mä niinku tästä tiettyjä pointteja me tähän tota VAHTI-kokonaisuuteen varmaan otetaan niinku hyödyksi ja avuksi että tässä oli tiettyjä asioita ja varsinkin sit kattoo vielä sen gradun että mitä muuta sieltä niinku löytyy, niin uskoisin, että hyödyttää. Nimenomaan tää heräte-idea mallina ja tää on tavallaan niinku siinä välillä ketterä moduuli joka voi olla niinku hyvinkin monella tavalla tehty ja toteutettu ja se johtaa kuitenkin siitä niinku käytännön toimintaan, on ihan hyvä niinku mallina, niinku uudenlaisena mallina ja ideana.

Rouskun mukaan malli antaa muutamia hyviä ideoita VAHTI-ohjeen kehittämiseen ja hänen mukaansa malli antaa hyvää suuntaa, mutta lisäksi tarvetta olisi yksityiskohtaisemman menetelmän kehittämiselle. Rousku kuvasi myös mallin mahdollistaman tilannekuvan muodostamisen tärkeyttä.

> Tästä saa tosiaan muutamia hyviä ideoita tohon kokonaisuuteen (VAHTI-ohjeen kehittämiseen), mut sitten se menetelmän kehittäminen….

> ...tää on juuri se, että… monet ei niinku ymmärrä sitä, kuvittelee et tää on tosiaan niinku neljä kertaa vuodessa ja vain sillon mutku me tarvitaaan juuri nimenomaan yhä enemmän tämmösiä niinkun ad-hoc -tyyppisesti tilanteita joissa pitää muodostaa tilannekuva ja arvioida ne riskit niin sitä kykyä pitäis pystyä enemmän tuomaan esille ja mahdollistamaan.

Rousku korosti vielä lopuksi mallin hyödynnettävyyttä toteamalla, että mallin sisältöä tullaan hyödyntämään meneillään olevassa VAHTI-työryhmän työssä.

Toisessa asiantuntijahaastattelussa haastateltiin **Mikko Siposta**. Mikko Siposen mukaan muodostetun mallin vaiheet ovat geneerisiä. Mallia voisi hänen mukaansa käyttää periaatteessa vaikka auton ostoon. Siposen mukaan mallin osalta olisi mielenkiintoista tietää, että mikä on oikeasti erikoista riskienhallinnassa verrattuna johonkin muuhun arviointiin tai analyysiin. Siponen vertasi muodostettua mallia kypsyysmalliin, jota esitetty malli ei Siposen mukaan kuitenkaan ole. Siposen mukaan:

> Geneerisyydestä johtuen… tyypillinen kritiikki lähtee siitä ja sopii myös tähän malliin... niin mitataan jonkun prosessin olemassaoloa ja eihän se tavallaan tarkoita sitä, että kun joku prosessi on tai ei oo…", vaan "mikä sen vaikutus siihen toiminnan laatuun oikeasti on… Mikä on se linkki… mikä evidenssi siihen niinkun on olemassa?

Siposen mukaan voi olla hankala näyttää, että evidenssiä on. Siponen esitti kysymyksen:

> Onks näillä vaiheilla… Onks se kysymys se et mitä näitten vaiheitten sisällä tehdään, tarkkoja toimenpiteitä, niin onks sillä laatuvaikutusta paljon enemmän kuin näillä vaiheilla.
>
> "Takaako tietyt vaiheet niinkun automaattisesti laatua vai tuleeko se laatu ihan jostain muusta asiasta. Tällaista vois niinkun, toki jos malli olis tarkempi…"

Siponen kuvaili riskien arviointia yleisellä tasolla ja mainitsi esimerkiksi Baskervillen (1991) artikkelin. Siponen pohti, että mihin riskien arviointi perustuu ja kyseenalaisti riskien arvioinnin kelpoisuuden, koska riskien euromääräiset arvot vaikuttavat hänen aiemmissa tutkimuksissaan olleen "vedetty ihan hatusta". Siponen pohti myös riskien arvioinnin merkitystä:

> Onko sillä niin väliä miten sen riskien arvioinnin tekee jos se on kuitenkin arvausta? …se vaikka olisikin hienot menetelmät ja stepit niin onks sillä hirveesti väliä jos se on arvausta monessa kohtaa?

Siponen mietti myös sitä, että miten johto voi kyseenalaistaa asiantuntijan näkemyksen:

> Kun tää riskianalyysi perustuu subjektiivisuuteen ja voi olla, että riskianalyysin tekijällä on esittää myös joitain lukuja johdolle niin se johto voi kysyä sitä evidenssiä, mutta eihän niitä ole tavallaan, mutta ei niillä ole sitä substanssitietämystä, että ne pystyis kyseenalaistamaan.

Siponen mietti vastausta siihen, miten paljon asiantuntijat käyttävät riskianalyysiä uhkien esille tuomiseen:

> Kuinka paljon tätä… asiantuntijat käyttää sitä riskianalyysiä, et miksi just uhkia… onks se sen takia et halutaan sitä kautta tuoda niitä uhkia esiin, koska se on se asia miksi joku johto saadaan, saadaan uskotettua johdolle, että tässä on tämmöinen uhka.

Siposen mukaan riskien arviointi turvallisuuden ohjaustyökaluna on tutkimusaiheena mielenkiintoinen muun muassa siltä osin, että kuinka monessa yrityksessä riskien arviointia vääristellään tahallaan?

Siposelta kysyttiin haastattelun lopuksi olisiko hän valmis käyttämään esitettyä mallia omassa tai kuvitteellisessa organisaatiossa. Siponen kuvasi mallin löytyvän todennäköisesti 80 -luvun oppikirjoista erilaisten vaiheiden määrän ollessa joko muutama enemmän tai muutama vähemmän. Vaikka malli ei hänen mukaansa anna kovin konkreettista ohjetta, niin Siposen mukaan mallin käytölle ei ole estettä. Siposen mukaan vaiheissa ei ole sinällään mitään huomautettavaa ja vertaa muodostetun mallin vaiheita olemassa olevien standardien vaiheisiin, joissa ei niissäkään anneta kovin konkreettisia ohjeita.

Kolmannen asiantuntijahaastattelun kohteena oli **Jarno Limnéll**. Limnéllille kerrottiin mallista ja siihen vaikuttavista ilmiöistä yleisellä tasolla. Tämän jälkeen Limnéll kuvaili yleisesti riskien arviointia kolmen eri tason kautta, jotka ovat strateginen, operatiivinen ja teknis-taktinen. Limnéllin mukaan tänä päivänä digitalisaation turvaamisessa lähtökohta on teknis-taktisella tasolla, kun sen pitäisi olla strategisella tasolla. Limnéllin sanoo:

> Me lähdetään kattomaan tätä teknis-taktiselta tasolta ilman, että meillä on riittävää ymmärrystä, näkemystä ja sitoutumista täällä strategisella tasolla.

Limnéll otti tutkijat mukaan sparraukseen ja kysyi, mille tasolle tarkasteltava malli sijoittuu. Limnéllille kerrottiin, että mallin muodostamisessa on otettu huomioon tarpeet erityisesti strategisella tasolla, mutta malli soveltuu käytettäväksi myös muilla tasoilla ja sen tarkoituksena on olla monikäyttöinen.

Limnéll tiivistää tehdyn tutkimuksen ja kuvailee kulttuurin kehittymistä:

> Mä voisin tiivistää sen, että te haluatte muuttaa tämän digitaalisen maailman turvallisuuskulttuuria parempaan suuntaan. Oleellista siinä on se sana kulttuuri.
>
> Kulttuuri ei kehity tämän tason kautta (osoittaa teknis-taktisia tasoja taululta), vaan kulttuuri kehittyy tämän tason kautta (osoittaa strategian tasoa taululta).

Limnéll näki kaikkein tärkeimpänä asiana johdon sitoutumisen, koska sitoutuminen ja ohjaus tapahtuvat ylhäältä alaspäin (top-down) Haastattelun aikana käytiin keskustelua fyysisen ja digitaalisen turvallisuuden ympäristöistä. Limnéll korosti fyysisen turvallisuusympäristön olemassaolon muistamista. Limnéll pohti fyysisen ja digitaalisen turvallisuuden olevan tulevaisuudessa siinä määrin yhtä, että turvallisuuden eri osa-alueet ymmärretään yhdeksi isoksi kokonaisuudeksi. Fyysisen ympäristön kautta on usein helpompi saada vai-

kutusta myös digitaaliseen ympäristöön. Keskeinen asia on koko kompleksisen turvallisuusympäristön ymmärtäminen. Limnéll kuvasi niin sanottua turvallisuuden uutta paradigmaa: yhä kiihtyvää muutosnopeutta, ennalta-arvaamatonta epävakautta uutena normaalitilana sekä digitaalisen ja fyysisen maailman yhdentymistä kompleksisena kokonaisuutena. Limnéll korosti mainittujen asioiden esille nostamista esitellyssä mallissa.

Limnéll kuvasi kyberturvallisuutta piirtämänsä nelikentän kautta. Nelikentän osat ovat ennaltaehkäiseminen, torjunta, havaitseminen ja toipuminen. Nelikentän osat muodostavat jatkuvan prosessin. Kyber keskittyy Limnéllin mukaan nykyisin melko paljon torjuntaan, mutta alan painopiste on muuttumassa kohti havaitsemista.

Turvallisuus tulee Limnéllin mukaan nähdä aina lähtökohtaisesti mahdollistajana:

> Näin pitää myös tietoturvajohtajien ja turvallisuusjohtajien se myöskin niinku firman johdolle markkinoida, että hei tää mahdollistaa, että (yritykseen) luotetaan, kun meillä on turvallisuusasiat kunnossa. Kun me huolehditaan niin tää mahdollistaa et me ollaan hyviä.

Limnéll nosti lopuksi esille turvallisuuskulttuurin muuttamisen riskien arvioinnin näkökulmasta. Viime kädessä kyse on kuitenkin kulttuurin muuttamisesta. Limnéllin lainasi haastattelun aikana amerikkalaista kollegaansa toteamalla, että "kyberturvallisuus on joukkuepeliä".

Limnélliltä kysyttiin myös suoraa palautetta esitellystä mallista. Limnéllin mukaan malli on kuvan perusteella jossain määrin "hämärä". Elementit ovat kuitenkin periaatteessa samoja kuin hänen edustamansa organisaation (INSTA) työn alla olevassa turvallisuuspolitiikassa. Limnéll pitää jatkuvan prosessin kuvista ja hänen mukaansa tämän mallin kuva aukeaa vähän hankalasti.

Limnéllin kanssa käytiin lopuksi keskustelua aktiivisen tiedonhankinnan menetelmästä, joka perustuu hänelle esitettyyn malliin. Limnéllin mukaan esitelty aktiivisen tiedonhankinnan menetelmä on konkreettinen väline, joita tulevaisuudessa tullaan tarvitsemaan. Tältä osin malli soveltuu menetelmän pohjaksi.

6.2.2 Yhteenveto asiantuntijahaastatteluista

Haastateltujen asiantuntijoiden kommenteista on koottu edellä keskeisimmät esille nousseet asiat. Tässä kappaleessa keskeisimmät asiat kootaan synteesiksi, jonka perusteella on mahdollista tehdä muutoksia aikaisemmin muodostettuun malliin. Tässä kappaleessa esitellään sekä mallin hyvät puolet, että kehitysehdotukset. Asiantuntijoiden kehitysehdotuksiin otetaan molemmissa tapauksissa kantaa.

Muodostettu malli on laadittu organisaatioiden toiminnan kannalta oikealle tasolle. Mallin on laadittu niin, että se vaikuttaa ensisijaisesti organisaatioiden strategiselle tasolle. Riskien arviointi on organisaation kaikkien tasojen läpi kulkeva jatkuva prosessi, johon koko organisaation henkilöstö on saatava mukaan. Malli on laadittu riittävän yleisellä tasolla, mutta kuitenkin niin, että se

antaa ohjauksen organisaation riskien arvioinnin viitekehyksenä. Mallin kautta on mahdollista tehdä niin strategisen, operatiivisen kuin teknis-taktisen tason riskien arviointia ja muodostaa formaalia tietoa oppimisen ja ymmärryksen kasvattamiseksi.

Riskienhallinta ei ole nykyisellään kehittynyt toimintaympäristön muutosten edellyttämällä tavalla. Riskienhallintaa kuitenkin tehdään erilaisilla menetelmillä, jotka eivät välttämättä perustu tietoon ja kerättyyn dataan. Siponen kuvasi riskien arviointia jopa arvaukseksi ja näin ollen kyseenalaisti riskien arvioinnin perusteet. Siposen mukaan riskien euromääräiset arvot vaikuttaa hänen aiemmissa tutkimuksissaan olleen "vedetty ihan hatusta". Riskien arvioinnin tulosten esittäminen on Rouskun mukaan kokonaisuudessaan haastavaa. Rouskun mukaan todennäköisyyksien esittämiseksi tulisi esittää tarkentavia kysymyksiä.

Kaikki haastatellut asiantuntijat näkivät muodostetun mallin geneeriseksi, yleisen tason, malliksi, josta puuttuvat konkreettiset ja tarkemmat toimenpiteet. Siponen ja Limnéll toivoivat konkreettisia menetelmiä riskien arvioinnin toteuttamiseen, mutta ymmärsivät myös esimerkiksi standardien epätarkkuuden. On tärkeää huomata, että organisaatiot laativat riskien arviointia oman toimintansa lähtökohdista muokaten menetelmiä itselleen sopiviksi.

Rouskun ja Siposen mukaan mallin (kuvio 13) avulla on mahdollista tehdä hyvin laajasti erilaisia riskien arviointeja, mutta myös muita arvioita. Limnéll kuvaa mallia (kuvio 13) jossain määrin hämäräksi, koska pitää itse enemmän jatkuvan prosessin malleista, kuten Suomen kyberturvallisuusstrategian prosessimallista.

Riskien arvioinnin prosessin laatuvaikutusta pohdittiin muun muassa Mikko Siposen haastattelussa. Siponen esitti kysymyksen:

> Onks näillä vaiheilla… onks se kysymys se et mitä näitten vaiheitten sisällä sisällä tehdään, tarkkoja toimenpiteitä, niin onks sillä laatuvaikutusta paljon enemmän kuin näillä vaiheilla.
>
> …takaako tietyt vaiheet niinkun automaattisesti laatua vai tuleeko se laatu ihan jostain muusta asiasta. Tällaista vois niinkun, toki jos malli olis tarkempi….

Rousku nosti esille mallin "herätteen" käsitteen ja antoi tälle positiivista palautetta kuvaavasta määritelmästä. Riskienhallinta tulisi nähdä ennen kaikkea apuna mahdollisuuksien tunnistamisessa ja menestymisen turvaamisessa, koska Rouskun mukaan "pelolla on hankala myydä". Siponen kuvasi esitetyn mallin löytyvän todennäköisesti 80 -luvun oppikirjoista erilaisten vaiheiden määrän ollessa joko muutama enemmän tai muutama vähemmän.

Rouskun mukaan esitelty malli tulee osaltaan auttamaan riskien arvioinnin kehittymiseen liittyvissä ongelmissa. Riskienhallinnassa on puutteita päivittäisen toiminnan osalta ja että riskienhallinta koetaan liian erillisenä prosessina. Riskienhallinta keskittyy nykyisin yleensä strategiselle tasolle ja johdon näkemykseen tai projektien ja hankkeiden yhteydessä tehtävään riskienhallintaan. Malli mahdollistaa riskien arvioinnin kaikilla organisaation tasoilla. Riskienhallinta on Rouskun mukaan pahimmillaan liian määrämuotoista ja määräajoin

tapahtuvaa toimintaa. Riskienhallinta tulisi kuitenkin nähdä mallin mukaisesti koko ajan toimintaan liittyvänä aktiviteettina.

Rousku nosti esille organisaation menestyksen kuvaamisen tärkeyden ja ehdottaa, että mallissa korostetaan lisäksi organisaation luottamuksen kasvattamista enemmän. Rousku ehdotti malliin tiettyjen käsitteiden tarkempaa kuvaamista, koska kyseiset määritelmät eroavat lähteestä riippuen. Rousku nosti esille myös mallissa kuvattujen trendien tunnistamisen, kilpailukyvyn, ketteryyden ja dynaamisuuden tärkeyden. Rousku ehdotti, että mallissa korostetaan digitalisaation merkitystä. Digitalisaatio tuo Rouskun mukaan mahdollisuuksia muun muassa uhista ja riskeistä ilmoittamiseen.

Siposen mukaan mallin osalta on mielenkiintoista, että mikä on oikeasti erikoista riskienhallinnassa verrattuna johonkin muuhun arviointiin tai analyysiin? Siponen vertasi muodostettua mallia kypsyysmalliin, jota esitetty malli ei Siposen mukaan kuitenkaan ole. Siposen mukaan:

> Geneerisyydestä johtuen… Tyypillinen kritiikki lähtee siitä ja sopii myös tähän malliin... Niin mitataan jonkun prosessin olemassaoloa ja eihän se tavallaan tarkoita sitä, että kun joku prosessi on tai ei oo, vaan mikä sen vaikutus siihen toiminnan laatuun oikeasti on.

> Mikä on se linkki… Mikä evidenssi siihen niinkun on olemassa?

Siposen mukaan voi olla hankala näyttää, että evidenssiä on.

Siponen pohti myös riskien arvioinnin merkitystä, eli sitä onko arvioinnin tekotavalla lopulta merkitystä, jos se perustuu arvaukseen? Rousku ehdotti vastuunjakotaulukon osalta koko prosessin vastuutahon muuttamista prosessin omistajaksi.

6.2.3 Muodostettu malli organisaatioiden riskien arvioinnin viitekehyksenä

Kysyttäessä asiantuntijoilta mallin potentiaalia organisaatioiden riskien arvioinnin viitekehyksenä, olivat kommentit myönteisiä. Rouskun mukaan on positiivista, että mallista ei ole lähdetty tekemään liian konkreettista:

> “Sanotaan et kyllä, nimenomaan se et kyllä mä niinku tästä tiettyjä pointteja me tähän tota VAHTI-kokonaisuuteen varmaan otetaan niinku hyödyksi ja avuksi että tässä oli tiettyjä asioita ja varsinkin sit kattoo vielä sen gradun että mitä muuta sieltä niinku löytyy, niin uskoisin, että hyödyttää. Nimenomaan tää heräte-idea mallina ja tää on tavallaan niinku siinä välillä ketterä moduuli joka voi olla niinku hyvinkin monella tavalla tehty ja toteutettu ja se johtaa kuitenkin siitä niinku käytännön toimintaan, on ihan hyvä niinku mallina, niinku uudenlaisena mallina ja ideana”.

Rouskun mukaan malli antaa muutamia hyviä ideoita VAHTI-ohjeen kehittämiseen:

> Tästä saa tosiaan muutamia hyviä ideoita tohon kokonaisuuteen (VAHTI-ohjeen kehittämiseen), mut sitten se menetelmän kehittäminen…

Rouskun mukaan malli antaa hyvää suuntaa, mutta olemassa on tarve yksityiskohtaisemman menetelmän kehittämiselle. Rousku kuvasi myös tilannekuvan tärkeyttä, jonka malli mahdollistaa:

> ”...tää on juuri se, että… monet ei niinku ymmärrä sitä, kuvittelee et tää on tosiaan niinku neljä kertaa vuodessa ja vain sillon mutku me tarvitaaan juuri nimenomaan yhä enemmän tämmösiä niinkun ad-hoc -tyyppisesti tilanteita joissa pitää muodostaa tilannekuva ja arvioida ne riskit niin sitä kykyä pitäis pystyä enemmän tuomaan esille ja mahdollistamaan”.

Rousku korostaa vielä erikseen lopuksi mallin hyödynnettävyyttä toteamalla, että sitä tullaan hyödyntämään VAHTI-työryhmän työssä.

Vaikka malli ei anna kovin konkreettista ohjetta, niin Siposen mukaan mallin käytölle ei ole estettä. Siposen mukaan vaiheissa ei ole sinällään mitään huomautettavaa ja vertaa muodostetun mallin vaiheita olemassa olevien standardien vaiheisiin, joissa ei niissäkään anneta kovin konkreettisia ohjeita.

Limnéllin mukaan malli on samankaltainen kuin hänen edustamansa INSTA:n työn alla oleva malli.

> “Mä voisin tiivistää sen (muodostettu malli), että te haluatte muuttaa tämän digitaalisen maailman turvallisuuskulttuuria parempaan suuntaan. Oleellista siinä on se sana kulttuuri.”

Limnéll kuvasi kulttuurin kehittämisen ja johdon sitoutumisen merkitystä turvallisuuteen vaikuttamisessa, koska ohjaus tapahtuu ylhäältä alaspäin. Mallin ollessa lähtökohtaisesti strategisen tason malli, sen voidaan nähdä vastaavan tähän haasteeseen.

Kimmo Rouskun kanssa keskusteltiin riskien arvioinnin johdosta tehtyjen toimenpiteiden toteutumisen valvonnasta, mutta päädyttiin siihen, että valvonta ei sinällään kuulu riskien arvioinnin prosessiin vaan laajempaan riskienhallinnan kokonaisprosessiin.

Kaikissa haastatteluissa nostettiin esille mallin antama ohjaus riskien arvioinnin suorittamiseksi. Erityisesti kaivattiin eroja riskien arvioinnin ja muiden arviointien ja analyysien välille. Mallissa on kuitenkin pyritty säilyttämään koko organisaation yhteinen riskien arvioinnin kulttuuri, jonka osa-alueita tarkennetaan organisaation toiminnan mukaisesti. Organisaation kulttuuria on haastattelujen perusteella hankala lähteä muuttamaan strategista tasoa alemmilta tasoilta. Tälle löytyy myös tukea tutkimuksen teoreettisesta viitekehyksestä ja kirjallisuudesta. Johdon sitoutuminen, kommunikaatio koko henkilöstön kanssa ja yhteisöllisyys ovat keskeisiä menestystekijöitä riskien arvioinnissa. Organisaatiot laativat nykyisin varsin yksityiskohtaisia ohjeita esimerkiksi tutkimuksen osana olevien tietoturvapolitiikoiden osalta, mutta niiden sisältöä ei tästä huolimatta hallita organisaatioissa.

6.3 HERÄTE – Riskien arvioinnin prosessimalli

Seuraava luku esittelee tutkimuksen tärkeimmän tutkimustuloksen, eli muodostetun riskien arvioinnin prosessimallin. Tutkimuksen haastattelut suunnattiin finanssialan organisaatioiden tietoturvallisuusjohtajille ja tutkimuskysymystä lähestyttiin tietoturvapolitiikkaan liittyvän apukysymyksen kautta. Muodostumiseen on näin ollen vaikuttanut tulevaisuudessa voimakkaasti organisaatioiden toimintaympäristöön vaikuttava turvallisuuden osa-alue eli kyberturvallisuus. Prosessi on laadittu kuitenkin huomioiden turvallisuuden laajempi kenttä. Shameli-Sendi ym. (2016) ovat riskien arvioinnin taksonomiassaan nähneet vanhan taksonomian (laadullinen, määrällinen tai laadullisen ja määrällisen yhdistelmä) liian rajoittuneena verrattuna nykyajan nopeasti muuttuvaan toimintaympäristöön. Baskervillen (1991) näkemys riskianalyysin menetelmän kehittämisestä kvantitatiivisesta, tilastoihin perustuvasta menetelmästä, kohti organisaation johdon ja turvallisuusasiantuntijoiden kommunikointimenetelmää saa näin ollen tuoreessa Shameli-Sendin ym. (2016) tutkimuksessa tukea. Rasmussen (1997) on ehdottanut tutkimusta muun muassa ihmisille luontaisen päätöksenteon toimintatavoista muutoksen ja paineen alla, vaaraa aiheuttavien tapahtumien luokittelun ja näiden hallinnan sekä yhteiskunnan toimijoiden välisen yhteistoiminnan osalta. Tutkijoiden näkemyksen mukaan fyysistä ja digitaalista maailmaa ei voi erottaa toisistaan, jota tukee muun muassa Soomro ym. (2016) näkemys holistisemmasta näkökulmasta turvallisuuteen. Haastateltujen tietoturvajohtajien näkökulmasta tietoturvallisuus tulee nähdä entistä enemmän osana liiketoimintaa ja liiketoiminnan johtamista. Tätä näkemystä tukee aiempi tutkimus (mm. Siponen, Mahmood & Pahnila, 2014; Siponen, 2000; Baskerville, 1989). Tutkimukset (mm. Adams & Sasse,1999; Siponen & Oinas-Kukkonen, 2007) kuvaavat suurimman osan aikaisemmasta tutkimuksesta keskittyvän teknisten järjestelmää turvaavien mekanismien tutkimiseen, mutta ei kyseisten mekanismien käytettävyyteen. Käytettävyys ja käytettävyyden turvaaminen nousivat tehdyissä haastatteluissa liiketoiminnan kannalta merkittäviksi tekijöiksi. Teknisiä järjestelmiä turvaavien mekanismien tutkiminen on tärkeää, mutta haastattelujen perusteella sen ei tule muodostua itsetarkoitukseksi.

Mallin muodostamisen pohjana käytettiin pääosin tietoturvallisuuden ja tietojärjestelmien tieteellistä tutkimusta ja kirjallisuutta sekä alalla yleisesti käytössä olevia tietoturvallisuuden ja yleisemmän riskienhallinnan standardeja. Mallin muodostumiseen vaikutti erittäin vahvasti finanssialan organisaatioiden tietoturvajohtajien haastatteluista kerätty empiirinen materiaali. Näin ollen mallin pohja on vankasti tieto-/kyberturvallisuudessa ja se on pyritty muodostamaan nimenomaan tietoturvajohtajan näkökulmasta.

Näkökulmasta ja mallin tieteellisestä pohjasta huolimatta mallista tehtiin tarkoituksella yleisempi riskien arvioinnin prosessimalli. Mallin varsinaista dokumentaatiota (liite 10) ei kuitenkaan haluttu sitoa liian tiukasti johonkin tiettyyn kontekstiin. Tutkimuksen aikana tutkijat huomasivat, että turvallisuuteen liittyvää riskien arviointia ja –hallintaa ei pitäisi erottaa toiminnaksi, joka on liian erillään organisaatioin muusta toiminnasta. Tämän vuoksi on tärkeää, että

prosessit ovat mahdollisimman yhtenäisiä ja että niiden tulokset ovat vertailukelpoisia. Muodostamalla mallista yleisempi, pyritään osaltaan vastaamaan tähänkin haasteeseen.

Malli on nimetty Heräte -malliksi englannin kielestä lainatun käsitteen "trigger" mukaan. "Trigger", tässä tutkimuksessa "heräte", kuvaa liikettä aikaansaavaa tapahtumaa, eräänlaista laukaisevaa tekijää. Muodostetun mallin sisältö on kuvattu lukuun sisennetyllä tekstillä. Perusteet mallin muodostumiselle on kuvattu tähän lukuun. Heräte -mallin perusteet on johdettu kirjallisuudesta, tutkimuksessa käsiteltyjen standardien synteesistä, vaihtoehtoisista menetelmistä sekä kahden haastattelukierroksen aineistosta. Kerätyn materiaalin perusteella on muodostettu malli, joka vastaa organisaatioiden ketterien prosessien tarpeeseen. Riskien arvioinnin prosessimalli löytyy liitteestä 10 ja prosessimallista laadittu tiivistelmä posterin muodossa liitteestä 11. Mallista on tarkoituksella muodostettu geneerinen, yleisemmän tason malli, jota on mahdollista käyttää muuallakin, kuin riskien arvioinnin kontekstissa. Heräte -mallissa käytetään jatkossa lähdeviittauksissa mainintaa "standardien synteesi, luku 4.2, kohdat X ja Y", joka kuvaa tutkimuksen "Riskien arvioinnin menetelmät" kappaleessa laadittua neljän standardin synteesiä, jossa on 11 kohtaa.

Tutkimuksen olennaisin tulos, eli muodostettu riskien arvioinnin malli esitellään seuraavassa luvussa (6.3.1 – 6.3.8). Sitaatit alaluvuissa 6.3.1 – 6.3.8 ovat otteita Heräte –mallista. Heräte –mallin otteiden yhteydessä perustellaan tutkimuksen aineistolla niitä tekijöitä, jotka ovat vaikuttaneet mallin muodostumiseen.

6.3.1 Perusteet

Laaditun Heräte -mallin taustalla vaikuttavat merkittävästi tutkimuksen pohjana olevan tieteellisen teorian, standardien ja haastattelujen kautta havaittu johdon tuen sekä organisaatiokulttuurin merkitys organisaatioiden menestystekijöinä (mm. standardien synteesi, luku 4.2, kohdat 1 ja 5; RIMS, 2011; Baskerville, 1991). Prosessi antaa perusteita johtajien päätöksenteolle ja yhdenmukaistaa tämän lisäksi organisaation henkilöstön näkemystä riskien arvioinnin suorittamisesta. Riskien arviointi kuvaa käsitteenä uhkien kautta havaittujen riskien arvioimista organisaation kannalta. Tutkimuksessa riskien arviointi kuvataan organisaatioiden oman toiminnan tarkastelun ja oppimisen sekä innovaatioiden löytämisen ja menestyksen turvaamisen prosessina. Vastaavaa oppimisprosessia ovat kuvanneet aiemmin myös John Boyd OODA -silmukalla (Brehmer, 2005) ja W. Edward Deming PDCA -syklistä edelleen kehitetyllä PDSA -syklillä. (Deming, 2016; Moen & Norman, 2006). On tärkeää huomata, että mainitut menetelmät eivät perustu tieteelliseen tutkimukseen, vaan kehittäjiensä henkilökohtaisiin näkemyksiin oppimisprosessista. Menetelminä OODA -silmukka ja PDSA -sykli on kuitenkin koettu yleisesti toimiviksi. Tehtyjen haastattelujen aikana OODA -silmukkaan viitattiin nimellä, joka kuvaa menetelmän tunnettavuutta. Menetelmien vaiheita tarkastelemalla, tarkentamalla ja yhdistämällä on löydettävissä yhtäläisyyksiä haastateltujen organisaatioiden jokapäiväiseen toimintaan. PDSA -syklin ja OODA -silmukan prosesseissa on vähän suoritet-

tava vaiheita. Mayryn (2016) tutkimuksen tulokset organisaatioiden strategian tiedostamisesta organisaatioiden eri tasoilla tukee prosessien ketteröittämistä ja yksinkertaistamista. On aiheellista kysyä, onko organisaatioissa tarvetta monimutkaisille prosessikuvauksille, ellei henkilöstö suurelta osin, edes johtotasolla ymmärrä niitä? Brehmer (2005) kuvaa OODA-silmukkaa menetelmäksi nopealle päätöksenteolle, jossa toimintaa pyritään muokkaamaan saatujen havaintojen ja saavutetun ymmärryksen kautta tehokkaammaksi ja päämääriä palveleviksi. PDSA -sykli toimii Moenin ja Normanin (2006) mukaan viitekehyksenä yksityiskohtaisille menetelmille ja toimii kaikissa organisaatioissa sekä organisaation eri tasoilla. Helposti opittava ja käytettävä menetelmä tukee oppimista ja kehittymistä. Sykli lisäksi osallistaa pragmaattisen mallin kautta organisaation henkilöstöä ryhmätyöhön kehityksen takaamiseksi. (Moen & Norman, 2006). Heräte -mallissa otetaan huomioon organisaation tavoite toimia kohti yhteistä tavoitetta mallin toimiessa viitekehyksenä organisaation sisäisten toimintojen menetelmille.

> *Organisaatiolla on yksi strategia, jota kaikkien muiden prosessien tulee tukea. Riskienhallinta saa ohjauksen strategian kautta ja määrittää riskien arvioinnin perusteet. Riskien arviointi on osa organisaation kilpailukykyä, jolloin ketterät sekä dynaamiset toimintatavat ovat ratkaisevassa asemassa. Epävarmuus ja nopeat muutokset toimintaympäristössä tuovat mukanaan myös mahdollisuuksia. Laadukas riskien arviointi on keino erottua kilpailijoista, varmistaa osaltaan organisaation luotettavuus ja trendien tunnistamisen kautta löytää uusia mahdollisuuksia tulevaisuuden innovaatioille. (Ote Heräte –mallin dokumentaatiosta, liite 10)*

Tätä tukee muun muassa Porterin (1979) tutkimus, jonka mukaan organisaation johdon tulisi käyttää sellaisia arviointimenetelmiä, jotka kykenevät huomioimaan tulevaisuuden trendit ja kehityssuunnat. Edellä mainittua vahvistaa Mannermaan (1991) esittämät tulevaisuudentutkimuksen paradigmat, joiden mukaan tulevaisuus ei ole ennakoitavissa tai ennalta määrätty ja sen kulkuun voidaan vaikuttaa tehtävillä valinnoilla. Heräte -mallilla tunnistetaan herätteitä, syötteitä, joiden avulla on mahdollista löytää keinoja organisaation toiminnan suuntaamiseen. Tutkimuksen haastatteluaineisto antoi myös osaltaan tukea sille, että strategian ja riskienhallinnan tulisi olla riittävällä tasolla yhteydessä toisiinsa. Haastattelujen yhteydessä nostettiin esille nimeltä OODA-silmukan kaltainen lähestymistapa riskienhallintaan, koska mallin koettiin soveltuvan nopeasti muuttuvan maailman vaatimuksiin (Organisaatio C).

> *Yhä monimutkaistuva maailma luo organisaatiolle tarpeen tehdä tehokkaita toimenpiteitä yhä nopeammin. Organisaatioiden tulee pystyä reagoimaan nopeasti muuttuvan toimintaympäristön asettamiin haasteisiin. Riskien arvioinnin tulosten jakamisen avulla on mahdollisuus löytää uusia yhteistyömuotoja. Aikaisemmat riskien arvioinnin menetelmät ovat perustuneet riskienhallintaorganisaation keräämiin havaintoihin. Mallissa datan ja tiedon kerääminen perustuu aktiiviseen toimintaan. Aktiivinen tiedonhankinta tarkoittaa organisaation omaaloitteista, proaktiivista, kanssakäymistä ympäröivän maailman kanssa ja muutosten tunnistamista tiedon joukosta. Tämä malli tarjoaa mahdollisuuden mahdollisimman monipuolisen tiedon keräämiseen. Tieto ja tilannekuva ovat aina jossain määrin puutteellisia ja tämän vuoksi on tärkeää, että riskien arvioinnin prosessi on joustava ja dynaaminen. Malli pyrkii esittämään riskien arvioinnin prosessina, jossa olemassa olevaa tietoa käytetään mahdollisimman tehokkaasti hyväksi ja sitä pyritään aktiivisesti täydentämään prosessin edetessä.*

Mallin tavoite on pyrkiä mahdollisimman kattavaan tietoon ja tilannekuvaan. (Ote Heräte – mallin dokumentaatiosta, liite 10)

Aktiivista, ennakointiin pyrkivää toimintaa voidaan perustella esimerkiksi OODA-silmukan periaatteilla, joiden mukaan etulyöntiasema pyritään saavuttamaan sillä, että oma päätöksentekosykli onnistutaan muodostamaan vastustajan sykliä nopeammaksi. OODA -silmukka ja PDSA -sykli keräävät prosessin taustalle havaintoja. Nykyajan digitaalisen toimintaympäristön nopeat muutokset kuitenkin vaativat organisaatioilta kykyä muodostaa aktiivisen tiedonkeruun kautta tilannekuva, jonka kautta etulyöntiasema on mahdollista saavuttaa. Aktiivinen tiedonhankinta ja ennakointi eivät nousseet selvästi esiin standardien tarkastelussa, mutta haastatellut organisaatiot pääsääntöisesti tiedostivat sen tarpeen omiin käytännön kokemuksiinsa perustuen. Kyberympäristön asettama haaste riskien arvioinnille tiedostetaan muun muassa Shameli-Sendi ym. (2015) tutkimuksessa.

Aiemman tieteellisen tutkimuksen tarjoamat mallit ja teoria riskien arviointiin tai turvallisuuspolitiikan laatimiseen (mm. Karyda, 2005; Knapp, 2009) tarjoavat selkeät perusteet prosesseille, mutta nekään eivät huomioi nopeasti muuttuvan toimintaympäristön asettamia vaatimuksia.

Organisaation riskien arvioinnin tulee perustua henkilöstöä osallistaviin riskitietojen raportointiin ja työpajoihin, joissa pyritään kattavasti ylläpitämään tilannekuvaa organisaation riskeistä. Toiminnan tulee olla hyvin organisoitua ja vastuutettua prosessin omistajalle, kuten turvallisuusjohtajalle tai muulle nimetylle henkilölle, joka käy keskustelua johdon ja henkilöstön välillä. Henkilöstön sitoutuminen on organisaatiolle mahdollisuus saada havaintoja erilaisilta ihmisiltä. Ihmiset tekevät havaintoja asioista erilaisista lähtökohdista ja aikaisempiin kokemuksiinsa verraten. Muun muassa henkilöstön koulutus ja harrastuneisuus tuovat uusia näkökulmia kokonaisvaltaiseen riskien arviointiin. Merkittävän, asioita ja tilanteita ratkaisevan, tiedon lähdettä on riskien arviointi prosessin alkaessa hankala tietää.

Riskien arvioinnin tuloksena, toimintana, organisaatio pyrkii käsittelemään riskejä esimerkiksi luomalla painopisteitä tietoturvaperiaatteiden kautta tai tekemällä taloudellisia investointeja organisaation tietoturva-arkkitehtuuriin. Mallin taustalla on ajatus uhkien sekä muiden herätteiden kattavasta tunnistamisesta, riskien arvioinnin nopeuttamisesta, yksinkertaistamisesta ja yhdenmukaistamisesta organisaation strategian mukaisesti. Malli on laadittu tieteellisen kirjallisuuden, standardien ja kaksivaiheisen laadullisen tutkimuksen synteesinä. Muodostettu malli on rakennettu finanssialan organisaatioiden riskien arvioinnin lähtökohdista. Mallissa ei ole kuitenkaan rakenteita, jotka tekisivät siitä ainoastaan finanssialaan soveltuvan. Näin ollen malli soveltuu käytettäväksi organisaatioihin ja dynaamisiin prosesseihin toimialasta riippumatta.

Suomalaisten finanssialan organisaatioiden edustajilla ja mallin validointiin osallistuneilla asiantuntijoilla on ollut mallin muodostumisessa merkittävä osuus. Kiitoksia yhteistyöstä ja avoimesta keskustelusta. (Ote Heräte –mallin dokumentaatiosta, liite 10)

Työpajatyöskentely ja henkilöstön osallistaminen riskitiedon keräämisessä ja analysoinnissa nousi haastatteluaineistosta selvästi esiin. Pääsääntöisesti nekin organisaatiot, jotka eivät toteuttaneet henkilöstöä osallistuvia riskien arvioinnin menetelmiä, tiedostivat sen, että tätä kautta on mahdollista saada luotettavampia ja yhdenmukaisempia tuloksia. Tätä tukee myös standardien antamat

ohjeet riskien arvioinnin toteuttamisesta (standardien synteesi, luku 4.2, kohta 10).

Killingin ja Malnightin (2005) mukaan organisaatioiden johdon tulee hallita kaksi asiaa samaan aikaan:

- Johtajien tulee kyetä erottamaan ja tunnistamaan, miten voittaa tärkeimmät ja keskeisimmät taistelut.
- Johtajien tulee kyetä hahmottamaan, miten organisaatiota viedään kohti pidemmän aikavälin tavoitteita. Tässä korostuu organisaatioiden tehokkuuden parantaminen ja toimintojen jakautumisen, niin sanotun siiloutumisen, välttäminen.

Optimaalisessa tilanteessa organisaatio voittaa taisteluita ja kehittää organisaatioita samanaikaisesti. (Killing & Malnight, 2005).

6.3.2 Riskien arvioinnin vaiheet

Luvussa kuvataan riskien arvioinnin prosessin vaiheita ja vastuutahoja ensin yleisellä tasolla ja tämän jälkeen tarkemmin kuvion 13 ja taulukon 10 avulla. Heräte -mallin muodostamisessa on otettu huomioon haastateltujen organisaatioiden kokemukset ja hyvät käytänteet ketteristä sekä yhdenmukaisista prosesseista.

> *Mallin vaiheisiin on valittu organisaatioiden käytännön kokemuksia ja parhaita käytänteitä tehokkaan riskien arvioinnin toteuttamiseksi. Riskien arviointi koetaan nykyisessä muodossaan kankeaksi ja toimimattomaksi prosessiksi. Menetelmät koetaan perehtymistä vaativiksi ja niiden tulokset koetaan epätarkoiksi. Mallin muodostumisen taustalla on tarve prosessin yksinkertaistamiselle ja tehostamiselle. Prosessin tulee olla omaksuttavissa nopeammin ja ohjeiden tulee olla selkeämmät. (Ote Heräte –mallin dokumentaatiosta, liite 10)*

Kuvion 13 riskien arvioinnin prosessimallissa on kuvattu prosessin eri vaiheiden rajapintoja muihin vaiheisiin. Vaiheet menevät osin päällekkäin, jolloin numeroin ilmaistut vaiheet kuvaavat lähinnä prosessin pääpainon siirtymistä numeron osoittamaan vaiheeseen. Malli on syklimäinen, jatkuva, ketterä ja ennen kaikkea kehittyvä prosessi, jota on mahdollista käyttää organisaatioiden eri tasoilla. Malli muodostettiin organisaatioiden riskien arvioinnin tarpeisiin, mutta on sovellettavissa myös muihin kehittyviin prosesseihin, kuin ainoastaan riskien arviointiin. Kuvion 13 mallin vaiheita hyödyntäen on mahdollista toimia nopeasti muuttuvissa tilanteissa organisaation strategian mukaisesti tiedostaen se tosiasia, että parhaimmillaankin riskien arviointiin sisältyy epävarmuustekijöitä. (standardien synteesi, luku 4.2, kohta 2). Menestyksen kannalta on tarpeen tarkentaa mallin vaiheita organisaation strategian mukaisesti, mutta yhä nopeammin muuttuvassa maailmassa tulee eteen tilanteita, joissa tarvitaan erityisen yksinkertaista ohjeistusta toiminnan tueksi. (mm. standardien synteesi, luku 4.2, kohdat 2, 4 ja 6; RIMS, 2011; Brehmer, 2005; Deming, 2016; Moen & Norman, 2006). Knapp ym. (2009) prosessimallia käytettiin ensimmäisen vai-

heen haastatteluissa sen selvittämiseksi, onko mallin kuvaus liian yleinen. Tietoturvajohtajien näkökulmasta Knapp ym. (2009) malli ei ole liian yleinen. Mallin sisäisten ja ulkoisten vaikuttimen koettiin soveltuvan lisäksi riskien arviointiin.

KUVIO 13 Riskien arvioinnin prosessi *(Ote Heräte –mallin dokumentaatiosta, liite 10)*

Mallin ei oleteta antavan tyhjentäviä vastauksia riskien arviointiin vaan ohjaavan prosessia oikeaan suuntaan. Mallia soveltamalla organisaatioiden on mahdollista laatia omista lähtökohdistaan ketterämpi menetelmä riskien arviointiin. Vaiheet on käsitelty seuraavissa luvuissa yleisesti. Tarkemmat kuvaukset ovat luettavissa Kokkomäen ja Nortusen Jyväskylän yliopistossa laaditusta pro gradu -tutkielmasta. Riskien arvioinnin tulisi olla mahdollisimman joustava ja aktiivinen prosessi ja sen tulee kyetä reagoimaan nopeisiin muutoksiin. Arvioinnin vaiheet 1. - 3. menevät päällekkäin siten, että tiedonhankinnan tulee olla mahdollisimman monipuolista ja aktiivista. Tiedonhankinnan tulee jatkua koko ajan. Se ei ole irrallinen vaihe, joka lopetetaan sen suorittamisen jälkeen. Myös kerätyn tiedon analysoinnin tulee olla aktiivista ja jatkuvaa. Vaiheet määrittävät mallissa prosessin painopisteen eikä niinkään tiukasti vaiheesta toiseen etenevää kulkua. (Ote Heräte –mallin dokumentaatiosta, liite 10)

Taulukossa 10 kuvataan yksinkertaistetussa muodossa Heräte -mallin vaiheiden vastuut. Kaikessa organisaation toiminnassa, myös riskien arvioinnissa, tulee olla nimetty vastuuhenkilö. Vastuuhenkilö vastaa, että prosessi jatkuu ja toimenpiteet tulee suoritettua organisaation johdon määrittelemissä rajoissa. (standardien synteesi, luku 4.2, kohdat 6, 9 ja 11; RIMS, 2011). Riskien arviointi on strategiasta johdettu prosessi, jossa pyritään suodattamaan organisaation kannalta merkittävät riskit jatkotoimenpiteitä varten ja oppimisen pohjaksi. (Porter, 1980; RIMS, 2011).

Taulukko 10 Vastuunjako

	Vastuu	Suorittaja	Työtapa
1. Aktiivinen tiedonhankinta	Prosessin omistaja	Koko organisaatio	Tiedon aktiivinen kerääminen ohjatusti
2. Analyysi	Prosessin omistaja	Asiantuntijaryhmä	Työpajat ja asiantuntijaryhmät
3. Toimenpiteiden valmistelu	Prosessin omistaja	Valikoituu tilannekohtaisesti	Analysoidun riskin siirto asiasta vastaavalle toimijalle
4. Tiedon kertyminen ja oppiminen	Prosessin omistaja	Asiantuntijaryhmä	Vaiheiden 1-3 aikana kertynyt tieto ja palaute toiminnasta palaavat koordinoidusti joko uudeksi herätteeksi tai organisaation tietopääomaksi

(Ote Heräte –mallin dokumentaatiosta, liite 10)

Riskien arvioinnin prosessin kaikilla toimijoilla tulee olla tiedossa prosessista vastaava henkilö:

> *Vastuunjako eri vaiheissa on riippuvainen organisaation rakenteesta. Olennaista on se, että toiminnan kokonaisuus on organisoitu ja johdettu selkeästi. Riskien arvioinnin prosessi ei saa olla kuitenkaan liian henkilökeskeinen. Koko organisaation ammattitaito tulee pyrkiä hyödyntämään arvioinnin suorittamisessa. (Ote Heräte –mallin dokumentaatiosta, liite 10)*

6.3.3 Heräte

Maailma muuttuu yhä nopeammin ja näin ollen erilaisten herätteiden tunnistaminen tulee jatkossa entistä tärkeämmäksi. Tulevaisuudentutkimuksessa on jo pitkään käytetty käsitettä “trendit”. Esiteltävän mallin avulla on mahdollista poimia data- ja tietovirroista merkkejä, joiden perusteella on mahdollista tunnistaa toimintaan vaikuttavia tekijöitä (standardien synteesi, luku 4.2, kohta 7). Suurten kokonaisuuksien hahmottaminen on edelleen erittäin tärkeää, mutta organisaation kilpailukykyyn vaikuttaa yhä voimakkaammin pienten muutosten aiheuttamien tapahtumakulkujen havainnointi.

> *Riskienhallinnassa pyritään löytämään kokonaisvaltaisesti organisaation strategiaa uhkaavia tekijöitä ja ilmiöitä sekä hallitsemaan niitä. Organisaatio etsii ja pyrkii tunnistamaan ympäröivästä maailmasta, erityisesti omasta toimintaympäristöstään, herätteitä, joiden avulla on mahdollista puuttua riskeihin ennalta. Organisaatioilla on oman toimialansa vaikutuksesta ja tiedon kertymisen kautta tiedossa riskejä, joiden herätteitä pyritään havainnoimaan. Herätteiden havainnointi ja aktiivinen tiedonhankinta menevät vaiheina osittain päällekkäin ja tästä syystä riskien arvioinnin prosessimallissa on huomioitava myös herätteiden vaikutus.*
>
> *Riskien arvioinnin aloitukselle ei voi määrittää yhtä aloittavaa herätettä. Herätteiden merkityksellisyyttä arvioivat ihmiset. Ihmisten aiemmat kokemukset määrittävät, miten ihminen pystyy tunnistamaan kaikesta datasta ja olemassa olevasta tiedosta merkitykselliset herätteet. Organisaation tietoisuuden ja historiatiedon kasvaessa on mahdollista automatisoida siirty-*

mistä herätteestä suoraan toimintaan, jolloin riskien arviointi voidaan jättää tekemättä tai prosessin kulkua voidaan nopeuttaa. Esimerkkinä herätteestä voivat olla tunnistetut hyökkäykset organisaation tietojärjestelmiä kohtaan, jolloin puolustusmekanismit voivat reagoida suoraan herätteestä (tunkeutumisyritys) ja estää vastapuolen yritykset.

Riskien arviointi tuottaa prosessin aikana uusia herätteitä, jolloin tiedon kertymisen ja oppimisen (mallin vaihe 4) kautta organisaatiossa pyritään luomaan syvempi ymmärrys omasta toimintaympäristöstä ja sen riskeistä. (Ote Heräte –mallin dokumentaatiosta, liite 10)

Tarve herätteiden tunnistamiselle nousi vahvasti esiin finanssialan organisaatioiden haastatteluissa. Kaikki organisaatiot tiedostivat toimintaympäristön asettaman vaatimuksen siitä, että heidän tulisi pyrkiä mahdollisimman ennakoivaan toimintaan.

6.3.4 Aktiivinen tiedonhankinta

Aktiivisen tiedonhankinnan kautta organisaatioiden tulee pyrkiä riskienhallinnassaan entistä aktiivisempaan ja ennakoivaan toimintaan. (standardien synteesi, luku 4.2, kohta 4, 5, ja 8). Aktiivisella tiedonhankinnalla organisaatio kykenee hyödyntämään laajasti erilaisia tietolähteitä oman tilannekuvansa muodostamiseksi. Heräte -mallissa on otettu kantaa jo olemassa olevan tietovarannon, oman henkilöstön, aktiivisempaan rooliin datan keräämisessä sekä aiemmin opitun tiedon hyödyntämisessä (standardien synteesi, luku 4.2, kohta 8 ja 10). OODA-silmukan (Brehmer, 2005) ja PDSA -syklin (Deming, 2016; Moen & Norman, 2006) kaltaiset menetelmät perustuvat havaintoihin maailmasta. Heräte -mallissa tiedonhankinta pyritään kuvaamaan organisaation lähtökohdista tapahtuvaksi aktiiviseksi toiminnaksi, jota tehdään jatkuvasti prosessin edetessä. Aktiivinen tiedonhankinta jatkuu siis myös prosessin seuraavissa vaiheissa, jolloin kerättyä tietoa saadaan tarkennettua. Tutkimuksen haastatteluissa koettiin, että aktiivinen tiedonhankinta on jo tämän päivän, mutta ennen kaikkea tulevaisuuden keino organisaation menestykseen. Borum ym. (2015) mukaan kybertiedustelulla pyritään havaitsemaan mahdolliset riskit ja uhat kyberturvallisuudelle jo ennen hyökkäystä. Organisaatioiden investoinnit teknologiaan, kuten palomuureihin ja tunkeutumisen havaitsemisjärjestelmiin (IDS), ovat soveltuvia, mutta riittämättömiä. Jatkuvassa muutoksessa tiedustelu on aikaisempaa tärkeämpi tekijä.

Organisaation tulee itse ymmärtää, mitä tietoa tarvitaan strategian toteutumiseksi. Nykyaikaiselle organisaatiolle on ominaista aktiivinen tiedon hakeminen eri lähteistä. Aktiivinen tiedonhankinta kuvaa organisaation jatkuvaa kanssakäymistä ympäröivän maailman kanssa. Keskeinen toiminta-ajatus on olla itse aloitteellinen osapuoli. Tietoa hallitsevien yksilöiden, ryhmien ja järjestelmien kanssa pyritään muodostamaan yhteistyöverkostoja. Tietoa tuottavat muun muassa oman organisaation henkilöstö, sidosryhmät, yhteistyöverkostot ja erilaiset käytössä olevat teknologiat. Organisaatiossa olevien projektien aikana kertyvän datan ja tiedon käyttöön tulee kiinnittää erityistä huomiota.

Tiedonhankinnan perustana tulee käyttää organisaation jo olemassa olevia varantoja. Toiminnan suuntaamisen ja kehittymisen kannalta on kuitenkin merkityksellistä havainnoida aktiivisesti mahdollisuuksia saada tietoa uusista lähteistä sekä uusia teknologioita käyttäen.

Etua strategian toteuttamiseen on mahdollista hakea erilaisia muutoksia, trendejä, tunnistamalla. Trendien tunnistamisessa on mahdollista käyttää apuna julkisia sekä palveluntarjoajien maksullisia datavarantoja.

Riskien arvioinnin perusteena olevan tiedon hankinnan tulee olla koordinoitua. Organisaatiossa tehtyjen toimenpiteiden ja muiden tapahtumien jälkeen tieto tulee palauttaa uusien herätteiden ja oppimisprosessin perustaksi. Henkilöstöllä tulee olla mahdollisuus kirjata ylös mahdollisia havaintoja riskien arvioinnin perustaksi riskien arvioinnin analyysin tueksi.

Vastuuhenkilö tiedon hankinnalle on kyseisen prosessin omistaja. Organisaatiosta riippuen henkilön tehtävänimike voi vaihdella, mutta keskeistä on keskusteluyhteys johdon ja henkilöstön edustajien kanssa.

Organisaation riskien arvioinnin kannalta tärkeitä asioita ovat koko henkilöstön motivointi, riskitiedon ja trendien jakaminen sekä suunnitellusti toteutettu henkilöstön palkitseminen. (Ote Heräte –mallin dokumentaatiosta, liite 10)

Organisaatioiden kannalta on huomattava ero sillä, kerätäänkö tietoa historiasta ja menneistä tapahtumista vai pyritäänkö tunnistamaan tulevaisuuden mahdollisuuksia. Historiatiedon tarkastelun kautta päädytään usein reaktiiviseen toimintaan jo tapahtuneiden vahinkojen ja toteutuneiden uhkien osalta. Proaktiivinen toiminta ja mahdollisten vahinkoa aiheuttavien uhkien, organisaatiota koskevien riskien, tarkastelu on usein kustannustehokkaampaa kuin vahinkojen paikkaaminen.

6.3.5 Analyysi

Data on tietoa, jolla ei välttämättä ole organisaatiolle sellaisenaan merkitystä. Analyysin kautta organisaatiolla on mahdollisuus jäsentää aktiivisesti kerätty tieto itselleen merkitykselliseen muotoon. Analyysin suorittamisessa tulee hyödyntää mahdollisimman laajasti koko organisaation ammattitaitoa ja osaamista. (mm. standardien synteesi, luku 4.2, kohdat 2, 3, 5, 6, 8 ja 10). Analyysin laatimisessa on merkityksellistä organisaation kyky oppia ja kerätä tarvitsemaansa tietoa. Tiedon kertymisen ja oppimisen sekä analyysin vaiheet täydentävät toisiaan koko ajan. Analyysin kautta tunnistettuja suurempia kokonaisuuksia, jäsenneltyä tietoa ja tätä kautta muodostettua analyysia tulee ohjata viipymättä uusiksi herätteiksi ja herätteiden keräämisen pohjaksi laajasti organisaation sisällä.

Analyysi kuvaa organisaation keräämän datan suodattamista tiedoksi. Organisaatiot keräävät tietoa aktiivisesti, jolloin riskien arvioinnin perusteena olevan jäsennellyn tiedon keräämiseksi tulee suorittaa erityisiä työpajoja, workshoppeja. Työpajoihin osallistuvat organisaation eri toimintayksiköiden nimetyt riskien arvioinnin vastuuhenkilöt. Vastuuhenkilöiden valinnassa tulee painottaa laajaa ymmärrystä riskien arvioinnin perusteena olevan tiedon hankinnassa ja koko henkilöstön näkemyksen esille tuomisessa. Työpajat ovat suunniteltuja ja valmisteltuja tilaisuuksia, joissa käydään läpi ennalta määriteltyjä asioita. Riskejä tuodaan esille laajasti organisaation toiminnan eri osa-alueilta, mutta työpajoissa pääpaino on kuitenkin suunniteltujen asioiden läpikäymisellä.

Tiedon hankinnan ja analyysin välille ei voi määrittää yhtä tiettyä tekijää, joka määrittää siirtymisen vaiheesta toiseen. Kuvaava esimerkki on, että organisaatiot järjestävät suunnitelmien mukaisesti, omaan toimintaansa perustuen, neljännesvuosittain, puolivuosittain tai kerran vuodessa työpajoja. Analysointi tulee ymmärtää kuitenkin vuosittaisia työpajoja laajemmin. Organisaation havaitseman riskin arviointiprosessi saattaa olla hyvinkin nopea ja dynaaminen prosessi, jossa prosessin omistaja kerää toiminnan kannalta keskeiset henkilöt yhteen. Tällöin päätös tehdään olemassa olevan tiedon perusteella mahdollisimman nopeasti. Tällaisia tilanteita ovat muun muassa organisaation toiminnan kannalta kriittisten toimintojen suojaaminen ja toimintojen jatkuvuuden turvaaminen. Päivittäistä operatiivista toimintaa ja riskien arviointia ei tule erottaa toisistaan. Analyysi tehdään samalla tavalla riippumatta käytettävissä olevasta ajasta. Nopeasti eteen tulevassa tilanteessa analyysi suoritetaan sen hetkisen tiedon perusteella prosessin omistajan tai hänen erikseen määräämänsä henkilön johtaessa toimintaa.

Riskien arviointi on aina arvio, johon liittyy useita epävarmuustekijöitä. Analyysin perustana olevan materiaalin tulee sisältää mahdollisimman paljon mitattavissa olevia, kvantitatiivisia, arvoja. Tämä ei kuitenkaan tarkoita sitä, että riskille on mahdollista määrittää tarkka arvo ennalta määritellyllä asteikolla. Riskien arvioinnin tuloksen tulee olla sekä johdon että muun henkilöstön ymmärtämässä muodossa. Tämä tarkoittaa usein sitä, että arvo tulee esittää asteikon lukuarvoa monipuolisemmin käyttäen kvalitatiivisia, laadullisia, mittareita. Toisinaan riskin tuottama vahinko on varsin abstrakti ja tällöin on arvioitava käytettävissä olevan tiedon perusteella kuinka suuren vahingon riski toteutuessaan voi aiheuttaa ottaen huomioon niin konkreettiset fyysiseen omaisuuteen kuin maineeseen vaikuttavat tekijät.

Analyysin tulee tuottaa lopulta yhdenmukaista materiaalia, jota voidaan verrata toisiin riskeihin ja historiatietoihin. Vertailuaineiston eli formaalin, määrämuotoisen, historiatiedon puutteen vuoksi täysin kvantitatiiviseen menetelmään perustuvaa arviointia ei ole mahdollista tehdä. Jotta vertailua olisi mahdollista tehdä, tulisi organisaation kerätä tietoa tapahtumista ja pyrkiä jakamaan sekä vaihtamaan tietoa muiden samalla toimialalla toimivien ja toimialan ulkopuolisten organisaatioiden kanssa. Organisaation kehittyessä ja riskien arvioinnin materiaalin kertyessä on tulevaisuudessa mahdollista tehdä kvantitatiivisin arvoin perusteltavia arvioita.

Tiedon analysoinnista vastaa prosessin omistaja ja sen suorittaa asiantuntijaryhmä. (Ote Heräte –mallin dokumentaatiosta, liite 10)

Analysoidun tiedon jakaminen on tärkeää oppimisen ja tiedon kertymisen takaamiseksi. Ihmiset suunnittelevat, ottavat käyttöön ja murtavat tietojärjestelmät, joten ihmisen toiminta tulee ottaa yhä tarkemmin huomioon. Esimerkiksi Adams ja Sasse (1999) kuvaavat, että tietojärjestelmien turvallisuuden tulisi olla tunnettu ja vakavasti otettava organisaation prosessi. Turvallisuustietoisuutta tulee jakaa mahdollisimman laajasti. (Adams & Sasse, 1999). Tiedon jakaminen tulee ymmärtää yksittäisiä prosesseja laajemmin.

6.3.6 Toimenpiteiden valmistelu

Toimenpiteiden valmistelulla pyritään tukemaan tulevien toimenpiteiden koordinoitua suunnittelua ja valmistelua. Toimenpiteiden valmistelu luo organisaatiolle kyvyn siirtyä tulevaisuudessa entistä nopeammin suoraan toimintaan. Tämä on mahdollista, kun organisaation ymmärrys omista kyvyistä kas-

vaa. Kaikki valmistellut toimenpiteet luovat osaltaan valmiuksia tulevalle toiminnalle. (standardien synteesi, luku 4.2, kohdat 4, 6, ja 8; RIMS, 2011). Toimenpiteiden valmistelun kautta jatkokäsittelyä edellyttävät toimenpiteet, kuten riskit, siirretään organisaatiossa tahoille, joilla on todelliset ja parhaat mahdollisuudet käsitellä asia. Tämä voi edellyttää uudelleenjärjestelyjä muun muassa henkilöstön sijoittamisen tai budjetoinnin suhteen. Ydinajatus on yhdistää päällekkäisiä toimenpiteitä kokonaisuuksiksi ja tehdä toiminnasta kustannustehokkaampaa. Vastuussa oleva henkilö koordinoi resurssien käyttöä toimenpiteen suorittamiseksi. Päällekkäisten toimintojen osalta juuri johtamisvastuu on tärkeää määritellä tehokkaan ja tarkoituksenmukaisen toiminnan tueksi.

> *Toimenpiteiden valmistelu kuvaa sitä, että toimenpiteet, joihin riskien arvioinnin perusteella tulee ryhtyä, siirretään sille organisaation toimijalle, jolla on tosiasiallinen kyky suorittaa ne. Ennen siirtymistä varsinaiseen toimintaan tulee toimenpiteet suunnitella ja valmistella. Toiminnan tulee olla koordinoitua ja johdettua. Tätä kautta valituilla toimenpiteillä saadaan todennäköisemmin huomattavasti tehokkaampi vaikutus.*
>
> *Ihannetilanteessa valmisteltujen toimenpiteiden toteuttamiseen osallistuu useampi toimija organisaation sisällä, jolloin resursseja saadaan tehokkaampaan käyttöön. Tämä tarkoittaa niin henkilöresursseja kuin organisaation eri toimijoille budjetoituja varoja. Riskien arvioinnin seurauksena löydettyjen, toimenpiteitä vaativien riskien käsittely vaatii usein monia asiantuntijoita. Työn päällekkäisyyttä tulee välttää kaikessa toiminnassa. Työpajatyöskentely tukee sekä henkilöstön että muiden resurssien tehokasta käyttöä. Organisaatio voi siirtyä suoraan toimintaan ilman erillistä valmistelua, mikäli sillä on aiempaan kokemukseensa perustuen riittävät edellytykset siihen.*
>
> *Toimenpiteiden valmistelusta vastaa prosessin omistaja. Toimenpiteiden suorittaja määräytyy analysoidun riskin tai riskien perusteella. (Ote Heräte –mallin dokumentaatiosta, liite 10)*

Killingin ja Malnightin (2005) Must Win Battles -strategiaopissa valitaan organisaation kannalta keskeisiä alueita ja luodaan toimintatapoja, joilla suunnataan organisaation resursseja päämäärän kannalta tärkeimpiin ja olennaisiin asioihin. Organisaation kannalta menetelmä yksinkertaistaa toimintamalleja ja auttaa keskittymään ennalta määriteltyihin kehittämistoimenpiteisiin, koska aktiivisesti seurattavia painopistealueet on valittu. Haastatelluissa organisaatioissa korostettiin sitä, että on tärkeää, että valittujen toimenpiteiden suorittaminen on koordinoitua. Toimenpiteitä valittaessa on tärkeää, että ne ovat valmisteltuja ja harkittuja. Jos valittu toimenpide on käsketty ilman riittävää ymmärrystä siitä, mitä sen tekeminen todellisuudessa vaatii, toimenpiteellä ei välttämättä saada aikaan toivottua vaikutusta tai sen toteuttaminen saattaa olla jopa mahdotonta.

6.3.7 Tiedon kertyminen ja oppiminen

Organisaation toiminnassa tulisi aina olla tietoinen reflektointi taaksepäin. Riskien arvioinnin kontekstissa tiedon kertyminen ja oppiminen antavat organisaatiolle mahdollisuuden arvioida toimintaansa ja kehittää sitä. (standardien synteesi, luku 4.2, kohta 8; RIMS, 2011). Useissa haastatteluissa painotettiin ai-

kaisempien riskien arvioinnin menetelmien puutteita oppimisen osalta ja erityisesti virheistä oppimisen osalta. Osassa organisaatioista riskien arvioinnin tuloksilla ei ollut suoraa yhteyttä organisaation päivittäiseen toimintaan. Haastatteluissa kuitenkin painotettiin juuri oppimisen tärkeyttä organisaation menestymisen mahdollistajana. Tietoa jakamalla sekä tukemalla henkilöstön oppimista ja tilannetietoisuutta voidaan kerryttää organisaation tietopääomaa. Tietoa jakamalla voidaan henkilöstön mielenkiintoa ohjata organisaation painottamille toiminnan osa-alueille ja näin ollen pyrkiä uusien herätteiden keräämiseen. Tiedon jakaminen tukee myös organisaation strategian tuomista osaksi henkilöstön päivittäistä toimintaa. Vuosittaisten tai puoli-vuosittaisten koulutuspäivien lisäksi henkilöstö oppii ymmärtämään oman toimintansa tarkoituksen osana organisaation strategiaa päivittäisessä toiminnassa. Strategian toteuttaminen ei voi olla korusanoja vuosittaisissa julkaisuissa vaan toimintaa organisaation päämäärien saavuttamiseksi.

> *Organisaation tulee tietoisesti kerryttää riskien arvioinnista kertynyttä tietoa ja oppia suorittamastaan riskien arvioinnista. Riskien arvioinnin prosessi antaa organisaatiolle mahdollisuuden analysoida oman toimintansa vahvuuksia ja heikkouksia. Tämän tiedon jakaminen ja hyödyntäminen koko organisaation laajuudella auttaa sitä kehittämään toimintaansa. Riskien arvioinnin ei siis tulisi olla prosessi, joka suoritetaan kaavamaisesti suunnitelmassa määritettyyn aikaan, vaan sen tulisi olla jatkuva sykli, jonka kautta organisaatio voi muokata ja kehittää aktiivisesti toimintaansa.*
>
> *Tiedon kertymisen ja oppimisen tulee olla koordinoitua ja johdettua toimintaa. Johdon lisäksi tätä vaihetta kohtaan tulee olla vahva sitoutuminen läpi koko organisaation. Riskien arvioinnin prosessin kautta kertynyttä tietoa tulee jakaa organisaatiossa sekä ylhäältä alas- että alhaalta ylöspäin. Prosessin aikana kertynyt tieto tulee dokumentoida systemaattisesti. Tätä kautta kaikki mahdollinen tieto on aina tarvitsijoiden käytössä.*
>
> *Tiedon kertymisen ja oppimisen vaiheen suorittamisesta vastaa prosessin omistaja. Käytännön suorittajana ovat riskien arviointiin osallistuneet asiantuntijaryhmät. Tiedon kertymisen ja oppimisen tulisi noudattaa oppivan organisaation periaatteita. On oleellista, että tietoa vaihdetaan aktiivisesti joka suuntaan. Saavutetun syvemmän ymmärryksen kautta organisaatio voi kehittää toimintaa ja saavuttaa kilpailukykyä. (Ote Heräte –mallin dokumentaatiosta, liite 10)*

Tehtyjen haastattelujen perusteella datan ja tiedon keräämisessä henkilöstöltä sekä analysoidun tiedon jakamisessa takaisin henkilöstölle oli puutteita. Organisaatioissa koettiin, että tällä osa-alueella on tulevaisuudessa kehittämistä. Organisaatioiden keskeinen näkemys oli, että kaikki mahdollinen tieto toiminnan pohjaksi on tarpeellista. Tiedosta on mahdollista suodattaa organisaation kannalta merkitykselliset asiat ja näin ollen tiedon määrämuotoisuus muodostuu asiaksi, johon tiedon vertailun vuoksi on syytä kiinnittää erityistä huomiota. Kaikki organisaatiot olivat avoimia omien prosessien kehitykselle ja kiinnostuneita erityisesti määrämuotoisen ja vertailtavan tiedon muodostamisesta.

6.3.8 Toiminta

Toiminta -vaihe ei sisälly Heräte -malliin, mutta vaiheiden hyvin läheisen merkityksen vuoksi toimintaa ja sen tavoitetta kuvataan alla olevassa kappaleessa. Toiminnalla tarkoitetaan toimenpiteitä, joihin riskien arvioinnin tuloksilla on vaikutusta. Riskien arvioinnin prosessin tulee tukea organisaation strategiaa. Arvioitujen riskien aiheuttamien toimenpiteiden määrittämisessä tulee tukeutua näin ollen organisaation tavoitetilaan ja menestyksen turvaamiseen. Johdon tulee ymmärtää turvallisuustyökalujen, kuten tietoturvapolitiikan käyttö (Chang & Ho, 2006; Soomro ym., 2016). Riskien arvioinnin ja sen vaikutuksen alaisena olevan toiminnan ei tulisi olla liian riski- ja uhkakeskeistä, vaan organisaation tulisi pyrkiä myös tunnistamaan toimintansa vahvuuksia ja uusia toimintamahdollisuuksia. Tutkimuksen liittäminen organisaatioiden päivittäiseen ja konkreettiseen toimintaan toteutettiin ottamalla osaksi haastatteluja Knapp ym. (2009) tietoturvapolitiikan muodostamisen prosessimalli. Prosessimallia ja tähän kohdistunutta kritiikkiä Alshaikh ym. (2015) käsiteltiin tutkimuksen ensimmäisellä haastattelukierroksella. Alshaikh ym. (2015) kritisoivat kyseistä mallia liiasta yleisyydestä. Knappin ym. prosessimalli ei kyseisen tutkimuksen mukaan tarjoa riittävästi kuvauksia tietoturvapolitiikan johtamisen käytäntöihin. (Alshaikh ym., 2015).

> Riskien arvioinnin tuloksilla pitäisi olla konkreettista vaikutusta organisaation toimintaan. Organisaation strategian toteuttamisen kannalta oikein ajoitetut ja tehokkaat toimenpiteet luovat mahdollisuuden menestykseen. Ajan ja tilan hallinta omassa toimintaympäristössä ovat keskeisiä tekijöitä. Organisaatioiden tulisi pyrkiä olemaan aloitteellisia omassa toiminnassaan, jotta toiminta ei perustu eteen tuleviin tilanteisiin reagointiin vaan ennen kaikkea strategisten tavoitteiden toteuttamiseen ja oma-aloitteiseen toimintaan.
>
> Konkreettisia toimia, joilla riskeihin voidaan vaikuttaa ovat tietoturvallisuuden osalta esimerkiksi erilaiset turvallisuuteen vaikuttavat järjestelmät tai palvelut, henkilöstön koulutus tai organisaation tietoturvaperiaatteiden muokkaaminen. Oleellista on, että se toiminta, johon resursseja suunnataan perustuu oikeaan ja systemaattisella prosessilla saavutettuun kuvaan organisaation tilasta, eli havaituista riskeistä.
>
> Riskien arvioinnin prosessi tarjoaa organisaatiolle tietoa sen toimintaan vaikuttavista riskeistä. Systemaattisen prosessin kautta organisaatiolla on mahdollisuus muodostaa riskeistään kattava kuva. Tämän tilannekuvan avulla organisaatio voi eri aktiviteettien kautta hallita havaittuja riskejä. Organisaatio tavoite on trendien tunnistaminen kerätystä tiedosta. Trendien tunnistamisen kautta organisaatioiden on mahdollista löytää uusia painopistealueita ja innovaatioita toiminnalleen. *(Ote Heräte –mallin dokumentaatiosta, liite 10)*

Tehtyjen haastattelujen kautta pyrittiin tarkastelemaan käytännön kautta, kuinka tarkaksi prosessimallit tulee rakentaa. Haastatteluiden perusteella Knapp ym. (2009) tietoturvapolitiikan muodostamisen prosessimalli on riittävän tarkka ja kuvaa prosessin vaiheita sekä vaikuttavia tekijöitä. Haastattelujen perusteella prosessia olisi tarpeen tarkentaa organisaatioiden sisällä, mutta periaatteet mallissa ovat toimivia. Erityisesti organisaatioiden oppimiseen ja teh-

tyjen toimenpiteiden, toiminnan, vaikutusten arviointi koettiin erityisen mielenkiintoiseksi.

7 YHTEENVETO JA POHDINTA

Tutkimuksen tavoitteena oli muodostaa riskien arvioinnin prosessimalli finanssialan tietoturvajohtajien näkökulmasta. Tutkimus tehtiin kaksivaiheisena kvalitatiivisena tutkimuksena. Tutkimusmenetelmän tavoitteena oli pyrkiä uuden riskien arviointimallin luomiseen ja tämän validointiin.

7.1 Pohdinta

Tutkimuksen merkittävin tulos on Heräte -malli, joka on esitelty aiemmin tässä tutkimuksessa. Malli on tietoturvajohtajien näkemysten kautta muodostettu prosessimalli, jolle suoritettiin validointi kolmella suomalaisella asiantuntijalla: Jarno Limnéllillä, Mikko Siposella ja Kimmo Rouskulla. Heräte -mallin muodostuminen ja aiemmin kuvattu muodostumisen prosessi itsessään kuvaavat, miten tutkimuksen tulosten kautta on päädytty kyseiseen malliin eli toisin sanoen pohdinnan mallin muodostamiseksi. Tutkimusmenetelmän valinta tuki tutkimuksen tavoitetta. Tutkimuksen laatua ja luotettavuutta lisättiin suorittamalla asiantuntijavalidointi. Heräte -malli esiteltiin kolmelle asiantuntijalle ennen pro gradu -seminaaria. Asiantuntijoilta saatiin tukea mallin toimivuudelle sekä korjausehdotuksia. Palaute asiantuntijoilta otettiin vakavasti ja tarvittavat muutokset tehtiin.

Tutkimusaiheen rajaus nähtiin tutkimuksen aikana erittäin onnistuneeksi. Finanssialan tietoturvajohtajat toivat tutkimukseen tämän päivän näkemyksen riskien arvioinnin parhaista käytänteistä ja kehittämistarpeista. Finanssialan toimintaympäristö on suurelta osin digitaalinen ja sen toiminta on täysin riippuvainen tietoliikenneyhteyksistä ja sähköstä. Finanssialalla on lisäksi parhaat tilastot riskien arviointiin liittyvistä ilmiöistä, kuten kyberrikollisuudesta (McAfee Labs, 2014) ja yleisesti vakuuttamisesta (Hamilton, 2015). Finanssiala on lisäksi tarkoin säädelty ja alalla kiinnitetään erityistä huomiota riskeihin. Rajauksen kautta pyrittiin löytämään käytänteitä, joita on mahdollista hyödyntää myös finanssialan ulkopuolella. Heräte -riskien arvioinnin prosessimalli on täs-

tä erinomainen esimerkki. Tulevaisuuden sovellukset riskien arvioinnin osalta vaativat poikkitieteellistä ja organisaatioiden rajat ylittävää yhteistyötä.

Tutkimuksessa pyrittiin vastaamaan seuraavaan kysymykseen:

Miten riskien arvioinnin prosessi tulisi suorittaa tietoturvallisuusjohtajien näkökulmasta, jotta se tukisi organisaation menestystä?

Tutkimuksen tarkoituksen selkeyttämiseksi ja tutkimuksen kannalta soveltuvien haastateltavien rekrytoinnin helpottamiseksi tutkimusta lähestyttiin seuraavan apukysymyksen kautta:

Miten riskien arvioinnin tulokset vaikuttavat organisaation tietoturvapolitiikan/tietoturvaperiaatteiden laadintaan?

Tutkimuskysymykset laadittiin niin, että tutkimuskysymyksiä edelleen tarkentamalla on mahdollista rakentaa yhteys organisaation strategiasta aina yksittäisiin toimenpiteisiin. Kysymys siitä "Miten riskien arvioinnin prosessi tulisi suorittaa tietoturvallisuusjohtajien näkökulmasta, jotta se tukisi organisaation menestystä?" tähtäsi mallin rakentumiseen, eikä niinkään tyhjentävien vastausten antamiseen siitä, miten riskien arviointi tulisi suorittaa, jotta organisaatio menestyisi. Riskien arviointimallista edelleen muodostettava tarkempi riskien arvioinnin menetelmä laaditaan mallin kaltaisesti aina organisaatiokohtaisesti. Tietylle organisaatiolle laadittu menetelmä olisi rajannut mallin käytettävyyttä ja syvempi ymmärrys erilaisten organisaatioiden ja organisaation eri tasojen välisestä kanssakäymisestä olisi jäänyt huomattavasti heikommaksi. Riskien arvioinnin vaikutus tietoturvapolitiikan muodostumiseen auttoi sekä tutkijoita että haastateltavia jäsentämään tutkimuksen varsin laajaa aihetta ja muodostamaan näkemystä mihin tutkimuksella on tarkoitus vastata. Toisin sanoen riskien arvioinnin prosessin tutkiminen vailla varsinaista konkreettista päämäärää olisi ollut huomattavasti hankalampaa. Tutkimuksen alussa esitettyjen tutkimuskysymysten pohjalta rakennettiin riskien arvioinnin prosessimalli. Heräte -riskien arvioinnin prosessimalli esiteltiin aiemmin omassa luvussaan. Tutkimuskysymysten osalta voidaan lyhyesti todeta, että tavoite saavutettiin muodostamalla riskien arvioinnin prosessimalli. Asiantuntijoiden arvion perusteella malli on geneerinen malli riskien arvioinnin suorittamiseen. Asiantuntijoiden mukaan Heräte -malli antaa vastauksen prosessin suorittamiseen. Apukysymyksenä tutkimuksessa käytettiin riskien arvioinnin vaikutusta tietoturvapolitiikan laadinnassa. Haastatteluissa organisaatiot kuvasivat, mikä tietoturvapolitiikan rooli organisaatiossa on, miten tietoturvapolitiikka rakentuu ja miten riskien arviointi vaikuttaa tietoturvapolitiikan laadintaan. Tietoturvapolitiikkaan liittyvän apukysymyksen osalta tutkimustulokset ovat jo itsessään oman tutkimuksensa arvoisia.

7.1.1 Johtopäätökset tutkimuksen ja teorian kannalta

Tässä luvussa kuvataan tarkemmin tutkimusta teoreettisen viitekehyksen kannalta. Jo tutkimuksen alkuvaiheessa tutkimuksen teoreettiseen viitekehykseen pyrittiin löytämään laadukkaita, arvostetuissa julkaisuissa julkaistuja tieteellisiä artikkeleita. Mallin muodostamisen kannalta tieteelliset artikkelit eivät antaneet riittävää laajuutta tutkimuksen taustaan liittyen, joten jo varsin varhain tiedonhakua laajennettiin myös luokiteltujen artikkeleiden ulkopuolelle. Tutkimuksen tuloksena pyrittiin muodostamaan uusi malli, joka tukeutuu varsin vahvasti organisaatioiden käytäntöön. Kunnianhimoisena tavoitteena oli malli, jota voidaan aidosti hyödyntää organisaatioissa. Muodostetun Heräte -mallin perusrakenne muodostui tieteellisten artikkeleiden ja kirjallisuuden, standardien, vaihtoehtoisten menetelmien ja käytännön kautta. Ainoastaan joko käytäntöön tai tieteellisiin julkaisuihin perustuva malli olisi rajannut pois tärkeän tiedon lähteen.

Tutkimuksen haastatteluissa kävi ilmi, että organisaatiot tukeutuvat varsin vähän varsinaiseen tutkimustietoon. Organisaatiot pyrkivät hyödyntämään regulaation ja lainsäädännön asettamissa rajoissa parhaita käytänteitä jokapäiväisessä työssään. Organisaatiot käyttävät muun muassa tutkimuksesta johdettuja standardeja, mutta edelleen soveltavat niitä oman tarpeensa mukaan.

Porter (1979) kirjoittaa tutkimuksessaan, että organisaatioiden tulisi välttää toimintansa analysoinnissa staattisia menetelmiä. Nykyisin käytössä olevat riskienhallinnan ja -arvioinnin menetelmät eivät aina kykene huomioimaan tätä tulevaisuudessa yhä enemmän korostuvaa haastetta. Tässä tutkimuksessa muodostettu riskien arvioinnin malli pyrkii vastaamaan tähän tarpeeseen ja tuomaan riskien arvioinnin alueelle uutta, useasta lähteestä yhdistettyä ja analysoitua tietoa. Tässä suhteessa voidaan sanoa, että tämä tutkimus tarjoaa tieteellisen tutkimuksen kautta muodostetun käytännöllisen riskien arvioinnin prosessimallin, joka osaltaan täyttää myös riskien arvioinnin teoreettisessa tutkimuksessa olevaa aukkoa.

Tutkimuksen teoriassa kuvattiin, miten Rasmussen ehdottaa tutkimusta muun muassa ihmisille luontaisen päätöksenteon toimintatavoista muutoksen ja paineen alla, vaaraa aiheuttavien tapahtumien luokittelun ja näiden hallinnan sekä yhteiskunnan toimijoiden välisen yhteistoiminnan osalta. (Rasmussen, 1997). Tutkimus pyrkii kehittämään riskienhallintaa ja -arviointia entistä monitieteellisempään suuntaan siten, että riskien arviointi ja analysointi tapahtuisi enemmän organisaatiota osallistavalla tavalla hyödyntäen laajemmin koko organisaation osaamisen rajatun turvallisuushenkilöstön lisäksi. Muodostettu Heräte -malli ottaa osaltaan kantaa Rasmussenin näkemykseen monitieteellisestä päätöksenteosta, joka osallistaisi organisaation henkilöstä asiantuntijoita laajemmin. Tämä tutkimus vahvistaa Rasmussenin (1997) näkemystä. Organisaatioiden haastattelujen kautta näkemys holistisesta näkökulmasta riskien arvioinnin suorittamiseen kasvoi. Soomron (2016) mukaan tietoturvallisuuden johtaminen tarvitsee kokonaisvaltaisempaa eli *holistista* näkemystä. Tämä edelleen tukee näkemystä prosessien yhtenäistämisestä organisaatioissa.

Shameli-Sendi ym. (2016) muodostaman informaatioturvallisuuden riskien arvioinnin taksonomian mukaan organisaatioiden tulisi pystyä tunnista-

maan omat tarpeensa sen suhteen, mitä he odottavat saavansa arviointiprosessin kautta. Shameli-Sendi ym. (2016) listaavat tutkimuksessaan muodostamansa taksonomian mukaisesti erilaisten tapojen etuja ja haittoja. Muodostettua Heräte -mallia on sen yleisyydestä johtuen vaikea sijoittaa kyseiseen taksonomiaan. Muodostettu riskien arvioinnin malli tarjoaa organisaatioille laajemman viitekehyksen, jonka kautta he voivat muodostaa omiin tarpeisiinsa soveltuvan menetelmän. Tarkempaa menetelmää muodostettaessa Shameli-Sendi ym. (2016) taksonomia tarjoaa selkeän jaon ohjaamaan prosessia haluttuun suuntaan.

Aiemmat riskien arviointiin tai turvallisuuspolitiikoiden muodostamiseen liittyvät tutkimukset eivät tuo selkeästi ilmi tarvetta aktiiviselle toimintaympäristön seuraamiselle ja analysoinnille. Tässä tutkimuksessa muodostettu Heräte -malli tuo tälle alueelle uutta tietoa, jonka avulla organisaatiot pystyvät kehittämään toimintaansa siihen suuntaan, että toiminnan analysointi olisi koordinoidumpaa, henkilöstön osallistaminen koko prosessiin olisi laajempaa ja tiedonhankinta olisi mahdollisimman aktiivista ja ennakointiin pyrkivää.

Knapp ym. (2009) ja Karyda ym. (2005) kuvaavat tutkimuksissaan turvallisuuspolitiikoiden muodostamisprosessia. Turvallisuuspolitiikoiden kuten tietoturvallisuuspolitiikan muodostumisen taustalla olevan tiedon keräämisessä käytetään tutkimusten mukaan havaintoja ympäröivästä maailmasta. Organisaatioiden haastattelut ja tutkimustieto, kuten Borum ym. (2015), kuvaavat staattiset mallit vanhentuneiksi. Nykyaikaisen riskien arviointiprosessin tulee entistä aktiivisemmin pyrkiä keräämään tietoa omasta toimintaympäristöstään. Organisaatioissa aktiivinen tiedon kerääminen on ennen kaikkea mahdollisuus. Aiemman tieteellisen tutkimuksen tarjoamat mallit ja teoria riskien arviointiin tai turvallisuuspolitiikan laatimiseen (mm. Karyda ym., 2005; Knapp ym., 2009) tarjoavat selkeät perusteet prosesseille, mutta nekään eivät huomioi nopeasti muuttuvan toimintaympäristön asettamia vaatimuksia.

Tutkimuksessa lähestyttiin teknologian ja ihmisen välistä vuorovaikutusta useasta eri näkökulmasta. Organisaatiokulttuuri määriteltiin osana tutkimuksen tärkeimpiä käsitteitä. Turvallisuuskulttuuri on osa organisaation kulttuuria. Adamsin ja Sassen (1999) ja Karyda ym. (2005) mukaan henkilöstön sitoutuminen turvallisuustoimiin lisää sekä tietoisuutta, että kehittää turvallisuuskulttuuria. Adamsin ja Sassen (1999) mukaan on olemassa tietoa, että useat käyttäjä eivät noudata turvallisuusohjeita ja -sääntöjä. Organisaatioiden haastatteluissa monimutkaiset ja hankalasti ymmärrettävät ohjeet ovat suuri este henkilöstön sitouttamiselle koko organisaation yhteiseen turvallisuustoimintaan. Tutkimus tukee näin ollen Adamsin ja Sassen (1999) ja Karydan ym. (2005) näkemystä turvallisuuskulttuurin kehittymisen esteistä.

Spears ja Barki (2010) mukaan käyttäjät pystyvät tuomaan lisäarvoa organisaation tietojärjestelmien turvallisuuden suunnittelussa, analyysissa ja testauksessa, koska samalla tietoisuus mahdollisista uhkista lisääntyy. Spears ja Barki (2010) tutkimuksen tuloksia voidaan tarkastella laaditun Heräte -mallin kautta. Organisaatioiden määrällisesti suurin tietojärjestelmien loppukäyttäjäryhmä on oma henkilöstö. Riskien arvioinnin osalta suurin ympäröivästä maailmasta havaintoja tekevä ryhmä on henkilöstö. Organisaatioiden haastattelujen perusteella henkilöstö on toistaiseksi huonosti hyödynnetty voimavara riskien arvioinnissa. Useissa organisaatioissa on kokeiltu erilaisia osallistamismalleja,

mutta täysin toimivaa keinoa kerätä riskien arvioinnin perusteena olevaa tietoa ei ole pystytty toistaiseksi kehittämään. Haastatteluissa todettiin muun muassa, että varma keino saada riskien arviointi osaksi henkilöstön mielenkiintoa on sisällyttää riskien havainnointi osaksi toimenkuvia. Riskien arvioinnin ei haastattelujen perusteella koeta kuuluvan osaksi työtehtäviä, joten tulokset ovat näin ollen vaatimattomia ja riskien arvioinnissa ei kyetä hyödyntämään suurinta havaintoja tekevää ryhmää. Organisaatioilla on tahtoa hyödyntää henkilöstön piileviä voimavaroja, mutta keinot ovat toistaiseksi kehittymättömiä.

Tämä tutkimus ja muodostettu riskien arvioinnin prosessimalli tuovat kontribuutiota käytännön lisäksi myös teorian ja tutkimuksen kannalta. Aiempi tutkimus on jättänyt tilannekuvan hankkimisen ja ylläpitämisen liian pieneen rooliin. Tämä tutkimus pyrkii osoittamaan muun muassa aktiivisen tiedonhankinnan merkityksen tilannekuvan rakentamisessa. Nykyhetkessä hankittu laaja-alainen tieto voi osoittautua arvokkaaksi tekijäksi tulevaisuuden päätöksiä tehtäessä. Aiemmassa ja tutkimuksessa ja teoriassa ei ole kovin selkeästi osoitettu digitaalisen toimintaympäristön nopeasti tapahtuvien muutosten mukanaan tuomaa vaatimusta kyvystä nopeaan reagointiin ja dynaamiseen riskienhallintaan. Tämä kuitenkin oli selkeästi esiin tuotu tarve empiirisen aineiston kautta. Tämä tutkimus hahmottaa tämän tarpeen ja pyrkii myös antamaan siihen ratkaisun.

Myös luvussa 7.3 esitettävät jatkotutkimusaiheen pyrkivät osoittamaan tämän tutkimuksen teoreettista kontribuutiota esittämällä konkreettisia jatkotutkimusaiheita, joiden kautta on mahdollista vastata havaittuihin aukkoihin tutkimuksen ja teorian alueella.

7.1.2 Johtopäätökset käytännön kannalta

Tutkimuksen tavoitteena oli vastata nykyajan nopeasti muuttuvan digitaalisen toimintaympäristön asettamaan haasteeseen muodostamalla dynaaminen riskien arvioinnin prosessimalli. Muodostetun mallin avulla tavoitteena oli tarjota organisaatioille käytännön työkalu, jonka avulla ne voisivat muuttaa riskien arviointia entistä dynaamisempaan ja proaktiivisempaan suuntaan.

Mallin validointiin liittyvissä asiantuntijahaastatteluissa esiin nousi esiin riskienhallintaan, strategiaan ja kyberturvallisuuteen liittyvä ristiriita. Asiantuntijoiden kommenttien mukaan riskienhallintaa käsitellään usein pääasiassa strategisella tasolla. Kyberturvallisuutta käsitellään usein lähempänä käytännön tasoa, eli niin sanotulla teknis-taktisella tasolla. Nykyajan organisaatiot ovat yhä enemmän riippuvaisia digitaalisen toimintaympäristön toimivuudesta, joten kyberturvallisuuden voidaan sanoa olevan organisaatioille ennen kaikkea strateginen kysymys. Jos kyberturvallisuuden ja riskienhallinnan lähestymisen näkökulmissa on merkittävä ristiriita, niin toimivatko ne samoilla periaatteilla kohti yhteistä päämäärää? Tässä tutkimuksessa muodostettu riskien arvioinnin malli antaa organisaatioille keinon arvioida omaa toimintaansa aktiivisesti niin heikkouksien kuin vahvuuksienkin näkökulmasta. Muodostettu malli on lähtökohtaisesti strategisen tason malli. Organisaation arvioidessa omaa toimintaansa edellä mainitun kaltaisesti sekä riskien että vahvuuksien kannalta, tulevat

myös kyberturvallisuuteen liittyvät näkökulmat käsiteltyä strategisen näkökulman kannalta sen sijaan, että keskityttäisiin liikaa teknis-taktiseen tasoon. Muutoksen ja vaikuttamisen tulee lähteä liikkeelle ennen kaikkea strategiselta tasolta.

Heräte-mallin käytettävyyttä voidaan pohtia useasta näkökulmasta. Malli on visuaalisesti aina jossain määrin tekijöidensä näköinen, joten siihen ei ole tarvetta sen laajemmin puuttua. Mallia validoitaessa asiantuntijat näkivät mallin varsin "geneerisenä" yleisen tason mallina, jota on mahdollista käyttää varsin laajasti erilaisia (riskejä) sisältäviä päätöksiä tehtäessä. Käytännön kannalta voidaan todeta, että tavoitteeseen on osittain päästy. Tarkoitus on ollut muodostaa helposti omaksuttava ja käytettävä malli, joka ei nopeissakaan tilanteissa vaadi liian syvällistä koulutusta. Muodostettu Heräte -malli (kuvio 13) on mahdollista suorittaa pelkästään mallin kuvaa tarkastelemalla ilman erillistä koulutusta.

Tutkimuksen aikana saatiin riskien arvioinnin prosessin lisäksi vastauksia finanssialan organisaatioiden tietoturvapolitiikan muodostumisessa. Pääosassa organisaatioita tietoturvapolitiikka koettiin strategisen tason ohjauksen antavaksi asiakirjaksi. Lähtökohtaisesti tietoturvapolitiikkaa tai sen laatimista ei koettu niin ongelmaksi käytännön toiminnassa kuin haastateltavien kuvaama aikaisempi tutkimus muun muassa suomalaisissa yliopistoissa osoittaa.

Tutkimuksen alussa kuvattiin muun muassa Juha Sipilän hallituksen strategisen hallitusohjelman, VTT:n laatiman ja Valtioneuvoston kanslian helmikuussa 2016 julkaiseman "Kyberosaaminen Suomessa - Nykytila ja tiekartta tulevaisuuteen" -tutkimuksen, Sisäministeriö julkaiseman ensimmäisen Valtioneuvoston selonteon sisäisestä turvallisuudesta 19.5.2016 sekä lisäksi yleisesti digitaalisen toimintaympäristön merkitystä organisaatioiden toimintaan. (Valtioneuvoston kanslia, 2015; Sisäministeriö, 2016b; VTT, 2016). Kaikille edellä kuvatuille raporteille yhteistä on tarve muuttaa aikaisempia toimintamalleja digitalisaation lisääntyessä. Olennaista on ilmiön ymmärtäminen omaa toimintaympäristöä laajemmin. Tutkimuksessa on pyritty viranomaisten ja erilaisten konsulttiyritysten raporttien kautta kuvaamaan digitalisaation kehityssuuntia, jotta ilmiöstä on mahdollista saada kattavampi kuva. Raporttien perusteella koko yhteiskunnan toiminta on yhä enemmän riippuvainen digitaalisten palveluiden toimivuudesta ja riippuvuus kasvaa entisestään verkkoon liittyvien ihmisten ja laitteiden määrän kasvaessa. Tutkimuksessa on myös pyritty tuomaan näkökulmana organisaation riskien hallinnan toimenpiteiden ja resurssien suuntaamiseksi juuri organisaation kannalta keskeisimpiin riskeihin. Kaikkiin organisaatioiden toimintaympäristössä ilmeneviin riskeihin ei löydy aina välittömästi ratkaisua. Riskien arviointi on myös aina arvio. Mannermaa (2008) mukaan tulevaisuuden yhteiskunnassa pärjäävät henkilöt, jotka pystyvät tekemään päätöksiä keskittyen olennaiseen. Samankaltaista ajattelumallia soveltavat Killingin ja Malnightin (2005) Must Win Battles -strategiaopissa. Kyseisessä strategiaopissa valitaan organisaation kannalta keskeisiä alueita ja luodaan toimintatapoja, joilla suunnataan organisaation resursseja päämäärän kannalta tärkeimpiin ja olennaisiin asioihin. Organisaation kannalta menetelmä yksinkertaistaa toimintamalleja ja auttaa keskittymään ennalta määriteltyihin kehittämistoimenpiteisiin, koska aktiivisessa seurannassa olevat painopistealueet on

valittu. Asiaa tulee edelleen tutkia, mutta tutkimuksessa nousi edelle juuri kompleksisuudesta ja resurssien rajallisuudesta johtuva riskien arvioinnin suuntaaminen painopistealueille. Vaikka riskien arviointia tulee tehdä laajasti, on organisaatioissa muun muassa työpajojen ohjauksen kautta saatu hyviä kokemuksia resurssien suuntaamisesta oikeisiin asioihin. Tämä näkyi myös osassa organisaatioissa tietoturvapolitiikan ollessa osa strategisten painopistealueiden toteuttamista.

7.2 Tutkimuksen luotettavuuden ja rajoitteiden arviointi

Tuomen ja Sarajärven mukaan merkittävä hyvän tutkimuksen kriteeri on tutkimuksen sisäinen johdonmukaisuus. Tutkijan on huolehdittava muun muassa, että tutkimussuunnitelma on laadukas, valittu tutkimusasetelma on sopiva ja että raportointi on tehty hyvin. Hyvää tutkimusta ohjaa eettinen sitoutuneisuus eikä ainoastaan tarkistuslistan mukaiset mallit. (Tuomi & Sarajärvi, 2009). Laadullisen tutkimuksen tulokset ovat suuresti riippuvaisia tutkijan omista päätelmistä. Tämä tutkimus on tehty parityönä, joten kaikki tutkimuksessa tehdyt valinnat ovat kahden eri henkilön yhteisen päätöksen tuloksia. Tutkimuksen yleisen luotettavuuden voidaan ajatella lisääntyneen, koska kaikki merkittävät päätökset ovat vertaisarvioituja tutkijoiden kesken.

Hirsjärven ja Hurmeen (2001) mukaan reliabiliteetin ja validiteetin käsitteitä tulisi käsitellä lähinnä määrälliseen tutkimukseen liittyen. Heidän mukaansa nämä käsitteet liittyvät eksaktiin mittaamiseen ja laadullisessa tutkimuksessa näistä käsitteistä voitaisiin luopua. Hirsjärven ja Hurmeen (2001) mukaan edellä mainitut käsitteet perustuvat siihen ajatukseen, että "tutkija voi päästä käsiksi objektiiviseen todellisuuteen ja objektiiviseen totuuteen". Tämän tutkimuksen luotettavuutta on pyritty lisäämään siten, että tutkimusraportin tarkoitus on kuvata koko tutkimusprosessin kulku ja tehdyt valinnat mahdollisimman tarkasti. Tähän kuvaukseen on pyritty kuvaamalla koko prosessi loogisesti aloittamalla tutkimuksen taustan, rajausten ja näkökulman kuvaamisesta. Käsitteiden ja teoreettisen viitekehyksen kuvaamisen kautta raportti pyrkii avaamaan lukijalleen vaiheittain koko tutkimuksen toteuttamisen prosessin siten, että lukija pystyisi saamaan kattavan käsityksen siitä, mitkä tekijät tieteellisessä teoriassa, valituissa standardeissa ja haastatteluaineistossa ovat vaikuttaneet mallin muodostumiseen. Tutkimusraportin on tarkoitus olla looginen ja vaiheittainen kuvaus tutkimustulosten, eli käytännössä muodostetun mallin, rakentumisesta. Hirsjärvi ym. (2002) kirjoittavat, että laadullisen tutkimuksen ei tulisi painottua ainoastaan tehdyn tutkimuksen jälkiselostukseen, vaan sen tulisi olla pelkän selostuksen lisäksi analyysiä tutkittavasta ilmiöstä. Tämän analyysin kautta tutkijan kuuluu kirkastaa näkemystään lukijalle ja pyrkiä induktiiviseen tutkimusotteeseen, jossa päädytään yksityisistä havainnoista yleisempiin merkityksiin. Tässä tutkimusraportissa on pyritty saavuttamaan edellä mainitut tavoitteet.

Aineiston analyysin osalta tutkijat käyttävät tässä raportissa suoria lainauksia haastatteluaineistosta. Sitaattien tarkoituksena on antaa lukijalle mah-

dollisuus arvioida tutkijoiden analyysiprosessia. Tätä pyrittiin tukemaan myös teemoittain esitettävillä koonnostaulukoilla, joista on mahdollista saada kokonaiskuva tutkimukseen osallistuneiden organisaatioiden vastauksista tutkittaviin aiheisiin liittyen.

Tutkimuksen näkyvin tulos on muodostettu riskien arvioinnin malli. Raportin tavoitteena on tuoda lukijalle näkyviksi ne seikat, mitkä ovat vaikuttaneet mallin muodostumiseen. Raportti pyrkii perustelemaan mallin muodostamiseen vaikuttaneet valinnat tieteellisen teorian, valittujen riskienhallinnan ja tietoturvallisuuden standardien, kirjallisuuden ja haastatteluaineiston kautta. Lisäksi malli on validoitu ja siihen on pyydetty palautetta kolmelta asiantuntijalta. Asiantuntijoiden kommentit on otettu huomioon muokattaessa mallia lopulliseen muotoonsa. Asiantuntijoiden ehdotukset mallin kehittämisessä sisältyy tähän tutkimukseen.

Tutkimuksessa muodostettu riskien arvioinnin malli on rakennettu tietoturvajohtajan näkökulmasta ja empiirinen aineisto on kerätty finanssialan organisaatioista. Tästä huolimatta mallista on pyritty tekemään näkökulmaansa ja aineistoansa yleiskäyttöisempi niin, että sen käyttömahdollisuudet ulottuisivat myös finanssialaa tai tietoturvallisuutta laajemmalle. Edellä mainitut rajaukset ja valinnat on kuitenkin syytä huomioida mallin laatua ja luotettavuutta arvioitaessa.

Tutkimuksen luotettavuutta pyritään parantamaan monitriangulaation keinoin. Triangulaatiolla tarkoitetaan (Tuomi & Sarajärvi, 2009; Hirsjärvi ym., 2000) laadullisen tutkimuksen teossa menetelmien yhteiskäyttöä. Monitriangulaatio on erotettu omaksi tyypikseen, jossa käytetään yhtä tai useampaa triangulaation päätyyppiä. (Tuomi & Sarajärvi, 2009; Denzin, 1978). Monitriangulaatio pyrittiin täyttämään tutkija-, aineisto- ja teoriatriangulaation keinoin. Koko tutkimusprosessiin osallistui kaksi tutkijaa (tutkijatriangulaatio), mallin muodostamisen aineistona on käytetty muun muassa standardeja (aineistotriangulaatio), tieteellistä tutkimusta ja haastatteluaineistoa ja tutkimuksen näkökulmia on pyritty löytämään monipuolisesti eri tieteenaloilta (teoriatriangulaatio).

Tutkimuksen toteuttamisen kuvaamisen yhteydessä tuotiin esille Myersin ja Newmanin (2007) kuvaamat ongelmat, jotka antavat mahdollisuuden tarkastella omaa suoriutumista haastatteluissa ja tätä kautta tutkimusten luotettavuutta. Tutkimuksen toteuttamisessa koettiin eduksi kahden tutkijan käyttö niin haastatteluihin valmistautumisessa, haastattelujen suorittamisessa kuin haastattelumateriaalin analysoinnissa. Tutkimuksen kohderyhmänä oleviin organisaatioihin saatiin luotua luottamukselliset välit ja rekrytointi saatiin tehtyä varsin lyhyessä ajassa. Myersin ja Newmanin (2007) mukaan ongelmia voi syntyä haastateltavan ajan puutteen vuoksi. Kahdessa tapauksessa haastattelun ajankohtaa siirrettiin haastateltavan ilmoittaman esteen vuoksi. Kaikki sovitut haastattelut saatiin lopulta tehtyä. Haastatteluissa haettiin vastauksia oikealta organisaation tasolta. Saatekirjeessä (liite 1) tosin myös mainittiin etsityn henkilön ominaisuuksista. Kaikilla haastatelluilla oli riittävät tiedot liiketoiminnan ja riskienhallinnan rajapinnassa toimimisesta, joka näkyi vastausten laadussa. Haastatelluilla oli näkemystä niin johtoryhmätyöskentelystä kuin operatiivisesta toiminnasta. Haastattelut käytiin hyvässä yhteisymmärryksessä ja haastattelurungon läpikäymisen jälkeen keskustelua jatkettiin aiheesta.

Tutkimuksen toteutukseen sisältyy myös rajoitteita. Empiirinen aineisto kerättiin finanssialan organisaatioista, joten sen osalta tutkimustulosten taustalla vaikuttavat näkemykset edustavat vain yhtä alaa. Finanssiala on riskienhallinnan kuin kyberturvallisuuden osalta ala, joka on vahvan regulaation alla. Tämä vaikutti siihen, että aineisto päätettiin kerätä juuri finanssialalta. Näkemykset empiirisen aineiston osalta siis edustavat yhtä alaa, mutta ovat monessa mielessä edelläkävijöiden tietoon perustuvia. Tutkimuksen tuloksena muodostettu malli on pyritty muodostamaan yleisemmäksi, että se olisi edellä mainitusta rajoituksestaan huolimatta käyttökelpoinen myös finanssialan ulkopuolella.

Tutkimuksen otanta oli ensimmäisessä vaiheessa yhteensä kuusi organisaatiota ja yhdeksän haastateltavaa ja toisessa vaiheessa kolme asiantuntijaa. Jos tutkijoiden käytössä olisi ollut enemmän resursseja, etenkin ajan suhteen, olisi otantaa voitu kasvattaa kummankin haastattelukierroksen osalta. Tästä huolimatta tutkijat kokevat, että tutkimuksen otanta antoi riittävän materiaalin mallin muodostamiseksi. Suurempi otanta olisi myös saattanut lisätä tutkimuksen luotettavuutta. Muun muassa kahden tutkijan käyttäminen ja mallin validointi koetaan kuitenkin tekijöinä, jotka osaltaan lisäävät tutkimuksen luotettavuutta pienehköstä otannasta huolimatta.

Muodostetun mallin yleisyys voidaan lukea toisaalta rajoitteeksi, mutta toisaalta eduksi. Tutkimuksen tarkoitus ei ollut muodostaa yksityiskohtaista, kontekstisidonnaista mallia, vaan tarjota yleisempi työkalu riskien arvioinnin ja organisaation toiminnan tason analysoimisen tueksi. Organisaatioiden ottaessa muodostetun mallin käyttöön, tulisi heidän aina muokata se tarkemmalle tasolle ja omiin työtapoihinsa ja resursseihinsa sopivaksi. Rajoitteistaan huolimatta tutkimuksen olennaisin tulos, eli muodostettu riskien arvioinnin prosessimalli on käyttökelpoinen myös tutkimuksen kohderyhmän ulkopuolella. Mayry (2016) on tutkinut organisaatioiden strategioiden omaksumista toiminnan eri tasoilla. Yhtenä keskeisenä tuloksena on se, että henkilöstö tuntee strategian kohtuullisen huonosti. Tämä havainto tukee osaltaan sitä, että käytettävien menetelmien tulisi olla mahdollisimman yksinkertaisia ja yleiskäyttöisiä.

Tutkimuksessa Heräte -riskien arviointimallin käytettävyyttä arvioitiin teoreettisesti asiantuntijoiden toimesta. Jatkotutkimuksessa mallin käytettävyyttä tulisi arvioida käytännössä osana organisaatioiden toimintaa.

7.3 Jatkotutkimusaiheet

Tutkimuksen aikana löydettiin jatkotutkimukseen soveltuvia aihealueita. Aihealueet, joihin olemme listanneet jo osittain käsiteltyjä otsikoita ja selostuksia, ovat listattuna tämän kappaleen jälkeen. Jatkotutkimuksen aiheet perustuvat organisaatioissa jo tunnistettuihin kehittämiskohteisiin ja -tarpeisiin. Kehittämiskohteita on pyritty huomioimaan laajasti yli tieteenalojen rajojen. Ehdotetut aiheet ovat kytkettävissä tiukasti kyberturvallisuuteen kontekstiin, mutta useimmat niistä antavat mahdollisuuden myös laaja-alaisempaan ja poikkitieteellisempään aiheen käsittelyyn.

1. Riskien arviointi turvallisuuden ohjauksessa (ohjaustyökaluna)

Teeman 2 käsittelyn yhteydessä esille nousi riskien arvioinnin kannalta mielenkiintoinen ilmiö. Organisaatio D:ssä kuvattiin riskien arvioinnin käyttöä turvallisuuden ohjaustyökaluna. Lyhyesti kuvattuna ilmiö tarkoittaa, että riskien arvioinnin suorittava toimija nostaa tarkoituksellisesti riskien arvioinnin tuloksena olevia numeerisia arvoja (kuten asteikon 1-5 arvoja), jotta toimijan näkökulmasta merkityksellinen toimenpide saadaan hyväksytettyä organisaation johdossa. Tällöin riskien arvioinnin tulokset eivät ole vertailtavia alkuperäisessä merkityksessään, koska arvioihin vaikuttaa myös arvioitsijan henkilökohtainen näkemys aiempaa enemmän. Asiantuntijahaastatteluiden yhteydessä Mikko Siponen kertoi, että tutkimuksessa esille noussut riskien arviointi turvallisuuden ohjaustyökaluna on tutkimusaiheena mielenkiintoinen:

> ...muun muassa siltä osin, että "kuinka monessa yrityksessä riskien arviointia vääristellään tahallaan". Siponen on miettinyt miten johto voi kyseenalaistaa asiantuntijan näkemyksen: "kun tää riskianalyysi perustuu subjektiivisuuteen ja voi olla, että riskianalyysin tekijällä on esittää myös joitain lukuja johdolle niin se johto voi kysyä sitä evidenssiä, mutta eihän niitä ole tavallaan, mutta ei niillä ole sitä substanssitietämystä, että ne pystyis kyseenalaistamaan. Siponen miettii miten paljon asiantuntijat käyttää riskianalyysiä uhkien esille tuomiseen: "kuinka paljon tätä… asiantuntijat käyttää sitä riskianalyysiä , et miksi just uhkia… onks se sen takia et halutaan sitä kautta tuoda niitä uhkia esiin, koska se on se asia miksi joku johto saadaan, saadaan uskotettua johdolle, että tässä on tämmöinen uhka."

Mikko Siposen näkökulmasta kyseinen aihe on tällä hetkellä heikosti tunnettu tieteellisessä kirjallisuudessa.

2. Riskien arviointi osana organisaation menestystä liiketoiminnan johtajan näkökulmasta.

Riskien arviointi on organisaation strategian toteutumiseen ja menestykseen tähtäävä prosessi. Tutkimuksessa käsiteltiin tietoisesti riskien arviointia juuri tietoturvajohtajien näkökulmasta. Jatkotutkimuksessa on tärkeää selvittää miten liiketoiminnan johtajat, kuten organisaation ylin johto tai liiketoimintayksiköiden johtajat näkevät muodostetun Heräte -mallin käytettävyyden koko organisaation riskien arvioinnin prosessina.

3. Henkilöstön piilevät voimavarat riskien arvioinnin toteuttamisessa

Tutkimuksessa riskien arvioinnin tietoa ei merkittävästi kerätty organisaation suurimman tietopääoman haltijalta, organisaation henkilöstöltä. Riskien arviointi suoritetaan pääosin nimettyjen henkilöiden toimesta ja erikseen sovittuina ajankohtina. Aktiivisemman ja kattavamman tiedonkeruun kannalta koko henkilöstön kattava riskien arvioinnin perusteena käytettävän tiedon kerääminen on perusteltua. Tutkimukseen osallistuneissa organisaatioissa ei yhdessäkään todettu, että tietoa tulisi henkilöltä liikaa.

4. Menetelmä riskien arvioinnin formaalien tulosten tuottamiseksi

Tutkimuksen tavoitteena oli muodostaa riskien arvioinnin prosessimalli, jota on mahdollista käyttää organisaation kaikilla tasoilla. Prosessimalli antaa viitekehyksen toiminnalle, mutta ei toisaalta tuota itsessään formaaleja, määrämuotoisia, ja vertailtavia tuloksia. Riskien arvioinnin perusteena käytettävän tiedon tulisi sisältää mahdollisimman paljon määrällistä dataa tulosten tarkentamiseksi. Näin ollen mittarein tuetun menetelmän laatiminen organisaation eri tasoilla on perusteltua. On kuitenkin huomattava, että mittareiden tulee tuottaa nimenomaan vertailtavaa materiaalia.

5. Sovellus organisaation riskitiedon ilmoittamiseen

Tutkimuksessa ilmeni, että henkilöstön osallistamisessa riskitiedon ilmoittamiseen ja keräämisen on paljon kehitettävää. Riskitiedon ilmoittamiseen käytettävät työkalut ovat usein vaikeita käyttää ja niiden käyttöoikeudet saattavat olla rajoitetut hyvin pienelle joukolle. Yhtenä jatkotutkimusaiheena, tai jopa liikeideana, on helppokäyttöisen työkalun kehittäminen riskitietojen ilmoittamiseksi. Jos työkalu on riittävän helppokäyttöinen ja se on annettu laajan joukon käyttöön, pienenee kynnys riskitiedon ilmoittamiseksi huomattavasti. Työkalu voitaisiin kehittää esimerkiksi mobiiliapplikaation muotoon.

6. Tietoturvapolitiikan muodostamisprosessin (Knapp ym., 2009) käytettävyyden tarkastelu liiketoiminnan johtajan näkökulmasta

Tutkimuksessa ja Heräte -mallin rakentamisessa käytettiin apukysymyksenä tietoturvapolitiikan muodostumisprosessia. Tietoturvapolitiikan tulisi muodostua muun muassa riskien arvioinnin kautta. Tutkimuksessa tietoturvapolitiikan muodostumisen prosessimallina käytetään Knapp ym. (2009) laatimaa prosessimallia. Knapp ym. (2009) käytettiin ensimmäisen vaiheen haastatteluissa sen selvittämiseksi, onko mallin kuvaus liian yleinen. Tietoturvajohtajien näkökulmasta Knapp ym. (2009) ei ole liian yleinen. Mallin sisäisten ja ulkoisten vaikuttimen koettiin soveltuvan lisäksi riskien arviointiin. Jatkotutkimusta on mahdollista suunnata muun muassa liiketoimintajohtajille sen selvittämiseksi, onko Knapp ym. (2009) tietoturvapolitiikan muodostumisen prosessimalli liian yleinen kuten Alshaikh ym. (2015) kritisoivat tutkimuksessaan.

7. Organisaatioiden välisen riskitiedon jakamisen tehostaminen - nykytila ja mahdollisuudet / Regulaation ja lainsäädännön asettamat haasteet riskitiedon jakamisessa

Tutkimuksen tavoitteena oli osaltaan selvittää riskien arvioinnin perusteena käytettävän tiedon lähteitä. Haastattelujen perusteella organisaatioiden tulee omista lähtökohdistaan, erityisesti strategiaa tarkastellen, erottaa oleelliset tiedon lähteet toimintaympäristöstään ja pyrkiä aktiivisesti hankkimaan organisaation kannalta oleellista tietoa. Jatkotutkimuksen kannalta on mielenkiintoista

miten organisaatioiden välistä tiedonvaihtoa on lainsäädännön kannalta mahdollista toteuttaa. Yli organisaatiorajojen tapahtuva tiedonvaihto ja yhteistyö muiden toimintaympäristöön liittyvien toimijoiden kanssa ovat organisaatioiden keskeisiä menestystekijöitä

8. Riskienhallinnan toimenpiteiden vaikutusten arviointi

Riskien arvioinnin tulokset antavat osana riskienhallinnan prosessia tietoa organisaatiota uhkaavista riskeistä. Organisaatioille ei aina välttämättä ole täysin selvää, mihin riskien arvioinnin tulokset vaikuttavat ja millä tavalla. Riskien arvioinnin tulosten perusteella voidaan käynnistää toimenpiteitä, joilla pyritään saamaan vaikutusta havaittuihin riskeihin. Se, mitä vaikutusta näillä toimenpiteillä on, saattaa jäädä valvomatta.

Jatkotutkimusaiheena esitetään riskienhallinnan konkreettisten toimenpiteiden vaikutusten arviointia. Tutkimuksen tarkoituksena olisi tarkastella, miten valitut toimenpiteet todellisuudessa vaikuttavat havaittuihin riskeihin ja miten toimenpiteiden vaikutusten seurantaa voitaisiin parantaa.

9. Riskienhallinnan ja riskien arvioinnin opetus korkeakouluissa organisaatioiden (kuten finanssialan) tarpeiden näkökulmasta

Tutkimuksessa on hyvin voimakkaasti viitattu käytännön toimintatapoihin finanssialan organisaatioissa. Tutkimuksen haastatteluissa kerätty materiaali on tämän päivän kuvaus riskien arvioinnin prosessin hyvistä käytänteistä ja haasteista eri organisaatioissa (esimerkiksi finanssialalla). Tutkimusta tarkastelemalla on mahdollista vertailla korkeakouluissa tehtävää opetusta ja tutkimuksessa kuvattuja tarpeita.

10. Riskien arviointi digitaalisen liiketoiminnan kilpailukyvyn ja menestyksen mahdollistajana

Tutkimuksessa on laadittu riskien arvioinnin prosessimalli erityisesti tietoturvajohtajien näkökulmasta. Organisaation kannalta strategian toteutumiseen tähtäävät prosessit ja organisaation menestys ovat tärkeimpiä ominaisuuksia. Tutkimuksessa on merkittävästi painotettu organisaation menestyksen ja innovaatioiden luomisen tärkeyttä, jopa tutkimuksen pääotsikon kautta. Jatkotutkimuksen kannalta on erityisen tärkeää tunnistaa Heräte -mallin viitekehystä tarkentaen riskien arvioinnin mahdollisuudet organisaatioiden menestyksen ja innovaatioiden luomisen kannalta. Riskien arviointi tulee ymmärtää erityisesti menestyksen mahdollistajana eikä pelotteiden listaamisena.

11. Riskien analysoinnin työtapojen vertaileva tutkimus

Tässä tutkimuksessa ilmeni haaste liittyen riskien arvioinnin subjektiivisuuteen. Kahden eri kokoonpanon saamat riskien arvioinnin tulokset saattavat olla täysin toisistaan poikkeavat, vaikka ne käyttäisivät arvioinnin perusteena täsmälleen samaa dataa. Poikkeamat voivat selittyä muun muassa kokoonpanojen eroilla ja käytetyillä työtavoilla. Organisaatioiden tavoitteena tulisi kuitenkin olla vertailukelpoisen ja yhdenmukaisen aineiston tuottaminen. Tähän tavoitteeseen pääsemiseksi riskien arvioinnin työtapojen ja johtamisen tulisi olla mahdollisimman yhdenmukaista. Tähän voidaan pyrkiä esimerkiksi riittävän hyvin valmistellulla ja johdetulla työpajatoiminnalla.

Jatkotutkimusehdotuksena on vertaileva tutkimus siitä, miten paljon eri menetelmillä toteutetut riskien arvioinnin tulokset poikkeavat toisistaan ja miten riskien arvioinnin prosessia voitaisiin tehostaa ja yhdenmukaistaa.

LÄHTEET

Adams, A. & Sasse, M. (1999). Users are not enemy. Communications of the ACM, 42(12),41 - 46.

Ahteensuu, M. (2008). Riskianalyysi ja ennaltavarautumisen periaate. Haettu 9.6.2016 osoitteesta http://filosofia.fi/node/4062

Albrechtsen, E. (2007). A qualitative study of users´ view on information security. Computers & Security, 26(4), 276-289.

Al-Rodhan, N. (2015). Strategic Culture and Pragmatic National Interest. Global Policy.

Alshaikh, M., Maynard, S.B., Ahmad, A. & Chang, S. (2015). Information Security Policy: A Management Practice Perspective. Australasian Conference on Information Systems 2015. Haettu 22.2.2016 osoitteesta https://acis2015.unisa.edu.au/wp-content/uploads/2015/11/ACIS_2015_paper_49.pdf

Altman, Y. & Baruch, Y. (1998). Cultural theory and organizations: analytical method and cases. Organization Studies, 19(5), 769-785.

Amara, R. (1981). The Futures Field: Searching for Boundaries and Definition. The Futurist, 15, 25-29.

Ashton, K. (1999). That 'Internet of Things' thing. RFID Journal. Haettu 28.1.2016 osoitteesta http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

Bandyopadhyay K, Mykytyn P.P. & Mykytyn K. (1999). A framework for integrated risk management in information technology. Management Decision 1999, 37(5), 437.

Baskerville, R. (1989). Logical controls specification: an approach to information system security", teoksessa Klein, H. and Kumar, K. (ed). Systems Development for Human Progress. North- Holland, Amsterdam.

Baskerville, R. (1991), "Risk analysis: an interpretive feasibility tool in justifying information systems security". European Journal of Information Systems, 1(2), 121-130.

Baskerville, R. & Siponen, M. (2002). An information security meta-policy for emergent organizations. Logistics Information Management, 15(5 / 6) 337 - 346.

Bodin, L.D., Gordon, L.A. & Loeb, M.P. (2008). Information Security and Risk Management. Communications of ACM, 51(4), 64 - 68.

Borum, R., Felker, J., Kern, S., Dennesen, K. & Feyes, T. (2015). Strategic cyber intelligence. Information & Computer Security, 23(3), 317 - 332

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. (2009). If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. European Journal of Information Systems, 18(2), 151-164.

Boyd, A. (2016). DNI Clapper: Cyber bigger threat than terrorism. Federal Times, 4.2.2016. Haettu 10.2.2016 osoitteesta

http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-bigger-threat-terrorism/79816482/

Brehmer, B. (2005). The dynamic OODA loop: Amalgamating Boyd's OODA loop and the cybernetic approach to command and control. Proceedings of the 10th international command and control research technology symposium, 365-368.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awaraness. MIS Quarterly, Special Issue, 34(3), 523-548.

Capgemini Consulting & Sogeti High Tech. (2014). Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT. Haettu 26.1.2016 osoitteesta https://www.capgemini-consulting.com/resource-file-access/resource/pdf/securing_the_internet_of_things.pdf

Capgemini. (2015). Non-cash Transactions Globally & Regionally. World Payments Report. Haettu 2.2.2016 osoitteesta https://www.worldpaymentsreport.com/reports/noncash_inhabitant

Caralli, R.A, Stevens, J.F., Young, L.R. & Wilson, W.R. (2007). Introducing Octave Allegro: Improving the Information Security Risk Assessment Process. Software Engineering Institute, CERT Program. Carnegie Mellon University. Haettu 3.2.2016 osoitteesta ftp://ftp.sei.cmu.edu/pub/documents/07.reports/07tr012.pdf

Cederberg, A. (2015). Future Challenges in Cyberspace. GCSP Policy Paper 2015(4). Geneva Centre for Security Policy. Haettu 15.2.2016 osoitteesta http://www.gcsp.ch/News-Knowledge/Publications/Future-Challenges-in-Cyberspace

Cederberg, A. & Eronen, P. (2015). How are societies defended against hybrid threats. Strategic Security Analysis. Geneva Centre for Security Policies. Haettu 2.6.2016 osoitteesta http://www.gcsp.ch/News-Knowledge/Publications/How-are-Societies-Defended-against-Hybrid-Threats

Center for a New American Security. (2013). Active Cyber Defense. A Framework for Policymakers. Policybrief February 2013. Haettu 26.1.2016 osoitteesta http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf

Chang, S.E. & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345–361

CSBS. (2014). Cybersecurity 101: A Resource Quide for Bank Executives. Conference of State Bank Supervisors (Muokattu 15.12.2014). Yhdysvallat: Washington. Haettu 2.3.2016 osoitteesta https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf

Darke, P., Shanks, G. & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. Information Systems Journal 8(4), 273-289.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20(1), 79-98.

Deming. (2016). Deming -instituutin verkkosivut. Haettu 2.6.2016 osoitteesta https://www.deming.org/theman/theories/pdsacycle

Denzin, N.K. (1978). The research art. New York: McGraw-Hill.

Dhillon, G. (1997). Managing Information System Security. Lontoo: Macmillan.

Dhillon, G. & Backhouse, J. (2000). Information system security management in the new millennium. Communications of the ACM, 43 (7), 125–128.

Douglas, M. (1990). Risk as a Forensic Resource. Daedalus, 119(4).

Doz, Y. & Kosonen, M. (2008). Fast Strategy. How Strategic Ability Will Help You Stay Ahead of the Game. Harlow: Pearson Education.

EBA. (2016). Risk Assessment of the European Banking System, December 2015. European Banking Authority. Luxemburg: Publications Office of the European Union. Haettu 11.2.2016 osoitteesta http://www.eba.europa.eu/documents/10180/1315397/EBA+RISK+ASSESSMENT+REPORT.pdf/46d91b9a-f393-4b54-96eb-df06ca01bec5

Eisenhardt, K.M. (1989). Building theories from case study research. Academy of Management Review 14(4), 532-550.

Eisenhardt, K.M. & Graebner, M.E. (2007). Theory building from cases: Opportunities and challenges. Academy of Management Journal 50(1), 25-32.

ENISA. (2016). ENISA Threat Landscape 2015. European Union Agency for Network and Information Security. Julkaistu 27.1.2016. Haettu 10.2.2016 osoitteesta https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015

Ertaul, L., Braithwaite, T., & Bellman, B. L. (2005). Enterprise security planning (ESP). Teoksessa. Proceedings of EURO mGOV (Vol. 2005).

Eskola, J. & Suoranta, J.. (1996). Johdatus laadulliseen tutkimukseen. Rovaniemi: Lapin yliopisto.

Euroopan komissio. (2013). Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö. Yhteinen tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Euroopan unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja. Bryssel: Euroopan komissio.

Europol. (2015). The Internet Organised Crime Threat Assessment (IOCTA) 2015. Haettu 26.1.2016 osoitteesta https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015

FERMA. (2002). FERMA: A Risk Management Standard. Federation Of European Management Associations. Haettu 23.2.2016 osoitteesta http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-english-version.pdf

FERMA. (2016). Federation Of European Management Associations. Haettu 23.2.2016 osoitteesta http://www.ferma.eu/about/mission-and-objectives/what-is-ferma/

FIPS. (2006). Minimum Security Requirements for Federal Information and Information Systems.

Finanssialan Keskusliitto. (2014a). Pankit Suomessa 2014. Haettu 2.2.2016 osoitteesta https://www.fkl.fi/materiaalipankki/julkaisut/Julkaisut/Pankit_Suomessa_2014.pdf

Finanssialan Keskusliitto. (2014b). Vakuutusyhtiöt Suomessa 2014. Finanssialan Keskusliitto. Julkaisut ja tutkimukset 2015. Haettu 2.2.2016 osoitteesta https://www.fkl.fi/materiaalipankki/julkaisut/Julkaisut/Vakuutusyhtiot_Suomessa_2014.pdf

Finanssialan Keskusliitto. (2015). Pankkibarometri IV/2015. Haettu 2.2.2016 osoitteesta https://www.fkl.fi/materiaalipankki/julkaisut/Julkaisut/Pankkibarometri_IV_2015.pdf

Finanssialan Keskusliitto. (2016). Perustietoa Finanssialan Keskusliitosta. Haettu 2.2.2016 osoitteesta https://www.fkl.fi/tietoa_meista/Sivut/default.aspx

Frosdick, S. (1997). The techniques of risk analysis are insufficient in themselves. Disaster Prevention and Management: An International Journal, 6(3), 165 - 177.

Gartner Inc. (2014). Forecast : The Internet of things, Worldwide, 2013. Haettu 26.1.2016 osoitteesta http://www.gartner.com/document/2625419?ref=QuickSearch&sthkw=G00259115

Gartner Inc. (2015). Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. Haettu 28.1.2016 osoitteesta http://www.gartner.com/newsroom/id/3114217

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. Computers & Security, 24(1), 16-30.

Giusto, D., Iera, A., Iorabito, G., Atzori, L. (2010). The Internet of Things : 20th Tyrrhenian Workshop on Digital Communications. Springer.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1(1), 3 - 17.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. Communications of the ACM, 46(3), 81-85.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. Computers & Security, 24(1), 16-30.

Global Telematics. (2016). The Meaning of Telematics. Haettu 28.1.2016 osoitteesta http://www.globaltelematics.com/telematics.htm

Google Inc. (2015). Google Drive. Haettu 19.11.2015 osoitteesta https://www.google.com/drive/

Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Richardson, R. (2006). CSI/FBI Computer Crime and Security Survey (2006). Haettu 22.1.2016 osoitteesta http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. Communications of the ACM, 46(3), 81-85.

Gordon, L.A., Loeb, M.P., Zhou, L. (2011). The impact of information security breaches: has there been a downward shift in cost? Journal of Computer Security, 19(1), 33 - 56.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1(1), 3 - 17.

Hagelstam, A. (2004). CIP – kriittisen infrastruktuurin turvaaminen. Käsiteanalyysi ja kansainvälinen vertailu. Huoltovarmuuskeskuksen julkaisu, 1/2005. Helsinki.

Hale, A.R. & Swuste, P. (1998). Safety rule: procedural freedom or action constraint? Safety Science, 29(3), 163-177.

Hardy, G.H. (1940). A Mathematician´s Apology. Cambridge: Cambridge University Press.

Healey, J. (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Atlantic Council. Yhdysvallat.

Herath, T., and Rao, H. G. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. European Journal of Information Systems 18:2, 106-125.

Hu, Q., Hart, P. & Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. Journal of Strategic Information Systems 16 (2), 153–172.

Huoltovarmuuskeskus. (2013). PK-yrityksen kyberturvallisuuden kehittäminen. Huoltovarmuusorganisaatio. Haettu 14.6.2016 osoitteesta http://www.huoltovarmuus.fi/static/pdf/754.pdf

Höne, K. & Eloff, J.H.P. (2002b). What Makes an Effective Information Security Policy? Network Security, 2002(6), 14 - 16.

Hakala, J.T. (2002). Luova prosessi tieteessä. Helsinki: Gaudeamus.

Hale, A.R. & Swuste, P. (1998). Safety rule: procedural freedom or action constraint? Safety Science, 29(3), 163-177.

Hamilton, M. (2015). Back to the future: The influence of criminal history on risk assesments. Berkeley Journal of Criminal Law. Haettu 28.1.2016 osoitteesta http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2555878

Hardy, G.H. (1940). A Mathematician´s Apology. Cambridge: Cambridge University Press.

Harms-Ringdahl, L. (2004). Relationships between accident investigations, risk analysis, and safety management. Journal of Hazardous materials, 111(1), 13-19.

Hartio, I. (2013). Suomalaisprofessori rankattiin maailman tutkijoiden top 100 -listalle. Keskisuomalainen, 16.3.2013. Haettu 19.5.2016 osoitteesta http://www.ksml.fi/kotimaa/Mikko-Siponen-Euroopan-paras/200968

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J.P. (2011). Value conflicts for information security management. Journal of Strategic Information Systems, 20, 373-384.

Helsingin seudun kauppakamari. (2015). Yrityksiin kohdistuvat kyberuhat. Haettu 26.1.2016 soitteesta

http://helsinki.chamber.fi/media/filer_public/36/0f/360fddcd-4cfe-41a6-ab89-c028aa0bf15c/kyberturvallisuus_2015.pdf

Herath, T., and Rao, H. G. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. European Journal of Information Systems 18(2), 106-125.

Hirsjärvi, S., & Hurme, H. (2001). Teemahaastattelu: teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2002). Tutki ja kirjoita. Helsinki: Tammi.

Hu, Q., Hart, P. & Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. Journal of Strategic Information Systems 16 (2), 153–172.

Höne, K. & Eloff, J.H.P. (2002a). Information security policy - what do international information security standards say? Computers & Security, 21(5), 402 - 409.

Höne, K. & Eloff, J.H.P. (2002b). What Makes an Effective Information Security Policy? Network Security, 2002(6), 14 - 16.

Hyppönen, M. (2016): Tietoiskuseminaari 2016. Turku 22.3.2016. Haettu 17.5.2016 osoitteesta https://youtu.be/lilFz9tmyCM?t=51m6s

IBM. (2012). Reputational risk and IT. How security and business continuity can shape the reputation and value of your company. Findings from the 2012 IBM Global Reputational Risk and IT Study. Global Technology Services Research Report. Haettu 11.2.2016 osoitteesta https://www-935.ibm.com/services/multimedia/2012_Representational_Risk_Study.pdf

IF. (2016). Tietoturvavakuutus. Haettu 14.6.2016 osoitteesta https://www.if.fi/web/fi/yritysasiakkaat/vakuutuksemme/tietoturvavakuutus/pages/tietoturvavakuutus.aspx

Insta. (2015). Jarno Limnéll johtajaksi Instaan. Haettu 19.5.2016 osoitteesta http://www.insta.fi/defsec/blog/jarno-Limnéll-johtajaksi-instaan-3/

Institute of Risk Management. (2002). A Risk Management Standard. Haettu 1.6.2016 osoitteesta https://www.theirm.org/the-risk-profession/risk-management/irms-risk-management-standard.aspx

Intel. (2015). A guide to the internet of things. How billions of online objects are making the web wiser. Haettu 28.1.2016 osoitteesta http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

Internet World Stats. (2016). World Internet Users and 2015 Population Stats. Haettu 15.2.2016 osoitteesta http://www.internetworldstats.com/stats.htm

ISO Guide. (2009). 73: 2009: Risk management vocabulary. International Organization for Standardization.

ISO/IEC 27000:2009. (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.

ISO. (2009). 31000: 2009 Risk management–Principles and guidelines. International Organization for Standardization, Geneva, Switzerland.

IT2015. (2015). Korkeakoulujen IT -päivät 2015 -verkkosivut. Haettu 19.5.2016 osoitteesta http://it2015.fi/node/119

Johnston, A., Warkentin, M. & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric. MIS Quarterly, 39(1), 113-134.

Jyväskylän yliopisto. (2016a). Tietojenkäsittelytieteiden laitoksen henkilökunnan esittelyt, Siponen Mikko. Haettu 19.5.2016 osoitteesta https://www.jyu.fi/it/laitokset/cs/staff/cs_staff/siponen-mikko

Jyväskylän yliopisto. (2016b). Informaatioteknologian tiedekunta ja Keski-Suomessa toimivat yritykset kehittävät organisaatioiden tietoturvapolitiikkaa miljoonarahoituksella. Haettu 19.5.2016 osoitteesta https://www.jyu.fi/ajankohtaista/arkisto/2016/01/tiedote-2016-01-12-11-55-05-096033

Kaplan, R. & Norton, D.P. (1992). The Balanced Scorecard – Measures That Drive Performance. Harvard Business Review, Tammikuu/Helmikuu 1992.

Kaplan, R.S & Norton, D.P. (2004). Strategiakartat. Aineettoman pääoman muuttaminen mitattaviksi tuloksiksi. Helsinki: Talentum.

Karkimo, A. (2015). Tivin blogaaja Kimmo Rousku vuoden tietoturvapäälliköksi. Tivi, 22.4.2015. Haettu 19.5.2016 osoitteesta http://www.tivi.fi/Kaikki_uutiset/2015-04-22/Tivin-blogaaja-Kimmo-Rousku-vuoden-tietoturvapäälliköksi-3220309.html

Karlöf, B. & Helin Lövingsson, F. (2006). Organisaation olemus. Helsinki: Edita Prima Oy.

Karyda, M., Kiountouzis, E. & Kokolakis, S. (2001). Redefining information systems security: viable information systems. Sec '01 Proceedings of the 16th international conference on Information security: Trusted information: the new decade challenge, 453-468.

Karyda, M., Kiountouzis, E. & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security, 24(3), 246 - 260.

Kauppalehti. (2014). Usko kryptovaluuttojen aikakauteen kasvaa. Haettu 14.6.2016 osoitteesta http://www.kauppalehti.fi/uutiset/usko-kryptovaluuttojen-valtakauteen-kasvaa/pHdazswA

Kelly Rainer Jr., R., Marshall, T.E., Knapp, K.J. & Montgomery, G.H. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? Information Systems Security, 16(2), 100-108.

Killing, P. & Malnight, T. (2005). Must-win Battles: Creating the Focus You Need to Achieve Your Key Business Goals. Iso-Britannia.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security, 28(7), 493-508.

Kotler, P. & Keller, K.L. (2006). Marketing management. Prentice-Hall

Kraemer, S., Carayon, P & Clem, J. (2009) Human and organizational factors in computer security: Pathways to vulnerabilities. Computers & Security, 28(7), 509 - 520.

Kujansivu, P., Lönnqvist, A., Jääskeläinen, A. & Sillanpää, V. (2007). Liiketoiminnan aineettomat menestystekijät. Mittaa, kehitä ja johda. Helsinki: Talentum.

Kuusisto, R., & Toivonen, H. (2014). Ihmiset, verkot ja uudet yhteisöt. Teoksessa V. Muttilainen, & V. Huotari (Eds.), Poliisin toimintaympäristö. Poliisiammattikorkeakoulun katsaus 2014, 185-193. Poliisiammattikorkeakoulun raportteja (112). Tampere: Poliisiammattikorkeakoulu. Haettu 27.1.2016 osoitteesta http://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/25564_Raportteja_112_toimintaymparistokatsaus2014.pdf?a1172b3b8dead288

Kvale, S. (1996). InterViews. An introduction to qualitative research interviewing. USA: Sage.

Lanne, M. (2007). Yhteistyö yritysturvallisuuden hallinnassa: Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuushallinnassa. VTT.

Langley, G., Nolan, K. & Nolan, T. (1994). The Foundation of Improvement, Quality Progress.

Langley, G., Nolan, K., Nolan, T., Norman, C. & Provost, L. (1996). The Improvement Guide. San Francisco: Jossey-Bass.

Langley, G., Moen, R., Nolan, K., Nolan, T., Norman, C. & Provost, L. (2009). The Improvement Guide, 2nd Edition. San Francisco: Jossey-Bass.

Lanne, M. (2007). Yhteistyö yritysturvallisuuden hallinnassa: Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuushallinnassa. VTT.

Lehto, M. & Kähkönen , A. (2015). Kyberturvallisuuden kansallinen osaaminen. Informaatioteknologian tiedekunnan julkaisuja No.20/2015. Jyväskylän yliopisto.

Leppänen, A. & Kankaanranta, T. (2014). Motiiveja kyberuhkien taustalla. Teoksessa V. Muttilainen, & V. Huotari (Eds.), Poliisin toimintaympäristö. Poliisiammattikorkeakoulun katsaus 2014 (185-193). Poliisiammattikorkeakoulun raportteja (112). Tampere: Poliisiammattikorkeakoulu. Haettu 27.1.2016 osoitteesta http://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/25564_Raportteja_112_toimintaymparistokatsaus2014.pdf?a1172b3b8dead288

Lima, M. & Castro, P. (2005). Cultural theory meets the community: worldviews and local issues. Journal of Environmental Psychology, 25(1), 23-35.

Limnéll, J., Majewski, K., & Salminen, M. (2014). Kyberturvallisuus. Docendo, Saarijärvi.

Limnéll, J. (2014). Kyber rantautui Suomeen. Aalto yliopiston julkaisusarja 12/2014.

Limnéll, J. (2015). Kyberturvallisuuden erikoiskurssin luento 3.9.2015. Maanpuolustuskoulutusyhdistys. Espoo: Aalto-yliopisto.

Lindström, G. (2012). Meeting the Cyber Security Challenge. Geneva Papers. Geneva Centre for Security Policy. Haettu 15.2.2016 osoitteesta

http://www.gcsp.ch/News-Knowledge/Publications/Meeting-the-Cyber-Security-Challenge

Lämsä, A-M. & Hautala, T. (2005). Organisaatiokäyttäytymisen perusteet. Helsinki: Edita Prima Oy.

Mannermaa, M. (1991). Evolutionaarinen tulevaisuudentutkimus. Acta Futura Fennica No. 2. Helsinki: Painatuskeskus.

Mannermaa, M. (1999). Tulevaisuuden hallinta. Skenaariot strategiatyöskentelyssä. Porvoo: WSOY.

Mannermaa, Mika. 2008. Jokuveli - Elämä ja vaikuttaminen ubiikkiyhteiskunnassa. Helsinki: WSOYpro.

Mantere, S., Tienari, J., Vaara, E. ja Välikangas, L. (2008). Strategia ajatteluna ja puheena: kehys strategiselle uudistumiselle. Teoksessa Kuusela, P. & Kuittinen, M. (2008). Organisaatiot muutoksessa. Helsinki: UNIpress Suomi

Marris, C., Langford, I. & O'Riordan, T. (1996). Integrating sociological and psychological approaches to public perceptions of environmental risks: detailed results from a questionnaire survey. Centre for Social and Economic Research on the Global Environment. University of East Anglia, Norwich.

Mattila, P. (2007). Johdettu muutos. Avaimet organisaation hallittuun uudistumiseen. Helsinki: Talentum.

Mayry, Marika. (2016). Harva työntekijä ymmärtää työpaikkansa strategiaa. Vaasan yliopiston verkkosivujen uutisia. Julkaistu 14.4.2016. Haettu 15.4.2016 osoitteesta http://www.uva.fi/fi/news/maury/

McAfee Labs. (2014). Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cyber crime II. McAfee Center for Strategic and International Studies. Haettu 11.2.2016 osoitteesta http://www.mcafee.com/jp/resources/reports/rp-economic-impact-cybercrime2.pdf

McAfee Labs. (2015). The Hidden Data Economy. The Marketplace for Stolen Digital Information. Haettu 26.1.2016 osoitteesta http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf

Microsoft. (2014). Cyberspace 2025: Today's Decisions, Tomorrows Terrain. Haettu 28.1.2016 osoitteesta https://www.microsoft.com/security/cybersecurity/cyberspace2025/#chapter-1

Mintzberg, H. (1985). The organization as political arena. Journal of Management studies, 22, 133 - 154.

Moen, R. & Norman, C. (2006). Evolution of the PDCA Cycle. Haettu 2.6.2016 osoitteesta http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf

Mussington, D. (2002). Concepts for Enhancing Critical Infrastructure Protection. Relating Y2K to CIP Research and Development. RAND Science and Technology Policy Institute. Haettu 27.1.2016 osoitteesta http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1259.pdf

Myers, M. & Newman M. (2007). The Qualitive Interview in IS Research: Examining the Craft. Information & Organization 17, 2 - 26.

Niemi, H. (2014). Rikollisuuden kehityspiirteitä pitkällä aikavälillä. Teoksessa V. Muttilainen, & V. Huotari (Eds.), Poliisin toimintaympäristö. Poliisiammattikorkeakoulun katsaus 2014 (185-193). Poliisiammattikorkeakoulun raportteja (112). Tampere: Poliisiammattikorkeakoulu. Haettu 27.1.2016 osoitteesta http://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/25564_Raportteja_112_toimintaymparistokatsaus2014.pdf?a1172b3b8dead288

Niiniluoto, I. (1997). Johdatus tieteenfilosofiaan. Helsinki: Otava.

NIST General Information. Haettu 2.2.2016 osoitteesta http://www.nist.gov/public_affairs/general_information.cfm.

NIST. (2002). Sp 800-30. Risk management guide for information technology systems.

NIST. (2010). National Institute of Standards and Technology. Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Life Cycle Approach. Special publication 800-37.

NIST. (2011). National Institute of Standards and Technology. Managing Information Security Risk, Organization, Mission and Information System View. Special publication 800-39.

NIST. (2013). Glossary of Key Information Security Terms. National Institute of Standards and Technology Interagency or Internal Report, NISTIR 7298 Revision 2, May 2013. Haettu 22.12.2015 osoitteesta http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Opetusministeriö. (2004). Opinnäytetöiden julkisuus. Opetusministeriön kirje yliopistoille ja ammattikorkeakouluille 28.1.2004. Dnro 3/500/2004.

Oxford Dictionaries. (2015). Cybersecurity. Haettu 22.12.2015 osoitteesta http://www.oxforddictionaries.com/definition/english/cybersecurity?q=cyber+security

Oxford Dictionaries. (2016c). Contextualism. Haettu 22.2.2016 osoitteesta
http://www.oxforddictionaries.com/definition/english/contextualism

Oxford Dictionaries. (2016d). Holistic. Haettu 17.5.2016 osoitteesta
http://www.oxforddictionaries.com/definition/english/holistic

Pfleeger, S. (2000). Risky business: what we have yet to learn about risk management.
Journal of Systems Software, 53, 265-273.

Peltier, T. (1999). Information security policies and procedures: a practioner's reference. CRC Press.

Peltier, T. R. (2005). Information Security Risk Analysis. Auerbach publications. Boca Raton, Florida: CRC Press.

PK-RH. (2016). SRHY-riskienhallinta. Haettu 1.2.2016 osoitteesta http://www.pk-rh.fi/index.php?page=riskienhallintaprosessi

Pohjola, M. (2015). Digitaalisaatio ja tuottavuus finanssialalla. Aalto-yliopiston Kauppakorkeakoulu. Haettu 2.2.2016 osoitteesta http://www.fkl.fi/materiaalipankki/tutkimukset/Dokumentit/Raportti_Pohjola.pdf

Porter, M. E. (1979). How competitive forces shape strategy.

Porter, M. E. (1980). Competitive Strategy: Techniques for Analyzing Industries and Competitors. New York: Free Press.

Puolustusministeriö. (2008) Pitkä sähkökatko ja yhteiskunnan elintärkeiden toimintojen turvaaminen. Haettu 26.1.2016 osoitteesta http://www.defmin.fi/files/1436/pitka_sahkokatko_ja_yett.pdf

Purser, S. (2016). The current situation in European Cyber Security. Kyberturvallisuus koskettaa meitä jokaista -luentosarja. Aalto -yliopisto. Haettu 10.2.2016 osoitteesta https://www.youtube.com/watch?v=jOfAuDm9yLI

Puusa, A. & Juuti, P. (2011). Menetelmäviidakon raivaajat. Perusteita laadullisen tutkimuslähestymistavan valintaan. Johtamistaidon opisto. Vantaa: Hansaprint.

Puustinen, P. (2013). Vaihdantavallankumous: Finanssipalvelun uusi logiikka. Helsinki: Talentum.

PwC. (2014a). Sensing the future of the Internet of Things. Digital IQ Snapshot. PriceWaterhouseCoopers LLP. Haettu 28.1.2016 osoitteesta https://www.pwc.com/us/en/increasing-it-effectiveness/assets/future-of-the-internet-of-things.pdf

PwC. (2014b). Eyes wide shut. Global insights and actions for banks in the digital age. Findings from PwC's Global Digital Banking Survey. Haettu 2.2.2016 osoitteesta https://www.pwc.com/im/en/publications/assets/banking/global_digital_banking_survey1.pdf

PwC. (2014c). Retail Banking 2020. Evolution or Revolution? Haettu 2.2.2016 osoitteesta http://www.pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf

Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. Safety Science, 27(2/3), 183-213.

Rayner, S. (1984). Disagreeing about risk: the institutional cultures of risk management and planning for future generations". Teoksessa Halden, S. (Ed.): Risk Analysis, Institutions, and Public Policy. Associated Faculty Press, New York, 150-169.

Reason, J. (1998). Achieving a safe culture: theory and practice. Work & Stress, 12(3), 293-306.

RIA. (2014). 2014 Annual Report. Cyber Security Branch of the Estonian Information System Authority. Viro. Haettu 11.2.2016 osoitteesta https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014_ENG.pdf

RIMS. (2011). An Overview of Widely Used Risk Management Standards and Guidelines. A Joint Report of RIMS Standards and Practices Committee and RIMS ERM Committee. Risk and Insurance Management Society, Inc. Haettu 2.2.2016 osoitteesta https://www.rims.org/resources/ERM/Documents/RIMS%20Executive%20Report%20on%20Widely%20Used%20Standards%20and%20Guidelines%20March%202010.pdf

Roth, H. (2015). Culture: An Underrated Element in Security Policies. Geneva Center for Security Policies. Geneva Papers, 17/15.

Rubin, A. (2000). Tulevaisuuden tutkimus tiedonalana ja tieteellisenä toimintana. Haettu 30.12.2015 osoitteesta http://www.metodix.com/fi/sisallys/01_menetelmat/03_tieteenalakohtaiset/02_tulevaisuudentutkimus/kooste

Royal Society. (1992). Risk: analysis, perception and management. Report of a Royal Society study group. Lontoo: The Royal Society.

Sanastokeskus TSK. (2004). "Tietoturva". Tiivis tietoturvasanasto. TSK31. Haettu 14.6.2016 osoitteesta http://www.tsk.fi/tiedostot/pdf/TiivisTietoturvasanasto.pdf

Schein, E.H. (1987). Organisaatiokulttuuri ja johtaminen. Espoo: Weilin + Göös.

Schein, E.H. (2009). Yrityskulttuuri - selviytymisopas. Tietoa ennakkoluuloista ja kulttuurimuutoksesta. Espoo: Laatukeskus.

Shameli-Sendi, A., Aghababaei-Barzegar, R. & Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). Computers & Security, 57, 14-30.

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security. Information Systems Security, 11(4), 33-49.

Siponen, M.T., (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8 (1), 31 - 41.

Siponen, M. (2015). Opintojakson Advanced Information Security Management (TJTSM56) luennot. Jyväskylän yliopisto.

Siponen M., Mahmood, M.A. & Pahnila, S. (2014). Employees' adherence to information security policies: an exploratory field study. Information & Management, 51(2), 217–224.

Siponen, M.T. & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective esearch Contributions. ACM SIGMIS Database, 38(1), 60 - 80.

Siponen, M. T. & Willison, R. (2007). "A Critical Assessment of IS Security Research Between 1990-2004". Proceedings of the 15th European Conference on Information Systems, St. Gallen, Switzerland, June 7-9, 1551-1559.

Sisäministeriö. (2016a). Suomen kansallinen riskiarvio 2015. Sisäasiainministeriön julkaisuja, 3/2016. Helsinki. Haettu 15.2.2016 osoitteesta http://www.intermin.fi/julkaisu/032016?docID=65646

Sitra. (2016). Megatrendit 2016 - Tulevaisuus tapahtuu nyt. (Elina Kiiski Kataja). Sitran muistio 14.1.2016.

Soomro, Z.A., Shah, M.H. & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215 - 225.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS quarterly, 503-522.

Suomen Pankki. (2016). Riskien hallinta ja -valvonta. Haettu 10.6.2016 osoitteesta

http://www.suomenpankki.fi/fi/pankkitoiminta/riskienhallinta/pages/default.aspx

Suomen Riskienhallintayhdistys. (2016). Kansainvälinen yhteistyö. Haettu osoitteesta http://srhy.fi/toiminta/kansainvalinen_yhteistyo

Teece, D.J., Pisano, G. & Shuen, A. (1997). Dynamic Capabilities and Strategic Management. Strategic Managent Journal, 18(7), 509-533.

Tienari, J. & Piekkari, R. (2011). Z ja epäjohtaminen. Helsinki: Talentum.

Tilastokeskus. (2015). Energian hankinta ja kulutus 2015, 3. neljännes. Haettu 26.1.2016 osoitteesta http://www.tilastokeskus.fi/til/ehk/2015/03/ehk_2015_03_2015-12-18_fi.pdf

Tsohou, A., Karyda M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. Information Management & Computer Security,14(3), 198 - 217.

Tuomi, J. & Sarajärvi, A. (2009). Laadullinen tutkimus ja sisällönanalyysi, 5. uudistettu laitos. Helsinki: Tammi.

Turner, B. (1978). Man- Made Disasters. Lontoo: Wykeham.

Turvallisuus- ja puolustusasiain komitean sihteeristö. (2013). Suomen kyberturvallisuusstrategia.

Turvallisuuskomitea. (2015). Sähköriippuvuus modernissa yhteiskunnassa. Haettu 26.1.2016 osoitteesta http://www.vvy.fi/files/4666/sahkoriippuvuus_modernissa_yhteiskunnassa_verkkojulkaisu.pdf

Työsuojelu. (2016). Turvallisuusjohtaminen. Työsuojeluhallinnon www-sivut. Haettu 25.1.2016 osoitteesta http://www.tyosuojelu.fi/tyosuojelu-tyopaikalla/turvallisuusjohtaminen

Työturvallisuuslaki. (2002). 23.8.2002/738.

Whitman, M.E. & Mattord, H.J. (2010). Management of Information Security. Course Technology.

Valtioneuvoston kanslia. (2015). Ratkaisujen Suomi - Päministeri Juha Sipilän hallituksen strateginen ohjelma 29.5.2015. Hallituksen julkaisusarja 10/2015. Valtioneuvoston kanslia. Haettu 24.2.2016 osoitteesta http://valtioneuvosto.fi/documents/10184/1427398/Ratkaisujen+Suomi_FI_YHDISTETTY_netti.pdf/801f523e-5dfb-45a4-8b4b-5b5491d6cc82

Valtioneuvoston periaatepäätös 16.12.2010. Yhteiskunnan turvallisuusstrategia.

Valtioneuvoston päätös huoltovarmuuden tavoitteista 857/2013. Annettu 5.12.2013.

Viestintävirasto. (2014). Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti. Haettu 26.1.2016 osoitteesta https://www.viestintavirasto.fi/attachments/tietoturva/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

Von Wright, G.H. (1970). Tieteen filosofian kaksi perinnettä. Helsingin yliopiston filosofian laitoksen julkaisuja 1970(1).

VTT. (2003). Riskianalyysin menetelmät. Haettu 1.2.2016 osoitteesta http://virtual.vtt.fi/virtual/proj3/s-2-s/riskianalyysit_sivut.pdf

VTT. (2016). Kyberosaaminen Suomessa - Nykytila ja tiekartta tulevaisuuteen. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016. Haettu 24.2.2016 osoitteesta http://tietokayttoon.fi/documents/10616/2009122/9_Kyberosaaminen+Suomessa.pdf/29c8f675-0790-4c2f-91c2-69187b34b37e?version=1.0

Walker, A. (2014). Banking without banks: Exploring the disruptive effects of coverging technologies that will shape the future of banking. Journal of Securities Operations & Custody, 7(1), 69-80.

Wood, C. (1999). Security policies made easy. Baseline software.

Young, C.S. (2009). Metrics and methods for security risk management. Burlington: Syngress.

LIITE 1 SAATEKIRJE - ENSIMMÄISEN VAIHEEN HAASTATTELUT

15.3.2016

SAATEKIRJE FINANSSIALAN YRITYSTEN EDUSTAJILLE

Tuomas Kokkomäki
tuoantko@student.jyu.fi

Mika Nortunen
mihenort@student.jyu.fi

Arvoisa vastaanottaja.

Opiskelemme Jyväskylän yliopiston tietojenkäsittelytieteen laitoksella kyberturvallisuuden maisteriohjelmassa. Kyberturvallisuuden maisteriohjelman tavoitteena on tarjota vankka osaaminen kyberturvallisuuden kokonaishallintaa vaativissa johtamis- ja kehittämistehtävissä. Olemme tutkimuksen ajan virkavapaalla työnantajiemme, puolustusvoimien ja poliisin, palveluksesta.

Pro gradu -tutkielmassamme tutkitaan riskien arvioinnin vaikutusta organisaation tietoturvapolitiikan muodostumiseen. Monissa aiemmissa tutkimuksissa esitetyt mallit ovat saaneet osakseen kritiikkiä liiasta suurpiirteisyydestään tietoturvapolitiikan muodostumiseen vaikuttaviin tekijöihin liittyen. Tavoitteemme on tuoda konkretiaa tälle alueelle yhdistämällä aiemmasta tutkimuksesta ja standardeista saatava teoria organisaatioiden käytännön kokemuksiin. Finanssialan ollessa yksi kriittisen infrastruktuurin osa-alue, alan toiminnan ollessa riippuvainen tietojärjestelmien toimivuudesta ja maailman muuttuessa yhä nopeammin mielestämme tälle tutkimukselle on olemassa tarve. Olemme valinneet tietoturvapolitiikan tutkimuksemme ydinalueeksi, koska se on dokumentti, joka useimmissa organisaatioissa on olemassa.

Tutkimuksessa teemme kaksivaiheisen kvalitatiivisen tutkimuksen. Ensimmäisessä vaiheessa haastattelemme finanssialan yritysten edustajia ja tutkimme lisäksi riskienhallinnassa käytettäviä standardeja sekä kirjallisuutta. Ensimmäisen vaiheen haastattelujen jälkeen analysoimme kertyneen datan. Tämän jälkeen laadimme riskien arvioinnin prosessimallin osana tietoturvapolitiikan muodostumista yhdistämällä kertyneen datan teoriasta, standardeista ja kirjallisuudesta muodostuneeseen synteesiin. Tutkimuksen toisessa vaiheessa haastattelemme finanssialan yrityksiin liittyviä asiantuntijoita ja testaamme laatimamme mallin toimivuutta. Laadimme tutkimuksen valmistuttua raportin tuloksista ja toimitamme sen tutkimukseen osallistuneille yrityksille ja organisaatioille.

Tutkimuksemme tarjoaa osallistuville finanssialan yrityksille mahdollisuuden laajentaa ymmärrystään riskien arvioinnista tietoturvapolitiikan muodostumisen prosessissa. Tutkimus luo olemassa olevan teorian ja käytännön kautta nykyhetken kuvauksen riskien arvioinnista myös tutkimuskohdetta yleisemmällä tasolla.

Haastattelu toteutetaan henkilökohtaisilla teemahaastatteluilla. Haastattelu kestää maksimissaan kaksi tuntia. Toivoisimme pääsevämme haastattelemaan henkilöä, jolla on laaja tietämys sekä riskienhallinnan prosessista että tietoturvapolitiikan laadinnasta osana organisaation kokonaisstrategiaa.

Tutkimuksen raportti laaditaan siten, että yksittäiset organisaatiot tai henkilöt eivät ole tunnistettavissa. Tutkimuksen aineistoa ei luovuteta muille tahoille. Haastatelluilla henkilöillä on mahdollisuus tarkastaa tutkielman tekstisisältö ennen tutkielman palauttamista. Tutkimus valmistuu kesällä 2016 ja on tämän jälkeen yritysten käytettävissä.

Pro gradu -tutkielman ohjaajina toimivat:
Markus Salo, +358408054295, markus.t.salo@jyu.fi
Panu Moilanen, +358408254554, panu.moilanen@jyu.fi

Yhteistyöterveisin,

Tuomas Kokkomäki ja Mika Nortunen

LIITE 2 ASIANTUNTIJOIDEN REKRYTOINTI

14.4.2016

SAATEKIRJE

Tuomas Kokkomäki
tuoantko@student.jyu.fi

Mika Nortunen
mihenort@student.jyu.fi

Arvoisa vastaanottaja.

Opiskelemme Jyväskylän yliopiston tietojenkäsittelytieteen laitoksella kyberturvallisuuden maisteriohjelmassa. Kyberturvallisuuden maisteriohjelman tavoitteena on tarjota vankka osaaminen kyberturvallisuuden kokonaishallintaa vaativissa johtamis- ja kehittämistehtävissä. Olemme tutkimuksen ajan virkavapaalla työnantajiemme, puolustusvoimien ja poliisin, palveluksesta.

Pro gradu -tutkielmassamme tutkitaan riskien arvioinnin vaikutusta organisaation tietoturvapolitiikan muodostumiseen. Monissa aiemmissa tutkimuksissa esitetyt mallit ovat saaneet osakseen kritiikkiä liiasta suurpiirteisyydestään tietoturvapolitiikan muodostumiseen vaikuttaviin tekijöihin liittyen. Tavoitteemme on tuoda konkretiaa tälle alueelle yhdistämällä aiemmasta tutkimuksesta ja standardeista saatava teoria organisaatioiden käytännön kokemuksiin. Olemme valinneet tietoturvapolitiikan tutkimuksemme ydinalueeksi, koska se on dokumentti, joka useimmissa organisaatioissa on olemassa.

Tutkimus on kaksivaiheinen kvalitatiivinen tutkimus. Ensimmäisessä vaiheessa olemme haastatelleet finanssialan yritysten edustajia ja tutkineet lisäksi riskienhallinnassa käytettäviä standardeja sekä kirjallisuutta. Ensimmäisen vaiheen haastattelujen jälkeen olemme analysoineet kertyneen datan. Tämän jälkeen olemme laatineet riskien arvioinnin prosessimallin osana tietoturvapolitiikan muodostumista yhdistämällä kertyneen datan teoriasta, standardeista ja kirjallisuudesta muodostuneeseen synteesiin. Tutkimuksen toisessa vaiheessa haastattelemme asiantuntijoita ja testaamme laatimamme mallin toimivuutta suorittamalla niin sanotun "heikon markkinatestin". Laadimme tutkimuksen valmistuttua raportin tuloksista ja toimitamme sen tutkimukseen osallistuneille yrityksille ja organisaatioille.

Tutkimuksemme tarjoaa osallistuville finanssialan yrityksille mahdollisuuden laajentaa ymmärrystään riskien arvioinnista tietoturvapolitiikan muodostumisen prosessissa. Tutkimus luo olemassa olevan teorian ja käytännön kautta nykyhetken kuvauksen riskien arvioinnista myös tutkimuskohdetta yleisemmällä tasolla.

Haastattelu toteutetaan henkilökohtaisilla teemahaastatteluilla. Haastattelu kestää maksimissaan kaksi tuntia. Toivoisimme pääsevämme haastattelemaan juuri Teitä, koska uskomme juuri Teidän omaavan riittävän ammattitaidon liittyen tutkimuksemme toisen vaiheen asiantuntijahaastatteluihin.

Tutkimuksen aineistoa ei luovuteta muille tahoille. Haastatelluilla henkilöillä on mahdollisuus tarkastaa tutkielman tekstisisältö ennen tutkielman palauttamista. Tutkimus valmistuu kesällä 2016 ja on tämän jälkeen yritysten käytettävissä.

Pro gradu -tutkielman ohjaajina toimivat:
Markus Salo, +358408054295, markus.t.salo@jyu.fi
Panu Moilanen, +358408254554, panu.moilanen@jyu.fi

Yhteistyöterveisin,

Tuomas Kokkomäki ja Mika Nortunen

LIITE 3 SAATEKIRJE - ASIANTUNTIJAHAASTATTELUT

9.5.2016

SAATEKIRJE

Tuomas Kokkomäki
tuoantko@student.jyu.fi

Mika Nortunen
mihenort@student.jyu.fi

Arvoisa vastaanottaja.

Opiskelemme Jyväskylän yliopiston tietojenkäsittelytieteen laitoksella kyberturvallisuuden maisteriohjelmassa. Kyberturvallisuuden maisteriohjelman tavoitteena on tarjota vankka osaaminen kyberturvallisuuden kokonaishallintaa vaativissa johtamis- ja kehittämistehtävissä. Olemme tutkimuksen ajan virkavapaalla työnantajiemme, puolustusvoimien ja poliisin, palveluksesta.

Aloitimme syksyllä 2015 pro gradu -tutkielman aiheesta *riskien arvioinnin vaikutus organisaation tietoturvapolitiikan muodostumisessa*. Prosessin aikana painopiste on siirtynyt tutkimukseen *kyberturvallisuuden riskien arvioinnin ja yleisesti riskien arvioinnin vaikutuksesta organisaation strategian toteutumisessa*. Aiheen muotoutumiseen ovat vaikuttaneet sekä tutkijoiden kasvanut tietämys riskien arvioinnista että haastateltujen organisaatioiden näkemykset tutkimuksen tarpeesta. Riskien arvioinnin vaikutus tietoturvapolitiikan muodostumisessa on edelleen mukana tutkimuksessamme, mutta lähinnä yhtenä vaihtoehtoisena organisaation työkaluna, joka syntyy osaksi riskien arvioinnin vaikutuksesta.

Tutkimus on kaksivaiheinen kvalitatiivinen tutkimus. Ensimmäisessä vaiheessa olemme haastatelleet finanssialan yritysten edustajia ja tutkineet lisäksi riskien arvioinnissa käytettäviä standardeja sekä kirjallisuutta. Ensimmäisen vaiheen haastattelujen jälkeen olemme analysoineet kertyneen datan. Tämän jälkeen olemme laatineet riskien arvioinnin prosessimallin laatimalla synteesin teoriasta, standardeista, kirjallisuudesta ja haastatteluista. Nyt tehtävässä tutkimuksen toisessa vaiheessa esittelemme laatimamme mallin, haastattelemme asiantuntijoita ja testaamme laatimamme mallin toimivuutta. Mallia on mahdollista korjata asiantuntijahaastatteluista saadun palautteen perusteella.

Mallin esittely ja siihen liittyvä haastattelu toteutetaan henkilökohtaisesti. Tilaisuus kestää maksimissaan kaksi tuntia. Laadimme tutkimuksen valmistuttua raportin tuloksista ja toimitamme sen tutkimukseen osallistuneiden organisaatioiden käyttöön.

Terveisin,

Tuomas Kokkomäki ja Mika Nortunen

LIITE 4 ENSIMMÄISEN KIERROKSEN HAASTATTELURUNKO

30.3.2016

HAASTATTELURUNKO, 1. VAIHEEN HAASTATTELUT

Tuomas Kokkomäki
tuoantko@student.jyu.fi

Mika Nortunen
mihenort@student.jyu.fi

TAUSTATIEDOT

- Haastateltavan henkilön nimi, toimenkuva, organisaatio
- Mikä on roolinne riskienhallinnassa ja -arvioinnissa?
- Mikä on roolinne tietoturvapolitiikan laadinnassa?

TEEMA 1: RISKIENHALLINTA

1. Miten organisaationne riskienhallintaprosessi pääpiirteissään etenee?
2. Antaako organisaationne riskienhallinnan strategian kautta riittävän ohjauksen riskien arvioinnin suorittamiseen? (esim. tarkkuus, laajuus, muoto)
3. Kuka vastaa organisaationne turvallisuusstrategiasta ja sen laadinnasta?

TEEMA 2: RISKIEN ARVIOINTI

4. Miten suorittamanne riskien arvioinnin prosessi käytännössä etenee?
5. Mistä organisaationne saa riskien arvioinnin perustana olevan uhkatiedon?
6. Suorittaako organisaationne riskien arvioinnin itse vai käytättekö ulkopuolista arvioitsijaa?
7. Miten ja millä laajuudella riskien arvioinnin tulokset jaetaan organisaatiossanne?
8. Missä "muodossa" esitätte riskien todennäköisyydet? (Laadullinen, määrällinen, jotain muuta)
9. Riskien arvioinnin päivittäminen: miten usein arvioita päivitetään?

TEEMA 3: TIETOTURVAPOLITIIKAN LAATIMINEN

10. Miten organisaationne tietoturvapolitiikan muodostamisen prosessi etenee?
11. Miten riskien arvioinnin tulokset vaikuttavat tietoturvapolitiikan muodostumiseen käytännössä?
12. Oletteko käyttäneet tietoturvapolitiikkanne laadinnassa avoimesti saatavilla olevia tai kaupallisia standardeja ja käytänteitä? Oletteko muokanneet niitä paremmin omiin tarpeisiinne sopiviksi?

TEEMA 4: PARHAAT KÄYTÄNTEET

13. Mikä suorittamassanne riskien arvioinnin prosessissa on koettu toimivaksi?
14. Mitä suorittamassanne riskien arvioinnin prosessissa ei ole koettu toimivaksi?
15. Mitkä tekijät / toimintatavat olette kokeneet toimiviksi tietoturvapolitiikan laatimisen prosessissa?

LIITE 5 ASIANTUNTIJAHAASTATTELUIDEN RUNKO

9.5.2016

Teemat toiselle haastattelukierrokselle

Teiltä asiantuntijoilta toivomme palautetta ja kehittämisehdotuksia muun muassa seuraavista teemoista:

- Ensivaikutelma mallista
- Malli riskien arviointi prosessin perustana
- Malli organisaation oman menetelmän viitekehyksenä
- Teoreettinen tarkastelu siitä, olisiko organisaatio valmis ottamaan kyseisen mallin käyttöönsä
- Hyvät puolet ja kehityskohteet
- Malli toiminnan yksinkertaistajana / tehostajana
- Mallin potentiaaliset käyttökohteet
- Tuoko malli lisäarvoa nykyisiin menetelmiin

Toivomme teemojen lisäksi vapaata keskustelua esittelemämme mallin rakenteesta ja sen käyttömahdollisuuksista.

LIITE 6 STANDARDIN REFERAATTI – ISO 31000:2009

ISO (the International Organisation for Standardization) on kansainvälinen standardisoimisjärjestö. Se on itsenäinen, ei-valtiollinen järjestö, jonka tarkoituksena on asiantuntijoiden ammattitaidon kautta jakaa tietoa ja kehittää merkityksellisiä kansainvälisiä standardeja tukemaan innovaatioita ja tarjoamaan ratkaisuja globaaleihin haasteisiin. (ISO, 2009; http://www.iso.org/iso/home/about.htm, 15.2.2016).

ISO:n standardien tarkoitus on tarjota yleisiä suosituksia ja ohjeita eri aloille laadun, turvallisuuden ja tehokkuuden takaamiseksi (http://www.iso.org/iso/home/about.htm, 15.2.2016). ISO - standardi 31000:2009 "Risk Management - Principles and Guidelines" on yleinen riskienhallinnan standardi, jonka tarkoituksena on tarjota riskienhallinnalle yleiset periaatteet ja suuntaviivat. ISO nostaakin yhdeksi tämän standardin keskeisimmistä tavoitteista kontekstin luomisen. Riskienhallinnan kontekstin kautta organisaatiolla on mahdollisuus asettaa riskienhallinnalleen tavoitteet ja keinot näiden tavoitteiden saavuttamiseksi. (ISO, 2009).

Riskienhallinta

Tausta ja kohdeyleisö

ISO:n standardi 31000:2009 on yleinen riskienhallinnan standardi ja se soveltuu laajasti erilaisille organisaatioille ja toimijoille, kuten esimerkiksi:

- oman organisaationsa riskienhallintapolitiikan laatimisesta vastaavat toimijat
- riskienhallinnan toteutuksen tapahtumisesta vastuussa olevat toimijat
- organisaation riskienhallinnan arviointia suorittavat toimijat
- standardien, ohjeiden ja politiikoiden kehittäjät ja laatijat.

(ISO, 2009).

ISO (2009) kuitenkin toteaa, että tätä standardia ei ole laadittu millekään tietylle organisaatiolle tai ryhmälle, vaan sen periaatteet ovat sovellettavissa kenelle tahansa ja minkä tyyppisiin riskeihin tahansa. (ISO, 2009).

Riskienhallinnan perusteet

ISO (2009) määrittää riskienhallinnan prosessiksi, jonka pitäisi olla olennainen osa organisaation johtamista, sulautettu organisaation kulttuuriin ja käytäntöihin sekä räätälöity sopimaan organisaation liiketoimintaprosesseihin. (ISO, 2009). Organisaatioiden ei tulisi ottaa mitään riskienhallinnan menetelmää käyttöön sellaisenaan, vaan sen soveltuvuus tulisi aina sopeuttaa kyseisen organisaation toiminnan kontekstiin.

ISO (2009) listaa tehokkaan riskienhallinnan periaatteiksi seuraavat asiat:

- Riskienhallinta luo ja suojaa arvoa

- Riskienhallinta on organisaation prosessien olennainen osa
- Riskienhallinta on osa päätöksentekoprosessia
- Riskienhallinta ottaa huomioon epävarmuuden
- Riskienhallinta on systemaattinen, jäsennelty ja oikea-aikainen prosessi
- Riskienhallinta perustuu parhaaseen saatavilla olevaan tietoon
- Riskienhallinta on räätälöity organisaation toiminnan kontekstiin
- Riskienhallinta ottaa huomioon inhimilliset ja kulttuuriset tekijät
- Riskienhallinta on avoin ja kattava prosessi
- Riskienhallinta on dynaaminen, iteratiivinen ja muutoksiin reagoiva prosessi
- Riskienhallinta johtaa organisaation jatkuvaan kehittymiseen.

(ISO, 2009).

Riskienhallinnan tulee perustua laajempaan viitekehykseen, joka tarjoaa riskienhallinnan prosessille perustan ja suuntaviivat. Tämän viitekehyksen kautta riskeistä johdettu tieto tulee raportoitua riittävällä tasolla ja on päätöksentekijöiden käytössä kaikilla organisaation tasoilla. (ISO, 2009).

Riskienhallinnan tavoitteet

ISO (2009) luettelee useita esimerkkejä siitä, mitä oikein toteutetun riskienhallinnan kautta voidaan saavuttaa. ISO:n mukaan standardin mukaan toteutettu riskienhallintaa edesauttaa organisaation toiminnan tavoitteiden saavuttamista ja se kannustaa ennakoivaan johtamiseen. Riskienhallinta auttaa tunnistamaan riskit ja reagoimaan niihin ja se auttaa organisaatiota löytämään myös toiminnan mahdollisuuksia. Riskienhallinnan kautta on myös mahdollista parantaa hallintoa, raportointia ja sidosryhmien luottamusta organisaatioiden toimintaa kohtaan. Tehokkaan riskienhallinnan kautta voidaan lisäksi parantaa organisaation toiminnan tehokkuutta ja sietokykyä. (ISO, 2009). Kokonaisuudessaan ISO esittää riskienhallinnalle monia tavoitteita, jotka liittyvät organisaation toimintaan useista eri näkökulmista.

Riskienhallinnan vaiheet

ISO (2009) esittää riskienhallinnan prosessin seuraavan kuvion kaltaiseksi.

KUVIO 5

Viestintä ja tiedonvaihto

ISO:n mukaan viestinnän ja tiedonvaihdon toteuttaminen tulisi suunnitella mahdollisimman aikaisessa vaiheessa. Viestinnän ja tiedonvaihdon tavoitteena on, että varsinaisen riskienhallinnan prosessin suorittajat ymmärtävät ne perusteet, joihin päätösten tekemisen tulisi perustua sekä syyt sille, miksi tiettyihin toimenpiteisiin on ryhdytty. Viestinnän ja tiedonvaihdon kautta riskienhallinnalle määritetään konteksti / asiayhteys ja tuetaan seuraavassa vaiheessa tehtävää toimintaympäristön määrittämistä. Viestinnän tarkoituksena on myös huolehtia siitä, että sidosryhmien intressit on ymmärretty ja tarvittaessa otettu huomioon.

Toimintaympäristön määrittäminen
Toimintaympäristön määrittämisen kautta organisaatio määrittää riskienhallinnalle tavoitteet, laajuuden ja huomioon otettavat sisäiset ja ulkoiset muuttujat. Toimintaympäristön määrittämisen vaiheen toteuttaminen riippuu organisaatiosta ja se tulee aina muokata organisaation toimintaan sopivaksi. Tähän vaiheeseen liittyy myös riskienhallinnan kriteerien määrittäminen. Tällä tarkoitetaan esimerkiksi todennäköisyyksien määrittämisen ja esittämiseen liittyviä valintoja sekä riskitoleranssien määrittämistä. (ISO, 2009).

Riskien arviointi
Riskien arviointi on kokonaisprosessi, joka sisältää riskien tunnistamisen, analysoinnin ja merkityksen arvioinnin. Riskien arvioinnin alussa organisaation tulee tunnistaa riskien lähteet ja niiden mahdolliset vaikutukset. Tarkoituksena on tuottaa organisaation toimintaan vaikuttavista riskeistä kattava lista. On tärkeää, että riskien tunnistaminen tehdään huolella, koska tässä vaiheessa tunnistamatta jääneitä riskejä ei pystytä ottamaan huomioon seuraavissa vaiheissa. Riskien tunnistamisen keinot sovitetaan organisaation tavoitteisiin ja kykyihin. (ISO, 2009).

Tunnistaminen jälkeen suoritetaan riskien analysointi. Sen tarkoituksena on kehittää ymmärrys riskeistä. Riskien analysointi antaa syötteen riskien merkityksen arvioinnille. Analysoinnissa pyritään huomioimaan riskien vaikutukset ja lähteet sekä niiden esiintymisen todennäköisyys. Tässä vaiheessa tulisi myös suorittaa arviointi siitä, miten luotettaviksi tulokset arvioidaan ja tämä tulisi saattaa kaikkien päätöksentekijöiden tietoon. (ISO, 2009).

Riskien merkityksen arviointi pyrkii auttamaan riskien analysoinnin tuloksien perusteella tehtävien päätösten tekemisessä. Tämän vaiheen tarkoituksena on määritellä, mihin riskeihin pyritään vastaamaan ja mitkä ovat toimeenpanon prioriteetit. Päätöksissä tulisi ottaa huomioon riskien laajempi konteksti sekä määritetyt riskien sietoon liittyvät toleranssit. (ISO, 2009).

Riskien käsittely
Riskien käsittelyn yhteydessä valitaan ja toimeenpannaan yksi tai useampi keino riskien vaikutusten muokkaamiseksi. Riskien käsittelyyn liittyy kehämäinen prosessi, jossa arvioidaan riskien käsittelyn keinot, päätetään hyväksyttävissä olevat riskien tasot, luodaan tarvittaessa uusia keinoja riskien käsittelyyn ja arvioidaan riskien käsittelyn vaikutukset. (ISO, 2009).

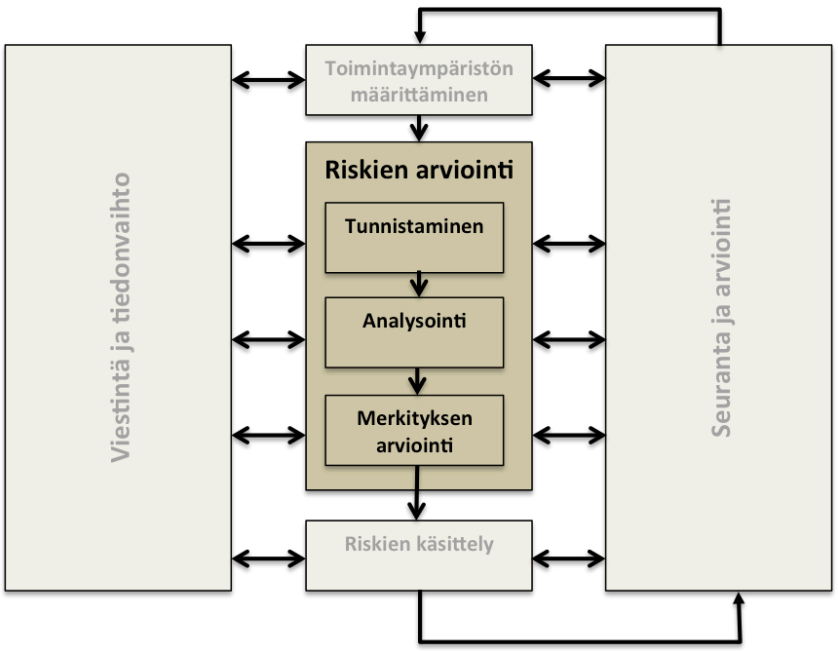
Sopivien riskien käsittelyn keinojen valintaan vaikuttaa tasapainoilu muun muassa kustannusten ja keinoilla saavutettavien etujen välillä. Toteutettavaksi valittavat keinot voidaan toteuttaa joko yksittäin tai keinojen yhdistelmänä. Riskien käsittelyn toteuttamisen suunnitelmassa tulee määritellä prioriteettijärjestys, jonka mukaan yksittäisiä riskien käsittelyn keinoja tulisi toteuttaa. (ISO, 2009).

Seuranta ja arviointi
Seurannan ja arvioinnin tulee olla riskienhallinnan suunniteltu osa ja siihen liittyvät vastuut tulisi olla tarkasti määritelty. Seurannan ja arvioinnin tulee kattaa riskienhallinnan prosessin kaikki vaiheet. Seurannan ja arvioinnin avulla voi-

daan varmistaa, että valitut riskien kontrollit ovat tehokkaita. Lisäksi voidaan hankkia lisää informaatioita tulevia riskien arviointeja varten sekä analysoida menneitä tapahtumia organisaation oppimisen hyväksi. Seuranta ja arviointi auttavat organisaatiota myös havaitsemaan toimintaympäristön muutoksia ja nousevia riskejä. (ISO, 2009).

Riskien arviointi
Perusteet
Riskien arvioinnin tarkoituksena on tarjota päätöksentekijöille parempi ymmärrys riskeistä, jotka voivat vaikuttaa organisaation toimintaan. Riskien arviointi tarjoaa perusteet, joiden avulla voidaan valita riskien käsittelyyn sopivat lähestymistavat. Riskien arvioinnin tulokset toimivat syötteenä organisaation päätöksentekoprosesseille. (IEC/ISO, 2009). ISO tarjoaa riskien arvioinnin tueksi useita tekniikoita ja menetelmiä, joita on avattu tarkemmin standardissa "ISO/IEC 31010:2009 - Risk management - Risk assessment techniques". Riskien arviointi on prosessi, joka tulee aina muokata ja sovittaa organisaation toimintaan ja resursseihin sopivaksi.

Riskien arvioinnin prosessi
ISO (2009) kuvaa riskien arvioinnin prosessin seuraavan kuvion kaltaiseksi:



KUVIO: Riskien arvioinnin prosessi (ISO, 2009; ISO/IEC, 2009)

Riskien arviointi on olennainen osa riskienhallinnan kokonaisprosessia. Riskien arviointi muodostuu riskien tunnistamisesta, riskien analysoinnista ja riskien merkityksen arvioinnista. Käytännön tapa suorittaa riskien arviointi riippuu suuresti riskienhallinnan kokonaisuudessa määritetyistä perusteista ja organisaation valitsemista metodeista ja tekniikoista. (ISO/IEC, 2009).

Riskien tunnistaminen
Riskien tunnistamisen tarkoituksena on löytää ja tunnistaa riskit. Tässä vaiheessa identifioidaan tapahtumat ja tilanteet, jotka voivat vaikuttaa organisaation tavoitteiden saavuttamiseen. Varsinaisten riskien lisäksi tulisi pyrkiä tunnistamaan riskeihin johtavat syyt ja niiden lähteet. Riskien tunnistamiseen on olemassa erilaisia metodeja, joita tarjotaan myös ISO:n standardissa. Tunnistamisen tarkkuutta ja kattavuutta voidaan parantaa tekniikoita yhdistelemällä. Riskien tunnistamisessa tulisi huomioida mahdollisimman kattavasti erilaiset näkökulmat, kuten laitteistolliset, inhimilliset ja organisationaaliset näkökulmat. (ISO/IEC, 2009).

Riskien analysointi
Riskien analysoinnin kautta organisaatio kehittää syvemmän ymmärryksen riskeistä. Analyysin yhteydessä määritellään riskien potentiaaliset seuraukset ja niiden todennäköisyydet. Näiden kautta organisaatio määrittää riskien tasot. Tämän vaiheen suorittaminen voi olla kokonaisuutena monimutkainen ja haastava ja se saattaa vaatia monien erilaisten metodien käyttämistä. (ISO/IEC, 2009).

Riskien analysoinnin tulokset voidaan esittää laadullisessa, määrällisessä tai semi-määrällisessä (semi-quantitative) muodossa. Siihen, mitä muotoa organisaatio käyttää, vaikuttaa muun muassa arvioinnissa käytettävän datan luotettavuus ja organisaation tarpeet. Analysoinnissa käytettävä metodologia tulosten esittämisen suhteen tulee määritellä riskienhallinnan ja -arvioinnin perusteita määriteltäessä. Arvioinnissa ja sen tuloksia tulkittaessa tulee aina ottaa huomioon, että kyse on arvioista, ei absoluuttisen oikeasta arvosta. Riskien tasoon vaikuttavat myös olemassa olevat keinot riskien vähentämiseksi ja ne tulee ottaa analysoinnin yhteydessä huomioon. (ISO/IEC, 2009).

Riskien merkityksen arviointi
Riskien merkityksen arvioinnin tarkoituksena on verrata aiemmissa vaiheissa määritettyjä riskien tasoja riskienhallinnan perusteissa määriteltyihin perusteisiin ja määrittää tätä kautta riskien merkittävyys ja tyypit. Riskien merkityksen arviointi käyttää riskeistä kerättyä ymmärrystä tehtäessä päätöksiä siitä, miten riskeihin pyritään vastaamaan. Riskien merkityksen arvioinnissa tulee määritellä, mihin riskeihin pyritään vastaamaan ja mitkä ovat prioriteetit. (ISO/IEC, 2009).

Riskien arviointiin osana riskienhallintaa tulee sisältyä myös riittävä dokumentointi. Tämän raportoinnin laajuus tulee määrittää osana riskienhallinnan perusteita. Dokumentoinnissa tulisi käyttää mahdollisimman ymmärrettäviä termejä ja riskien tasojen kuvaamisessa tulisi olla mahdollisimman selkeä ja yksiselitteinen. Dokumentoinnista tulisi tehdä mahdollisimman helposti ylläpidettävä ja sen aktiivinen päivittäminen tulisi olla osa riskienhallinnan toteuttamista. (ISO/IEC, 2009).

LIITE 7 STANDARDIN REFERAATTI – NIST

NIST (National Institute of Standards and Technology) on yhdysvaltalainen virasto, joka toimii kauppaministeriön alaisuudessa. Sen tehtävänä on kehittää innovaatioita ja kilpailukykyä muun muassa tieteen, standardien ja teknologian kautta. (http://www.nist.gov/public_affairs/general_information.cfm, haettu 2.2.2016). Special Publication 800 -sarja käsittelee NIST:n ITL:n (The Information Technology Laboratory) ohjeita, suosituksia ja standardeja liittyen informaatioturvallisuuteen. ITL:n vastuualueeseen kuuluu muun muassa tieto- ja viestintäteknisten järjestelmien johtamiseen ja teknisiin seikkoihin liittyvien standardien ja suositusten kehittäminen.

Riskienhallinta
Tässä tutkimuksessa esiteltävä NIST:n menetelmä riskienhallinnan toteuttamiseen perustuu pääosin asiakirjaan "NIST Special Publication 800-39: Managing Information Security Risk". Tämä asiakirja on NIST:n merkittävin tietoturvallisuuteen liittyvä standardi, jonka tarkoituksena on tarjota ohjausta informaatioturvallisuuteen liittyvien riskien hallintaan. Standardi pyrkii tarjoamaan jäsennetyn, mutta joustavan menetelmän, joka on tarkoituksellisesti laajapohjainen tarjoten kuitenkin yksityiskohtaiset ohjeet riskien arviointiin, niihin reagoimiseen sekä niiden jatkuvaan monitorointiin. (NIST, 2011).

NIST:n riskienhallintastandardi ei ole yleinen koko riskienhallinnan kattava menetelmä, vaan se keskittyy nimenomaan informaatioturvallisuuden alueeseen. Menetelmää tulisi siis käyttää osana jotain laajempaa riskienhallinnan menetelmää.

Kyseisen menetelmän kohdeyleisö käsittää laajasti monia riskienhallinnan ammattilaisia, kuten:

- yksilöt, joilla on valvontavelvollisuus riskienhallinnasta
- yksilöt, jotka vastaavat organisaation liiketoimintojen johtamisesta
- yksilöt, joiden tehtävänä on hankkia informaatiota liittyen teknologisiin palveluihin, tuotteisiin tai järjestelmiin
- yksilöt, joiden vastuulla on tietoturvallisuuden valvonta, johtaminen ja operationaalinen toiminta
- yksilöt, joiden tehtävänä on suunnitella, kehittää tai ottaa käyttöön tietojärjestelmiin liittyviä turvallisuusratkaisuja
- yksilöt, joiden tehtävänä on suorittaa turvallisuuden arviointia tai valvontaa. (NIST, 2011).

Riskienhallinnan perusteet
NIST:n standardi korostaa organisaation johdon vastuuta myös informaatio- tai kyberturvallisuuteen liittyen. NIST:n mukaan ylemmän johdon tulee olla sitoutunut riskienhallintaan organisaation toiminnan keskeisenä ja perustavan laatuisena toimintana. NIST kuvaa riskienhallintaa kokonaisvaltaiseksi, koko or-

ganisaation käsittäväksi toiminnaksi. Riskienhallinta tulee huomioida riskit aina strategiselta tasolta taktiselle tasolle. Riskienhallinnan tulee varmistaa, että riskeihin perustuva päätöksenteko on integroitu organisaation kaikille tasoille. Riskienhallinta on kompleksinen ja monitahoinen prosessi, joka vaatii koko organisaation sitoutumisen. (NIST, 2011).

Standardi ei suhtaudu riskienhallintaan eksaktina tieteenä. Riskienhallinta kokoaa yhteen näkemykset mahdollisimman laajasti: yksilöiltä, organisaation strategisesta suunnittelusta vastaavilta ryhmiltä, valvonnan suorittajilta, johtajilta sekä päivittäisessä toiminnassa mukana olevilta yksilöiltä ja ryhmiltä. Tämän on mahdollisuus tehdä tarvittavat ja riittävän riskien torjuntatoimet organisaation toiminnan suojaamiseksi. (NIST, 2011).

Tehokas riskienhallinnan prosessi vaatii organisaation ylemmän johdon vahvan sitoutumisen. Kun riskienhallinta on priorisoitu riittävän korkealle, on organisaation mahdollista saada riittävät resurssit laadukkaan ja laajan riskienhallintaohjelman toteuttamiseksi. Riskienhallinta tulisi tunnistaa strategiseksi kyvykkyydeksi ja toiminnan mahdollistajaksi. (NIST, 2011).

NIST:n mukaan tehokas kyberturvallisuuden riskienhallinta vaatii onnistuakseen tietyt avaintekijät:

- Riskienhallinnan vastuiden nimeäminen johtajille
- Johtajien ymmärrys kyberturvallisuuteen liittyvistä riskeistä ja niiden vaikutuksista organisaation toimintaan
- Riittävän riskinsietokyvyn saavuttaminen (jäännösriski) ja siitä kommunikoiminen koko organisaatiossa. Organisaatiolla tulee olla ohjeistus siitä, miten mahdolliset häiriötekijät vaikuttavat esimerkiksi päätöksentekoon.
- Ylemmän johdon vastuullisuus riskienhallintaan liittyvissä päätöksissä sekä tehokkaiden ja koko organisaation kattavien riskienhallintaohjelmien toteuttaminen. (NIST, 2011).

Riskienhallinnan tavoitteet

Standardin tarkoituksena on asettaa kyberturvallisuus laajempaan organisaation asiayhteyteen organisaation menestyksen hyväksi. Tähän pyritään seuraavien tavoitteiden kautta:

- Organisaation tulee varmistaa, että johtajat tiedostavat informaatioturvallisuuteen liittyvien riskien tärkeyden ja mahdollistavat riittävien rakenteiden luomisen tämän riskin käsittelemiseksi.
- Organisaation tulee varmistaa, että riskienhallinnan prosessia toteutetaan tehokkaasti kaikilla organisaation tasoilla.
- Organisaatiossa tulee ylläpitää asennetta, jossa kyberturvallisuuteen liittyvät riskit tunnistetaan ja tunnustetaan kokonaistoiminnan olennaiseksi osaksi.
- Informaatioteknologian järjestelmien käyttöönottoon tai käyttämiseen osallistuvien yksilöiden auttaminen ymmärtämään paremmin sitä, miten heidän toimintaansa sisältyvät riskit vaikuttavat koko organisaatioon kohdistuviin riskeihin ja sitä kautta mahdollisesti koko organisaation toimintaan. (NIST, 2011).

Riskienhallinnan vaiheet
NIST (2011) esittää riskienhallinnan prosessiksi, joka käsittää neljä vaihetta:

1. Riskien "raamittaminen", eli kontekstin muodostaminen riskeihin perustuvalle päätöksenteolle.
2. Riskien arviointi.
3. Riskeihin vastaaminen arvioinnin pohjalta.
4. Riskien jatkuva seuranta käyttäen tehokasta kommunikaatiota ja palautetta tavoitteena jatkuva kehittyminen organisaation riskeihin liittyvissä toiminnoissa. (NIST, 2011).

Riskien raamittaminen ("frame risk")
Ensimmäisen vaiheen tarkoituksena on luoda riskien konteksti. Tällä tarkoitetaan sen ympäristön kuvaamista, jossa riskiperusteiset päätökset tehdään. Vaiheen perimmäisenä tarkoituksena on luoda riskienhallinnan strategia. Tässä strategiassa osoitetaan, miten organisaatio aikoo arvioida riskit, vastata niihin ja monitoroida riskitilannetta. Ensimmäinen vaihe luo pohjan seuraaville vaiheille ja tässä vaiheessa tulisi kuvailla se ympäristö, jossa riskiperusteisia päätöksiä tehdään. (NIST, 2011).

Muodostaakseen realistisen ja uskottavan kehyksen riskeille organisaation tulee tunnistaa seuraavat asiat:

- Riskien olettamukset

Oletukset uhkista, haavoittuvuuksista, edellä mainittujen seurauksista ja niiden esiintymisen todennäköisyydestä.

- Riskien rajoitteet

Rajoitteet liittyen muun muassa riskien arviointiin ja riskeihin vastaamiseen.

- Riskitoleranssi

Hyväksyttävissä olevien riskien tasot, tyypit ja vakavuusasteet.

- Prioriteetit ja valinnat / kompromissit

Organisaation eri toimintojen suhteellinen merkitys, vaihtokaupat (trade-offs) erilaisten organisaation kohtaamien riskien välillä, aikaikkunat joiden kuluessa riskeihin täytyy pystyä vastaamaan, mahdolliset riskeihin vastaamisessa tunnistetut epävarmuustekijät.

(NIST, 2011).

Riskien raamittamiseen ja riskien hallinnan strategiaan kuuluvat myös strategisen tason päätökset siitä, miten organisaation ylempi johto menettelee liittyen organisaation toimintaan ja suojeltaviin varantoihin kohdistuviin riskeihin. (NIST, 2011). NIST:n standardin mukaisen riskienhallinnan ensimmäinen vaihe määrittelee perustan tuleviin vaiheisiin liittyen. Sen tarkoituksena on tehdä linjaukset ja päätökset, joilla luodaan perusta riskien arvioinnille ja konkreettisille toimille, joilla riskejä pyritään seuraavissa vaiheissa vähentämään.

Riskien arviointi
Standardin toinen komponentti on riskien arviointi. Se määrittää keinot, joilla organisaatio arvioi ensimmäisessä vaiheessa luotujen raamien kontekstissa. (NIST, 2011). Riskien arvioinnin tavoitteena on identifioida:

- Organisaatiota kohtaavat uhkat

Uhkat voivat kohdistua organisaation toimintaan, varantoihin tai yksilöihin ja ne voivat suuntautua myös toisten organisaatioiden kautta.

- Sekä ulkoiset että sisäiset haavoittuvuudet

Haavoittuvuudet eivät välttämättä rajoitu ainoastaan tietojärjestelmiin vaan niihin voi sisältyä myös esimerkiksi liiketoimintaprosesseista, turvallisuusarkkitehtuurista, laitteistosta tai jakeluketjusta muodostuvat haavoittuvuudet.

- Vahinko / haitta

Mikä on organisaatioon kohdistuva haitta, jos uhkat pääsevät hyödyntämään haavoittuvuuksia?

- Vahingon / haitan esiintymisen todennäköisyys

(NIST, 2011).

Prosessin tuloksena on riskin määritys, eli arvo tai tulos sille, mikä on vahingon vaikutus organisaatiolle ja mikä on vahingon todennäköisyys. Riskien arvioinnin tukemiseksi organisaation tulisi määrittää:

- Työkalut, tekniikat ja metodologiat joita riskien arviointiin käytetään
- Olettamukset liittyen riskien arviointiin
- Rajoitteet, jotka saattavat vaikuttaa riskien arviointiin
- Roolit ja vastuut
- Keinot, miten tieto kerätään, käsitellään ja miten siihen liittyen kommunikoidaan organisaatiossa
- Miten riskien arviointi käytännössä toteutetaan
- Miten tiedot uhkista hankitaan.

(NIST, 2011).

Riskeihin vastaaminen
Kolmas komponentti määrittelee sen, miten organisaatio vastaa riskiin sen jälkeen, kun se määritetty riskien arvioinnin kautta. Komponentin tarkoituksena on tarjota johdonmukainen ja koko organisaation kattava vastatoimi määritettyä riskiä vastaan riskien raamittamisen ja arvioinnin perusteella. (NIST, 2011). Kolmas komponentti sisältää seuraavat osa-alueet:

- Vaihtoehtoisten toimintatapojen kehittäminen riskeihin vastaamiseksi
- Näiden vaihtoehtoisten toimintatapojen arvioiminen
- Organisaation riskitoleranssin mukaisten toimintatapojen määrittely
- Vastatoimien toimeenpaneminen valittujen toimintatapojen mukaisesti

Organisaation tulee määritellä, minkälaisia vastatoimia toimeenpannaan ja mihin niillä pyritään (esimerkiksi riskin hyväksyminen, välttäminen, vähentäminen tai siirtäminen)

(NIST, 2011).

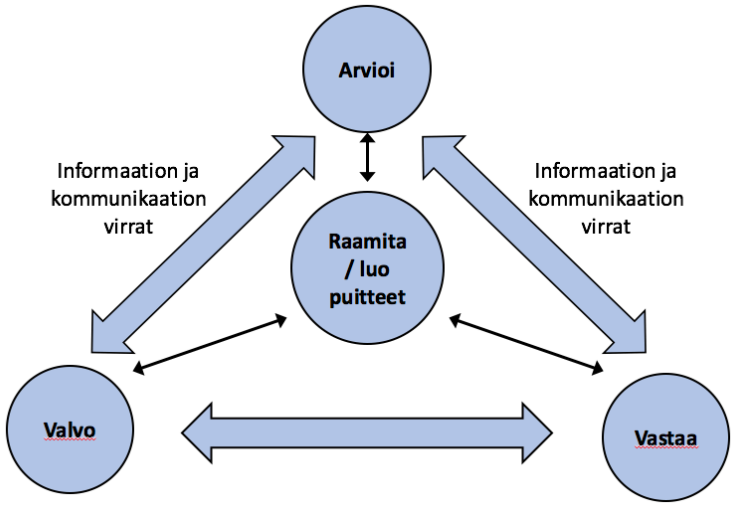
Organisaation tulee myös määrittää työkalut, tekniikat ja metodologiat, joita käytetään valittujen toimintatapojen kehittämiseen sekä se, miten valittuja toimintatapoja arvioidaan ja miten niihin liittyen kommunikoidaan organisaation sisäisesti ja organisaation ulkopuolelle. (NIST, 2011).

Riskien jatkuva seuranta
Menetelmän neljäs komponentti on riskien ja riskienhallinnan monitorointi ja tarkkailu. Monitoroinnin tarkoituksena on:

- Varmistaa, että riskejä vastaan valitut vastatoimet on toimeenpantu ja informaatioturvallisuudelle asetetut vaatimukset täyttyvät
- Määrittää käytössä olevien riskinhallintatoimien tehokkuus
- Tunnistaa riskien vaikuttavat muutokset organisaation informaatiojärjestelmille ja toimintaympäristölle.

(NIST, 2011).

Riskien seurantaan liittyvän komponentin tukemiseksi organisaatioiden tulee määritellä, miten ohjeiden noudattaminen ja vastatoimien tehokkuus todetaan. (NIST, 2011). Alla oleva kuvio esittää riskienhallinnan prosessin tiedon ja kommunikaation kulkemisen eri komponenttien välillä.



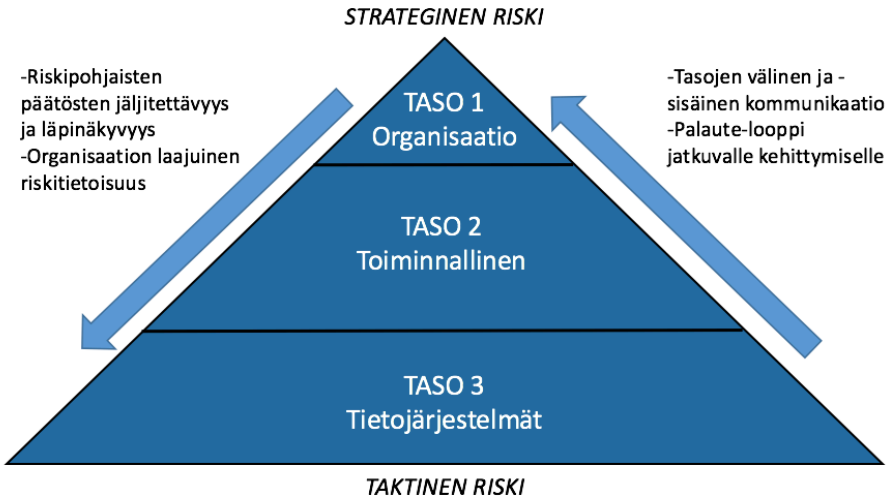
KUVIO: Riskienhallinnan prosessi (NIST, 2011, 8)

Nuolet kuvaavat tiedon liikkumista ja kommunikaatiota riskienhallinnan prosessissa. Ensimmäinen komponentti, riskien raamittaminen, antaa tietoa suoraan kaikille riskienhallinnan peräkkäisille komponenteille. Yksittäisen komponentin tuote (esimerkiksi riskienarvioinnin tulokset) toimivat syötteenä seuraavalle vaiheelle. Yhdessä nämä komponentit tuottavat päätöksentekijöille tietoa, joka auttaa heitä tekemään päätöksiä valittavien toimintatapojen suhteen. (NIST, 2011).

Nuolten kaksisuuntaisuus kuvaa informaation kulkemista kumpaankin suuntaan riskienhallinnan komponenttien välillä. NIST kuvaa riskienhallinnan joustavaksi prosessiksi, jossa tulee reagoida toimintaympäristön muutoksiin.

Riskienhallinnan ei pitäisi olla kaavamaista toimintaa, vaan tiedonkulun tulee olla saumatonta ja tarvittaessa täytyy pystyä esimerkiksi poikkeamaan vaiheiden suunnitellusta suoritusjärjestyksestä. (NIST, 2011).

NIST (2011) kuvaa riskienhallinnan prosessiksi, joka läpäisee koko organisaation ja kuvaa tätä alla olevan kuvion mukaisesti kolmiportaisella mallilla:



KUVIO: Riskienhallinnan monikerroksinen lähestymistapa (NIST, 2011, 9)

Tasot ovat organisationaalinen (taso 1), toiminnallinen taso (taso 2) ja tietojärjestelmätaso (taso 3). Riskienhallintaprosessin tavoitteena on organisaation riskeihin liittyvien toimintojen jatkuva kehittäminen ja prosessin tulisi toteutua saumattomasti koko organisaation läpi.

Ensimmäinen taso (taso 1) käsittelee riskiä organisationaalisesta näkökulmasta ja toteuttaa riskienhallinnan ensimmäisen vaiheen (riskien raamittaminen) tuottaen kontekstin seuraaville riskienhallinnan komponenteille. Ensimmäisen tason toiminta vaikuttaa suoraan tasoihin 2 ja 3. Ensimmäinen taso suorittaa priorisoinnin liittyen liiketoimintaan / prosesseihin. Nämä priorisoinnit vaikuttavat muun muassa investointistrategioihin ja rahoituspäätöksiin. Ensimmäisen tason strategiset päätökset vaikuttavat esimerkiksi tasolla 2 turvallisuusarkkitehtuurin kehittämiseen tai tasolla 3 erilaisten turvallisuusratkaisujen toteuttamiseen. (NIST, 2011).

Toinen taso (taso 2) käsittelee riskiä liiketoiminnan näkökulmasta. Se saa syötteen ensimmäisellä tasolla tehdyistä linjauksista. Tasolla 2 tehdään ratkaisuja ensimmäisen tason strategisten linjausten mukaisesti tarkoituksena tukea organisaation tehtävää ja ydintoimintoja. Tason 2 tulisi tuottaa niin sanottuja riski-tietoisia liiketoimintaprosesseja. Tasolla 2 tehdyt ratkaisut vaikuttavat suoraan tason 3 toimintaan.

Kolmas taso (taso 3) käsittelee riskiä tietojärjestelmien näkökulmasta. Se saa syötteensä tasoilta kaksi, eli riskin kontekstin määrittelystä ja tasolla 2 tehdystä valinnoista liittyen riskienhallinnan keinoihin. Tason 3 on lähimpänä taktisen tason käytännön toimintaa. Sen tehtävänä on tehdä käytännön toimintaan suoraan vaikuttavia ratkaisuja ja toteuttaa ylemmillä tasoilla määritettyjä ratkaisuja. Myös tällä tasolla tehtävien ratkaisujen tulisi perustua riskeihin, eli riskienhallintaprosessin tuottamaan tietoon. (NIST, 2011). NIST:n riskienhallinnan

kokonaisuus muodostuu kahden aiemmin esitellyn kuvion yhdistelmänä ja se on esitetty seuraavassa kuviossa:

KUVIO 6

Kokonaisuus rakentuu neljästä komponentista, jotka käsitellään koko organisaation kattavasti aina strategiselta ylätasolta taktiselle käytännön tasolle. Riskienhallinta kuvataan joustavana prosessina, jossa tiedon vaihtamista ja kommunikaatiota tapahtuu aktiivisesti organisaation eri tasojen ja riskienhallinnan eri komponenttien välillä. Vaikka malli esittääkin riskienhallinnan komponentit peräkkäisiksi tästä voidaan joustaa. Olennaista on se, että suoritettaessa riskienhallinnan eri vaiheita, otetaan huomioon muista vaiheista syntyvät tuotokset. (NIST, 2011).

Riskien arviointi

Riskienhallinta ja -arviointi on jatkuva prosessi ja riskien arviointia täytyy toteuttaa aktiivisesti koko järjestelmän elinkaaren tai organisaation toiminnan jatkumisen ajan. NIST:n menetelmä ei anna tiukkoja vaatimuksia sille, millä tarkkuudella tai menetelmällä riskien arviointi tulisi käytännön tasolla toteuttaa. NIST korostaa menetelmän joustavuutta ja organisaation vapautta valita omaan toimintaympäristöönsä parhaiten sopivat menetelmän riskien arvioimiseksi. Riskien arviointi ei koskaan anna tarkkoja tai yksiselitteisiä tuloksia. Organisaation tulisi aina tarkastella kriittisesti käytetyn arviointimenetelmän rajoitteet, arvioinnin aineistona käytetyn datan subjektiivisuus, laatu ja luotettavuus sekä tulosten tulkinnallisuus ja arvioinnin suorittaneiden henkilöiden tai ryhmien ammattitaito. (NIST, 2012).

Riskien arviointi on riskienhallinnan prosessin olennainen osa. Riskien arviointia käytetään organisaation toimintaa kohdistuvien riskien tunnistamiseen, arviointiin ja priorisointiin. Riskien arvioinnin tarkoitus on välittää päätöksentekijöille heidän tarvitsemaansa tietoa tunnistamalla organisaatiota uhkaavat oleelliset uhkat, haavoittuvuudet ja niiden vaikutukset sekä arvioimalla niiden esiintymisen todennäköisyyttä. (NIST, 2012).

NIST:n riskien arvioinnin mallin mukaan arviointia voidaan suorittaa kaikilla kolmella organisaation tasolla (organisationaalinen / strateginen taso, toiminnallinen taso, järjestelmätaso). Kaksi ylempää tasoa (strateginen ja toiminnallinen) käyttävät riskien arviointia arviointien, prosessien ja liiketoiminnan näkökulmasta. Alin, lähinnä käytäntöä oleva taso, käyttää riskien arviointia käytännön toiminnan näkökulmasta käsin. Riskien arviointi ei ole toimenpide, joka toteutetaan kerran. Riskien arviointi ei tuota kerralla päättäjien käyttöön pysyvää ja lopullista tietoa. Sen sijaan riskien arviointi tulee olla toistuva prosessi, joka viedään läpi kaikilla organisaation tasoilla. Riskien arvioinnin kautta organisaatiot määrittelevät riskit, jotka uhkaavat niiden ydintoimintoja. (NIST, 2012).

Riskien arvioinnin kautta voidaan saada tukea riskeihin perustuvaan päätöksentekoon muun muassa seuraaviin toimintoihin:

- Tietoturva-arkkitehtuurin kehittäminen
- Tietojärjestelmien yhteen liittämisen vaatimusmäärittely
- Järjestelmien turvallisuusratkaisujen suunnittelu
- Valtuutusten suunnittelu
- Liiketoimintojen / prosessien muokkaus
- Turvallisuusratkaisujen toimeenpano
- Turvallisuusratkaisujen käyttäminen ja ylläpitäminen

(NIST, 2012).

Ajan mittaan organisaation toiminta, käytettävät järjestelmät, uhkat ja toimintaympäristö muuttuvat ja kehittyvät. Tämän vuoksi myös riskien arvioinnin tulokset tulee säännöllisesti arvioida uudelleen. (NIST, 2012).

Riskien arvioinnin prosessi

NIST:n menetelmä kuvaa riskien arvioinnin neljävaiheiseksi prosessiksi. Menetelmän mukaiset vaiheet riskien arvioinnin toteuttamiselle ovat:

1. Arviointiin valmistautuminen
2. Arvioinnin suorittaminen
3. Tulosten jakaminen ja tuloksista kommunikoiminen
4. Arvioinnin ylläpitäminen.

(NIST, 2012).

Arviointiin valmistautuminen

Ensimmäinen vaihe on arviointiin valmistautuminen. Valmistautumisen tavoitteena on muodostaa konteksti varsinaiselle arvioinnille. Konteksti tulee riskienhallinnan kokonaisuuden ensimmäisen vaiheen kautta (riskien "raamittaminen" / strategian luominen). (NIST, 2012).

Valmistautumisen alussa täytyy määrittää koko arviointiprosessin tavoite. Tavoitteella tarkoitetaan sen informaation määrittelemistä, mitä arvioinnin tulisi tuottaa sekä niitä päätöksiä, joiden tekemistä arvioinnin tulosten tulisi tukea. Riskien arvioinnin tavoitteiden muodostumiseen vaikuttaa oleellisesti arvioinnin tyyppi eli se, että ollaanko tekemässä ensimmäistä arviota tai päivittämässä jo olemassa olevaan riskien arviointia. (NIST, 2012).

Valmistautumisen ja tavoitteiden asettamisen jälkeen tulee määritellä riskien arvioinnin laajuus. Laajuuden määrittämisen kautta pystytään hahmottamaan, mitä riskien arvioinnissa otetaan huomioon. Tämä määrittely vaikuttaa sen informaation laajuuteen, mitä prosessin jälkeen on käytettävissä. Laajuuden määrittelee lähtökohtaisesti organisaation ylempi johto, joka on alun perin käynnistänyt riskien arvioinnin prosessin ja määrittänyt riskienhallinnan strategian. (NIST, 2012).

Lisäksi tulisi kyetä määrittelemään, mitä oletuksia tai rajoituksia riskien arviointiin liittyy. Näihin liittyvät esimerkiksi olettamukset, rajoitukset, riskitoleranssit ja priorisoinnit, joita organisaatiot tekevät osana päätöksentekoprosessiaan. Edellä mainitut asiat vaikuttavat suoraan siihen, miten riskien arviointi käytännössä suoritetaan. Ennen varsinaista riskien arviointia organisaation tulee määrittää esimerkiksi minkä tyyppiset uhkat se ottaa arvioinnissa huomioon

(esimerkiksi sisäiset tai ulkoiset uhkat tai jokin tietty tiukasti rajattu uhka), mitä uhkatapahtumia huomioidaan (esimerkiksi tietojen kalastelu tai palvelunestohyökkäys) ja millä tarkkuudella. Lisäksi tulee määrittää, minkälaiset haavoittuvuudet arvioinnissa otetaan huomioon. Ennen arvioinnin suorittamista tulee myös päättää, miten todennäköisyydet ja uhkien vaikutukset määritellään sekä se, miten paljon jäännösriskiä voidaan hyväksyä. (NIST, 2012).

Merkittävänä riskien arvioinnin suorittamiseen vaikuttavana valmistautumistoimenpiteenä on myös arvioinnin lähestymistavan valinta. Arvioinnin tuloksia voidaan esittää esimerkiksi määrällisesti, laadullisesti. Lisäksi tulee määrittää, mistä näkökulmasta riskit analysoidaan (uhkien, vaikutusten tai haavoittuvuuksien näkökulmasta). Arvioinnin ja analysoinnin näkökulmien yhdistelmänä saadaan koko riskien arvioinnin prosessin analyyttinen näkökulma, jossa tulee lisäksi määritellä se tarkkuus, millä erilaisia uhkia pyritään arvioimaan ja analysoimaan. (NIST, 2012).

Arviointiin valmistautumiseen kuuluu myös se, että määritellään ne tietolähteet, joista arvioinnin perusteena käytettävää dataa hankitaan. Tämä data käsittää tiedon uhkista, haavoittuvuuksista ja niiden vaikutuksista. Tätä tietoa voidaan hankkia niin organisaation sisältä kuin sen ulkopuoleltakin. (NIST, 2012).

Ennen varsinaista riskien arviointia suoritettavat vaiheet ovat prosessin onnistumisen kannalta erittäin tärkeitä. Kokonaisprosessi on laaja ja monimutkainen ja se vaatii onnistuakseen vahvan pohjatyön ja selkeät rajaukset.

Arvioinnin suorittaminen

Riskien arvioinnin prosessin toinen vaihe on arvioinnin suorittaminen. Tämän vaiheen tarkoituksena on tuottaa tieto niistä riskeistä, jotka kohdistuvat organisaatioon. Tätä tietoa käytetään hyväksi riskienhallinnan myöhemmissä vaiheissa päätöksenteon yhteydessä. Suorittaakseen riskien arvioinnin organisaatioiden tulee analysoida uhkia ja haavoittuvuuksia, niiden vaikutuksia ja todennäköisyyksiä sekä prosessiin liittyviä epävarmuustekijöitä. Tähän vaiheeseen liittyy myös tarvittavan informaation kerääminen niiden reunaehtojen mukaisesti, jotka on määritelty arviointiin valmistauduttaessa. Ihannetapauksessa riskien arviointi kattaisi koko organisaation toiminnan käsittävät uhkat ja haavoittuvuudet, mutta organisaation käytössä olevat resurssit ja arvioinnille asetettu tavoite saattavat vaikuttaa tähän oleellisesti. (NIST, 2012).

Riskien arviointi on prosessi, joka NIST:n menetelmässä on jaettu useampiin alavaiheisiin. Nämä vaiheet on esitetty alla tietyssä järjestyksessä, mutta menetelmä antaa organisaatiolle vapauden muokata vaiheet tarvittaessa sopivampaan järjestykseen. Jos vaiheiden järjestystä muutetaan, tulee huomioida, että ne edelleen täyttävät riskien hallinnan strategiassa ja arviointiin valmistautumisen vaiheessa asetetut tavoitteet. (NIST, 2012).

Arvioinnin alussa tulee tunnistaa uhkien lähteet. Tällä tarkoitetaan niitä lähteitä, jotka voivat muodostaa uhkan organisaation toiminnalle tai järjestelmille. Arvioinnissa tulee huomioida sekä sisäiset että ulkoiset uhkat. Tietolähteet, joista tätä dataa kerätään, tulee lähtökohtaisesti määrittää jo arviointiin valmistautumisen vaiheessa. Lisäksi tulee tunnistaa uhkien lähteet. Nämä lähteet voivat olla erilaisia riippuen siitä, millä organisaation tasolla arviointia suo-

ritetaan. Näiden vaiheiden jälkeen on oleellista tunnistaa organisaation haavoittuvuudet. Myös tämän vaiheen tulokset voivat vaihdella riippuen organisaation tarkastelutasosta ja tasoilla on yhteys toisiinsa. Organisaatioiden ja niiden toiminnan monimutkaisuudesta johtuen tarkasteltavien haavoittuvuuksien määrä voi kasvaa huomattavan suureksi. Tämä lisää analyysin kompleksisuutta. (NIST, 2012).

Uhkan esiintymisen todennäköisyyden arvioiminen on vaativa ja monimutkainen prosessi. Se riippuu monista aiemmissa vaiheissa määritellyistä asioista, kuten uhkatiedon hankkimisesta. Todennäköisyyden arvioinnin tulosten esitysmuoto riippuu siitä, miten se on määrätty esitettäväksi (esimerkiksi laadullinen tai määrällinen esitystapa). (NIST, 2012). Aiempien vaiheiden huolellinen suorittaminen korostuu etenkin todennäköisyyksien arvioinnissa. Jos riskien arvioinnin perusteita ei ole määritelty riittävän hyvin, ei todennäköisyyksien arvioinnilla ole realistisia edellytyksiä onnistua.

Seuraavaksi varsinaisessa riskien arvioinnissa suoritetaan riskien vaikutuksen arviointi. Sen tarkoituksena on potentiaalisten uhkatapahtumien haitallisten vaikutusten arviointi. Vaikutusten arviointi voi sisältää esimerkiksi niiden kohteiden tunnistamisen, joihin uhkien konkretisoituminen voi vaikuttaa suoraan tai epäsuoraan. Kullakin riskienhallinnan organisationaalisella tasolla on tässäkin vaiheessa omat vastuunsa. (NIST, 2012).

Arvioinnin suorittamisen viimeinen vaihe on riskin määrittäminen. Riski määritellään uhkan potentiaalisen vaikutuksen ja sen esiintymisen todennäköisyyden yhdistelmän kautta. Tämän vaiheen toteuttamiseen ja esittämistapaan vaikuttavat olennaisesti riskienhallinnan ja -arvioinnin aiemmissa vaiheissa tehdyt linjaukset siitä, millä laajuudella ja millä lähestymistavalla riskien arviointi toteutetaan. (NIST, 2012).

Tulosten jakaminen ja tuloksista kommunikoiminen

Riskien arvioinnin ja varsinaisen riskin määrittelyn jälkeen prosessin tuloksista täytyy kommunikoida päätöksentekijöiden kanssa. Tätä kautta päätöksentekijät saavat käyttöönsä prosessin tuottaman informaation oman toimintansa tueksi. Kommunikaation toteuttamiseen voidaan käyttää monia menetelmiä, kuten johdon palavereita tai raportteja ja se voidaan toteuttaa muodollisesti tai epämuodollisesti. Olennaista on se, että tämäkin vaihe on tietoisesti määritelty, mielellään jo prosessin varsinaiseen riskien arviointiin valmistavissa vaiheissa. Hyvän kommunikoinnin ja dokumentoinnin kautta riskien arvioinnin tulokset ovat niitä tarvitsevien henkilöiden käytettävissä ja niitä voidaan ylläpitää. (NIST, 2012).

Arvioinnin ylläpitäminen

Riskien arvioinnin viimeiseksi vaiheeksi NIST määrittää arvioinnin ylläpitämisen. Sen tarkoituksena on ylläpitää ajantasaista tietoa organisaatioon mahdollisesti kohdistuvista riskeistä. Riskien arvioinnin tulokset auttavat päätöksenteossa ja ohjaavat riskeihin kohdistuvia vastatoimia. Riskien arviointi ei ole prosessi, joka pysähtyy jossain vaiheessa, vaan sen tulisi jatkua riskien tarkkailun ja arvioinnin ylläpitämisen kautta koko ajan. Tarkkailun kautta voidaan määrittää

vastatoimien tehokkuus, mahdolliset muutokset riskiympäristössä sekä todentaa ohjeiden ja määräysten noudattaminen. (NIST, 2012).

LIITE 8 STANDARDIN REFERAATTI - OCTAVE ALLEGRO

OCTAVE Allegro on Carnegie Mellon yliopiston Software Engineering Instituten (SEI) uusin OCTAVE -menetelmä. OCTAVE tulee sanoista *Operationally Critical Threat, Asset, and Vulnerability Evaluation.* Suomeksi tämä tarkoittaa operatiivisesti kriittisten uhkien, suojattavien kohteiden ja haavoittuvuuksien arviointia. Ensimmäinen kehitysversio julkaistiin syyskuussa 1999 ja aikaisemmat menetelmät ovat OCTAVE ja OCTAVE-S. OCTAVE -menetelmä on yksi de facto -standardeista tietoturvallisuuden ammattilaisten yhteisössä. (Caralli, Stevens, Young & Wilson, 2007). Vapaasti kääntäen de facto tarkoittaa tässä tapauksessa yleisesti hyväksyttyä menetelmää, jota ei kuitenkaan ole lakien tai säännösten nojalla määritelty. (Oxford Dictionaries, 2016b).

Taulukko: OCTAVE -menetelmän kehitys (Caralli ym., 2007, 2)

Ajankohta	**Julkaisun nimi**
syyskuu 1999	OCTAVE Framework, versio 1.0
syyskuu 2001	OCTAVE Framework, versio 2.0
joulukuu 2001	OCTAVE Criteria, versio 2.0
syyskuu 2003	OCTAVE-S, versio 0.9
maaliskuu 2005	OCTAVE-S, versio 1.0
kesäkuu 2007	OCTAVE Allegro versio 1.0

OCTAVE -menetelmä

Ensimmäinen OCTAVE -menetelmä perustuu organisaation sisältä kootun monialaisen analyysiryhmän työpajatyöskentelyyn. Analyysiryhmään kuuluu ylimmän johdon edustajia, eri sektoreiden johtoa ja henkilöstöä sekä jäseniä organisaation tietotekniikkaosastolta. (Alberts & Dorofee, 2002; Woody, 2006). OCTAVE -menetelmän käyttöönsä ottaneet yritykset ovat usein räätälöineet menetelmän organisaation tarpeiden mukaiseksi (Woody, 2006). Woodyn (2006) mukaan OCTAVE -menetelmä on tarkoitettu yli 300 henkilön suuryrityksille, joissa on:

- monikerroksinen hierarkia
- oma tietojenkäsittely infrastruktuuri
- kyky käyttää haavoittumisen arviointityökaluja
- kyky tulkita haavoittumisen arvioinnin tuloksia

Octave -menetelmä suoritetaan kolmessa vaiheessa (Alberts & Dorofee, 2002; Caralli ym., 2007), joista ensimmäisessä analyysiryhmä tunnistaa organisaation kannalta tärkeät tiedot ja niihin liittyvän turvaamisstrategian. Ryhmä päättää tämän jälkeen organisaation kannalta tärkeimmät tiedot ja kirjaa turvallisuusvaatimukset näille tiedoille sekä tunnistaa tietoihin mahdollisesti kohdistuvat uhat. Toisessa vaiheessa analyysiryhmä suorittaa tiedon rakenteiden arvioinnin ja täydentää mahdollisesti ensimmäisen vaiheen arviota. Kolmannessa vaiheessa

sa analyysiryhmä tunnistaa riskejä ja laatii riskien vähentämissuunnitelman tärkeille tietovarannoille. (Alberts & Dorofee, 2002; Caralli ym., 2007).

OCTAVE-S -menetelmä

Carallin (2007) mukaan OCTAVE-S -menetelmä on suunnattu pienille organisaatioille. OCTAVE:n uusin versio 1.0 on luotu erityisesti organisaatioille, joissa on alle 100 työntekijää. OCTAVE-S -menetelmässä on samat kolme vaihetta kuin aiemmassa OCTAVE -menetelmässä. Analyysiryhmä koostuu tavanomaisesti kolmesta viiteen henkilöstä, joilla on laaja-alainen kokemus organisaation toiminnasta. Henkilöiden valinnassa painotetaan organisaation kannalta tärkeään tietoon, turvallisuusvaatimuksiin, uhkiin ja turvallisuuskäytänteisiin liittyvää osaamista. Toinen merkittävä eroavaisuus on OCTAVE-S -menetelmän rakenteessa. Menetelmä sisältää valmiiksi työpohjia ja tietoturvamalleja turvallisuuden ja riskien arviointiin. Tämä helpottaa varsinkin henkilöitä, joilla on vähemmän kokemusta toiminnasta. Kolmanneksi OCTAVE-S -menetelmä on suunniteltu sisältämään mahdollisimman vähän organisaation informaatioinfrastruktuurin analysointia. (Caralli ym., 2007).

OCTAVE- ja OCTAVE-S -menetelmät on otettu käyttöön monissa organisaatioissa onnistuneesti ja ne ovat kestäneet hyvin aikaa. Woodyn (2006) mukaan OCTAVE on suunniteltu riittävän joustavaksi, jotta organisaatioiden ainutlaatuiset analyysin tarpeet voidaan ottaa huomioon räätälöityjen ominaisuuksien kautta. OCTAVE Allegro pyrkii yksinkertaistamaan aiempien menetelmien prosesseja. (ISACA, 2009). OCTAVE Allegro -menetelmää voidaan tarvittaessa käyttää kuten aikaisempia OCTAVE- ja OCTAVE-S -menetelmiä hyödyntäen työpajatyöskentelyä ja valmiita työpohjia. Tulevaisuudessa informaation turvaaminen tulee liittää yhä tiiviimmin liiketoiminnan prosesseihin ja palveluihin. OCTAVE Allegro auttaa organisaatioita parantamaan nopeasti riskien arvioinnin valmiuksia ja kehittämään olemassa olevaan taitoon perustuvan menetelmän osana tietoturvallisuuden riskienhallinnan kokonaisuutta. (Caralli, 2007).

Riskienhallinta

OCTAVE -menetelmällä pyritään ratkaisemaan käytännön ongelmia. Menetelmä pyrkii optimoimaan riskien arvioinnin prosessia, jotta organisaation on mahdollista saada riittävän hyvä lopputulos resursoimalla mahdollisimman vähän aikaa, henkilötyövoimaa ja muut rajoitteet huomioiden. (Caralli ym., 2007). Perinteisestä teknologia-keskeisestä ja taktisesta näkökulmasta suunnitelluista riskienarviointi menetelmistä poiketen OCTAVE -menetelmä on kohdennettu organisaation riskeihin strategiselle tasolle. (ISACA, 2009).

Riskienhallinnan onnistumisen kannalta keskeisiä elementtejä OCTAVE -menetelmässä ovat (Caralli ym., 2007; ISACA, 2009):

- ylimmän johdon tuen saaminen
- johtajan ja analyysiryhmän valitseminen OCTAVE -menetelmän arvioinnin johtoon
- arvioinnin laajuuden päättäminen
- arviointiin osallistuvien henkilöiden valinta

Ylimmän johdon sitoutuminen ja projektille osoitettu tuki ovat keskeisiä tekijöitä, koska menetelmä edellyttää (Caralli ym., 2007; ISACA, 2009):

- Näkyvää ja jatkuvaa tukea menetelmälle
- Aktiivista henkilöstön kannustusta osallistumiseen
- Vastuun ja valvonnan delegointia analyysiryhmälle
- Sitoutumista resurssien osoittamiselle
- Hyväksyntää tulosten tarkastamiselle ja päätöksenteolle seuraavissa vaiheissa

Riskienhallinnan tavoitteet

OCTAVE -menetelmien tavoite ja keskeinen hyöty ovat mahdollisuus yhdistää organisaation tavoitteet tietoturvallisuuden tavoitteisiin. Onnistuneesti menetelmää käyttäneet organisaatiot kykenevät organisaation ja operatiivisen näkökulman liittämiseen tietoturvallisuuden riskien hallinnassa, jolloin toiminta muuttuu haavoittuvuuksien hallinnasta ja reaktiivisesta toiminnasta kohti suurempaa tietoturvallisuuden riskienhallinnan kokonaisuutta. (Caralli ym., 2007). Aiempien OCTAVE -menetelmien yhteistyötä painottuva filosofia tuo yhteen organisaation henkilöstöä eri toiminnan tasoilta yhteisen päämäärän saavuttamiseksi. Organisaation sisällä oleva ymmärrys, kokemus ja mielipiteet voidaan ottaa näin ollen paremmin huomioon. Työryhmän työpajojen kautta tapahtuva tiedon kerääminen liitettynä myöhempään analysointiprosessiin tuo johtotasolle tietoa jota on muilla keinoin hankala saada (Caralli ym., 2007).:

- organisaation sisällä tiedonkulkua estävistä tekijöistä
- tietoturvapolitiikoiden tulkinnoista eri organisaation tasoilla
- eroista käytännön toiminnassa ja halutulla vaikutuksella

Aikaisempien OCTAVE- ja OCTAVE-S -menetelmien julkaisusta on kulunut jo melko pitkä aika. Tietoturvallisuuden toimintaympäristö on kuitenkin muuttunut organisaatioiden näkökulmasta hyvin paljon julkaisujen jälkeen. Merkittävä tekijä muutoksessa on siirtyminen kohti tietoon pohjautuvaa riskien arviointia. (Caralli ym., 2007). Stevensin (2005) mukaan tietovarojen, *assetien*, ollessa tietoturvallisuuden arvioinnin keskeinen tekijä voidaan kaikki muut *assetit* tuoda prosessiin *containereina*. Container tarkoittaa *objektia, joka säilyttää tai kuljettaa jotain* (Oxford Dictionaries, 2016a). Säilytyspaikka voi olla henkilö, esine, asia tai teknologia. Henkilö esimerkiksi voi säilyttää tietoa, kuljettaa tietoa kommunikoimalla toisten ihmisten kanssa ja prosessoida tietoa ajattelemalla. Objekti voi olla paperinpala, jolle on kirjoitettu tietoa ja teknologia esimerkiksi tietokanta. (Caralli ym., 2007). Tiedolle aiheutuvat uhat arvioidaan sen perusteella missä tieto sijaitsee ja prosessissa käsiteltävien tietovarojen määrä saadaan rajatummaksi. Keskittyminen organisaation tietovaroihin rajoittaa tehokkaasti kerättävän, prosessoitavan, järjestettävän, analysoitavan ja ymmärrettävän tiedon määrää, jotta riskien arviointi voidaan suorittaa. Osassa organisaatioita OCTAVE -menetelmää on aiemmin ollut hankala toteuttaa monimutkaisuudesta ja laajuudesta johtuen. Prosessiasiakirjojen ja työkirjojen läpikäyminen

sekä tarvittavan datan kerääminen organisaatiossa ovat haasteellisia tehtäviä. Aiemmista menetelmistä saadut kokemukset ovat olleet perustana uusimmalle OCTAVE Allegro -menetelmälle. (Caralli ym., 2007). Uuden menetelmän muodostamiseen johtivat seuraavat keskeiset tekijät (Caralli ym., 2007; ISACA, 2009).:

- käytettävyyden parantaminen
- riskien arvioinnin soveltamisalan jalostamiselle
- datan keräämisen ja uhkien tunnistamisen tekeminen suoraviivaisemmaksi
- henkilöstön harjoittelun ja tarvittavan tietotason vaatimusten vähentäminen
- institutionalisoinnin ja toistettavuuden parantaminen
- teknologisen näkökulman pienentäminen
- organisaation säännösten noudattamisen tukeminen

Caralli ym. (2007) mukaan ensimmäinen vaatimus parannetulle menetelmälle oli helppokäyttöisyys. Helppokäyttöisyyttä voidaan kuvata seuraavien näkökulmien kautta: menetelmän tulee koostua yksinkertaisista, mahdollisimman vähän opettelua vaativista prosesseista, toiseksi kerättävän ja hallinnoitavan datan sekä laadittavien työkirjojen määrän tulee vähentyä ja prosessin tulee kohdistua helposti määriteltävään ja käsiteltävään määrään tietoa. Toiseksi OCTAVE Allegron tulee mahdollistaa käyttäjän keskittyä tietoihin, jotka ovat tärkeimpiä. Tämä on mahdollista systemaattisen ja jatkuvan prosessin kautta. Tieto ja muut tekijät kuten ihmiset, teknologiat ja laitteistot tulee nähdä suurempana kokonaisuutena, jolloin voidaan mahdollisesti vähentää päällekkäisyyttä uhkien tunnistamisessa, analyysissä ja uhkien vähentämisen suunnittelussa. Kolmanneksi päivitetyn OCTAVE menetelmän tulee olla helposti institutionalisoitavissa organisaation rakenteisiin. Tämä oli mahdollista vähentämällä tarvittavaa ennakkotiedon määrää riskienhallinnasta ja informaatioteknologiasta. Menetelmän suorittamiseen osallistuvien henkilöiden määrä on näin ollen helposti nostettavissa suuremmaksi vähäisellä koulutuksella. Neljänneksi menetelmän tuli sitoa vähemmän resursseja. Tavoitteena on helppokäyttöisyydellä, vähemmällä datan käsittelyllä ja prosessoinnilla pitää menetelmän sitoman resurssin määrä mahdollisimman vähäisenä. Menetelmän piti osittain myös korjata käyttäjän tekemiä virheellisiä päätöksiä ennalta. Viidenneksi menetelmän tulee jatkuvana prosessina olla toistettavissa soveltuvin osin, jolloin kyetään näkemään riskienhallinnan ja turvallisuustoimien tehokkuuden tila organisaatiossa. Kuudenneksi menetelmän tuloksia tulee pystyä käyttämään organisaation toimintaa tukevasti. Menetelmän käytön tulee tuottaa jatkuvia ja vertailukelpoisia tuloksia koko organisaatiossa. Seitsemänneksi riskien arvioinnin menetelmänä OCTAVE Allegron tulee olla helposti ymmärrettävissä, käytettävissä ja tuottaa tarkoituksenmukaisia tuloksia, jotta työntekijät voivat paremmin tehdä työnsä. Kahdeksanneksi menetelmän tulee tukea organisaation kykyä toimia nopeasti ja saavuttaa politiikoiden noudattaminen tehokkaasti. Riskienarvioinnin menetelmän tulee tukea tietoturvallisuuden riskienhallintatoimia, jotka mahdollistavat organisaation erilaisten lakien ja sääntelyn noudattamisen.

Riskien arviointi
Perusteet
OCTAVE Allegro on tarkoitettu helpottamaan ja parantamaan nopeasti organisaatioiden omaa riskien arvioinnin kykyä. Menetelmän riskien arvioinnin perusteisiin kuuluu, että kaikkien organisaation toiminnallisten alueiden tulee toimia samoihin riskitekijöihin perustuvien arvioiden kautta. OCTAVE Allegron prosessi kohdistuu organisaation keskeisiin toimintoihin operatiivisten yksikköjen tasolla organisaatiossa. Lopputuloksena syntyy riskien arvioinnin suunnitelma, jonka tarkoitus on olla juuri kohdeorganisaatiolle kohdistettu ja kohdeorganisaation tarpeet huomioiden rakennettu. Teoriassa organisaation tulisi kyetä puuttumaan tunnistettuihin riskeihin operatiivisella tasolla ja viemään ne osaksi organisaation suurempia riskien lieventämisstrategioita. (Caralli ym., 2007).

Riskien arvioinnin prosessi
OCTAVE Allegro koostuu kahdeksasta toisiaan seuraavasta toimenpiteestä, jotka on jaettu neljään eri vaiheeseen. Seuraavassa kuviossa kuvataan OCTAVE Allegron toimenpiteet ja vaiheet.

KUVIO 7

OCTAVE Allegron toimenpiteiden tulokset toimivat seuraavan toimenpiteen pohjana. Alla on Caralli ym. (2007) tarkemmat kuvaukset vaiheiden ja toimenpiteiden sisällöstä:

Ensimmäisessä vaiheessa organisaatiossa luodaan kriteerit riskien mittaamiselle organisaation toiminnan mukaisesti.

Toimenpide 1: Laadi riskien mittaamisen kriteerit

Organisaatio määrittää mitkä osa-alueet ovat kaikkein tärkeimpiä liiketoiminnan ja tehtävän kannalta. Osalle organisaatiosta tällainen osa-alue voi olla esimerkiksi asiakassuhteet, kun taas toisille organisaatioille sääntelyn noudattaminen on tärkeintä. Octave Allegro sisältää työpohjia, joita voi käyttää asioiden tärkeysjärjestyksen määrittämisessä.

Toisessa vaiheessa kriittiseksi määritellyt tiedot profiloidaan. Profiloinnissa luodaan selkeät rajat kriittiselle tiedolle, tunnistetaan turvallisuusvaatimukset ja tunnistetaan tiedon säilytys-, välitys- ja prosessointitilat.

Toimenpide 2: Luo turvattavien riskien profiili

Organisaatiossa luodaan profiilit valituille turvattaville tiedoille. Profiili kuvaa tiedon yksilölliset ominaisuudet, piirteet ja arvon. Tarkoitus on selkeästi kuvailla turvattava tieto, jotta turvallisuusvaatimukset voidaan määritellä riit-

tävän tarkasti. Yksittäisen tiedon profiili taltioidaan yhdelle työpohjalle, joka toimii uhkien ja riskien tunnistamisen alustana seuraavissa toimenpiteissä.

Toimenpide 3: Tunnista turvattavien tietojen säilyttäjät (containers)

Kuvataan säilyttäjät (containers), joissa tietoa säilytetään, kuljetetaan ja prosessoidaan. Tiedon säilyttäjien tunnistaminen tulee kohdistua kaikkiin organisaation käyttämiin palveluihin. Organisaation tietovaroja saatetaan säilyttää myös organisaation suoran valvonnan ulkopuolella. Osa IT-infrastruktuurista on usein ulkoistettu, jolloin palveluntarjoajien hallussa on tiedon välitykseen käytetty laitteisto. Organisaation tarpeet voivat näin olla ristiriidassa palveluntarjoajan tuottaman palvelun kanssa.

Kolmannessa vaiheessa tunnistetaan uhat toisen vaiheen tiedon säilytys-, välitys- ja prosessointitiloille.

Toimenpide 4: Tunnista huolenaiheet

Tunnistetaan olosuhteet ja tilanteet, joissa organisaation tietoon voi kohdistua uhkia. Reaalimaailman ilmiöiden kuvaaminen ja mahdolliset seuraukset tunnistetaan nopeasti yleisellä tasolla. Kaikkien mahdollisten tilanteiden kuvaaminen ei ole tarpeellista vaan analyysiryhmä pohtii ensimmäisenä mieleen tulevat asiat.

Toimenpide 5: Tunnista uhkakuvat

Viides toimenpide jakaantuu kahteen toimenpiteeseen. Ensimmäisessä vaiheessa edellisen toimenpiteen 4 huolenaiheet laajennetaan uhkaskenaarioihin tai -näkymiin, jolloin uhan yksityiskohdat kuvataan tarkemmin. Viidennen toimenpiteen toisessa vaiheessa täydennetään uhkaskenaarioihin sisältyviä uhkia, joita ei ole aiemmin tunnistettu. Skenaarioita voidaan kuvata esimerkiksi alla olevassa taulukossa kuvatulla tavalla:

Taulukko: OCTAVE Allegro "Threat tree" (Caralli ym., 2007, 19)

Uhka	**Määritelmä**
Ihmiset käyttävät tekniikkaa	Uhkat organisaation tekniselle infrastruktuurille tai pääsy tiedon säilyttäjiin (tekniikka), jotka säilyttävät organisaation tietoa.
Ihmiset pääsevät fyysisesti käsiksi tietoon tai tiedon säilyttäjiin	Uhkat tässä luokassa kuvaavat uhkia, jotka ovat seurausta fyysisestä pääsystä tiedon säilyttäjään. Uhkat vaativat toteutuakseen henkilön suoran toiminnan ja voivat olla joko tarkoituksellisia tai tahattomia.
Tekniset ongelmat	Uhkat johtuvat ongelmista organisaation informaatioteknologiassa ja -järjestelmissä. Uhkat voivat olla esimerkiksi laitteisto- tai ohjelmistovikoja, haitallista koodia (virukset) ja muita järjestelmiin liittyviä ongelmia.
Muut ongelmat	Uhkat tässä luokassa ovat ongelmia tai tilanteita, jotka ovat organisaation oman hallinnan ulkopuolella. Uhkat voivat liittyä luonnonilmiöihin (esimerkiksi tulvat ja maanjäristykset) ja keskinäisestä riippuvuudesta johtuvat riskit. Keskinäisestä riippuvuudesta johtuvat riskit liittyvät esimerkiksi kriittisen infrastruktuurin saatavuuteen (esimerkiksi sähkö).

Viidennen toimenpiteen suorittaminen tarjoaa mahdollisuuden arvioida uhkien todennäköisyyttä uhkaskenaarioiden kuvauksissa. Tätä voidaan käyttää hyväksi myöhemmissä toimenpiteissä, kun organisaatiossa laitetaan riskien lieventämistoimenpiteet tärkeysjärjestykseen. Uhkien todennäköisyys on luokiteltu Octave Allegrossa korkeaan, keskitason ja matalaan.

Neljännessä vaiheessa riskit tunnistetaan ja analysoidaan sekä valmistaudutaan riskien lieventämistoimenpiteisiin.

Toimenpide 6: Tunnista riskit

Edellisen toimenpiteen 5 aikana uhat tunnistettiin ja toimenpiteen 6 aikana tunnistettujen uhkien mahdolliset seuraukset yritykselle kuvaillaan, jotta riskin profiili saadaan täydennettyä. Esimerkiksi organisaation sähköisen mainonnan keskeytyminen voi vaikuttaa organisaation maineeseen asiakkaiden keskuudessa sekä taloudelliseen asemaan.

Toimenpide 7: Analysoi riskit

Riskit järjestetään organisaation kannalta tärkeysjärjestykseen arvioimalla riskejä organisaation toiminnan näkökulmasta. Arvioinnissa lasketaan suhteellinen riski, jonka laskennassa otetaan huomioon missä määrin riski vaikuttaa haitallisesti organisaatioon ottaen huomioon useat vaikuttavuusalueet ja to-

dennäköisyys. Maineen ollessa organisaation tärkein turvattava osa-alue, riskit, jotka vaikuttavat organisaation maineeseen luovat suuremmat pisteet kuin riskit, joilla on vastaavan kaltaiset vaikutukset ja todennäköisyys muilla osa-alueilla.

Toimenpide 8: Valitse lähestymistapa riskien lieventämiseen

Organisaatiot päättävät tunnistettujen riskien joukosta sellaiset, jotka vaativat pienentämistä ja laativat näille riskeille lieventämisstrategian. Ensimmäiseksi riskit laitetaan tärkeysjärjestykseen lasketun arvon perusteella. Tärkeysjärjestyksen laatimisen jälkeen lieventämisstrategia ottaa huomioon tietovarojen arvon ja turvallisuusvaatimukset sekä tietovarojen säilytyspaikan ja organisaation yksilöllisen toimintaympäristön.

LIITE 9 STANDARDIN REFERAATTI – FERMA

FERMA on kansallisten riskienhallintayhdistysten kattojärjestö, jonka tarkoitus on optimoida jäsenyhdistystensä toimintaa kansallisten rajojen ulkopuolella tarjoamalla muun muassa yhteistyöverkoston. FERMA on perustettu vuonna 1974 ja on johtava riskienhallinnan organisaatio Euroopassa. FERMA on osa kansainvälistä IFRIMA (*International Federation of Risk and Insurance Management Associations*) yhdistystä. (FERMA, 2016). Suomen Riskienhallintayhdistys on FERMA:n jäsenyhdistys (Suomen Riskienhallintayhdistys, 2016).

FERMA -riskienhallinnan standardin julkaisivat alun perin vuonna 2002 Iso-Britannialaiset *The Institute of Risk Management (IRM), The Association of Insurance and Risk Manager (AIRMIC)* ja *The Public Risk Management Association (Alarm)*. FERMA, *Federation of European Risk Management Association*, hyväksyi standardin myöhemmin käyttöönsä. (IRM, 2016).

Riskienhallinta

FERMA -standardissa prosessi perustuu organisaation toiminnan tavoitteisiin. Organisaation toimijoille määritellään roolit ja vastuut riskien valvonnassa ja tiedottamisessa. Alla olevan taulukon mukaisesti hallitukselle, liiketoimintayksiköille, mahdolliselle riskienhallintayksikölle ja sisäiselle tarkastukselle on kaikille tunnistettu erityiset roolit. (FERMA, 2002; RIMS, 2011).

Taulukko: FERMA -standardin määrittelemät roolit ja vastuualueet

Toiminnallinen rooli	**Vastuut**
Hallitus	Riskienhallintaprosessin yleinen ohjaus, sisältäen strategisen riskienhallinnan, ja rakenteiden ja ympäristön luominen riskienhallinnan toiminnan tehokkuuden takaamiseksi
Liiketoimintayksiköt	Päivittäinen riskienhallinta, riskien havaitsemisen edistäminen operatiivisessa toiminnassa ja riskienhallinnan sisällyttäminen suunnitteluun ja työn operatiivisiin näkökulmiin.
Riskienhallintayksiköt	Riskitietoisen kulttuurin luominen, politiikoiden ja strategian asettaminen riskienhallinnalle. Riskienhallinnan vastuutaho sekä strategisella että toiminnallisella tasolla.
Sisäinen tarkastus	Keskittää toiminnan johdon tunnistamien merkittävien riskien ja riskienhallinnan prosessien tarkastaminen, auditointi, koko organisaatiossa. Luo varmuutta riskienhallintaan, tukee aktiivisesti ja osallistuu riskienhallinnan prosessiin.

Riskienhallinnan tavoitteet

Riskienhallinnan prosessissa organisaatiot suunnitelmallisesti pyrkivät osoittamaan toimintaansa liittyvät riskit. Riskienhallinnan tavoitteena on saavuttaa jatkuvaa hyötyä kaikessa organisaation toiminnassa. Hyvän riskienhallinnan tavoitteena on riskien tunnistaminen sekä käsittely ja tätä kautta hyödyn tuottaminen organisaation toiminnalle. Riskienhallinnan tavoitteena on laittaa järjestykseen mahdolliset hyödyt ja haitat, jotka voivat vaikuttaa organisaatioon.

Prosessi lisää onnistumisen mahdollisuutta ja toisaalta vähentää epäonnistumisen mahdollisuutta. Riskienhallinnan tulisi olla jatkuva ja kehittyvä prosessi, joka käy läpi koko organisaation strategian ja strategian käyttöönoton. Riskienhallinnan tavoite on olla liitoksissa organisaation kulttuuriin ja ylimmän johdon johtama prosessi sekä muuttaa strategian taktisiksi ja toiminnallisiksi tavoitteiksi, jotka osoittavat vastuullisuutta riskienhallinnassa koko organisaatiossa henkilön toimenkuvasta riippumatta. (FERMA, 2002).

Riskienhallinnan vaiheet

KUVIO 8

Riskienhallinnan prosessi sisältää organisaation strategisten tavoitteiden tunnistamisen, riskien arvioinnin, riskien uhkien ja mahdollisuuksien raportoinnin, päätöksenteon, riskien käsittelyn, jäännösriskin raportoinnin ja seurannan. Prosessi sisältää jatkuvan muodollisen auditoinnin ja muokkauksen. Aluksi tunnistetaan organisaatioon kohdistuvia epävarmuuksia. Organisaation toimintaympäristön, markkinoiden, lakien, sosiaalisten, poliittisten ja kulttuuristen piirteiden syvällinen tietämys ohjaa riskien tunnistamista. Riskien tunnistaminen edellyttää organisaation strategisten ja toiminnallisten tavoitteiden ymmärrystä. Riskien tunnistamisessa tulee käyttää järjestelmällistä menetelmää, jotta kaikki organisaatiota uhkaavat tekijät voidaan määritellä ja tätä kautta riskit selvittää. Liiketoimintaa ja päätöksiä voidaan tarkastella useilla eri tavoilla. Näkökulma voi olla esimerkiksi strateginen-, operatiivinen-, talouden-, tiedon- tai käytänteiden johtaminen. (FERMA, 2002).

Riskien kuvauksen tavoitteena on esittää jäsennellyssä muodossa tunnistetut riskit. Riskien kuvaamisen tulee olla kattavaa, joten menetelmän tulee olla hyvin suunniteltu. Riskit voidaan esittää muun muassa taulukkomuodossa, jolloin riskiä voidaan kuvata riskin tyypin, riskin aiheuttaman vahingon, laadun, haitallisuuden, riskin käsittelyn, mahdollisten vastatoimien ja strategiasekä politiikoiden kehittämisen kannalta. Keskeisimmät riskit voidaan määritellä muita riskejä tarkemmin. Riskien todennäköisyyden seuranta voi olla tilastollista tai laadullista riskin esiintymisen mahdollisuuden ja mahdollisten seurausten suhteen. Riskit voidaan lajitella seurausten suhteen esimerkiksi korkean tason-, keskitason- ja matalantason riskeihin. Riskit voidaan lajitella myös sen mukaan, kuinka todennäköistä riskin esiintyminen on. Riskianalyysiprosessin jälkeen on tarpeen arvioida arvioituja riskejä organisaation laatimien riskien tunnusmerkkien suhteen. Riskien tunnusmerkit voivat sisältää esimerkiksi kustannukset ja hyödyt, lainsäädännölliset vaatimukset, sosio-ekonomiset tekijät ja ympäristötekijät. Riskien arviointi ohjaa päätösten tekoa pohdittaessa riskin merkitsevyyttä organisaatiolle. Arvioinnissa määritellään, hyväksytäänkö riski tai käsitelläänkö sitä jollakin tavalla. Riskienkäsittelyssä valitaan ja otetaan käyttöön menetelmät riskien muokkaamiseksi. Riskien käsittely sisältää pääasiallisena keinona riskien hallitseminen/vähentämisen, mutta lisäksi riskien välttämisen, riskien siirtämisen ja riskien seurausten rahallisen kompensaation. Kaikkien riskien käsittelyjärjestelmien tulee sisältää vähintään organisaation tehokkaan ja taloudellisen toiminnan, tehokkaat sisäiset hallintakeinot ja lakien

sekä sääntelyn noudattamisen. Riskien raportointi ja viestintä sisältävät sekä sisäisen raportoinnin organisaation sisällä, että ulkoisen raportoinnin organisaation ulkopuolella. Riskienhallintaprosessin seuranta ja tarkastus takaavat, että riskit on tunnistettu ja arvioitu tehokkaasti sekä sopivat valvontamekanismit ja vastuut on määritelty. Politiikoiden ja standardien säännölliset auditoinnit tulee tehdä, jotta mahdolliset kehityskohteet voidaan tarkastaa. Prosessi varmistaa sopivien keinojen käytön ja organisaation sisällä olevan ymmärryksen ja sääntelyn noudattamisen. (FERMA, 2002).

Riskien arviointi

Perusteet

Riskien arviointi on prosessi, joka sisältää riskianalyysin ja riskien arvioinnin. FERMA:n määritelmä riskien arvioinnille perustuu ISO:n määritelmään. Riskianalyysi koostuu riskien tunnistamisesta, riskien kuvauksesta ja riskien todennäköisyyden arvioinnista. (FERMA, 2002).

Riskien arvioinnin prosessi

Riskien arviointi on prosessi, joka sisältää riskianalyysin (Risk Analysis) ja riskien arvioinnin (Risk Evaluation). FERMA:n määritelmä riskien arvioinnille perustuu ISO:n määritelmään. (FERMA, 2002).

Riskianalyysi koostuu riskien tunnistamisesta (Risk Identification), riskien kuvauksesta (Risk Description) ja riskien todennäköisyyden arvioinnin (Risk Estimation). *Riskien tunnistamisessa* tunnistetaan organisaatioon kohdistuvia epävarmuuksia. Organisaation toimintaympäristön, markkinoiden, lakien, sosiaalisten, poliittisten ja kulttuuristen piirteiden syvällinen tietämys ohjaa riskien tunnistamista. Riskien tunnistaminen edellyttää organisaation strategisten ja toiminnallisten tavoitteiden ymmärrystä. Riskien tunnistamisessa tulee käyttää järjestelmällistä menetelmää, jotta kaikki organisaatiota uhkaavat tekijät voidaan määritellä ja tätä kautta riskit selvittää. Liiketoimintaa ja päätöksiä voidaan tarkastella useilla eri tavoilla. Näkökulma voi olla esimerkiksi strateginen-, operatiivinen-, talous- tiedon- tai käytänteiden johtaminen. *Riskien kuvauksen* tavoitteena on esittää jäsennellyssä muodossa tunnistetut riskit. Riskien kuvaamisen tulee olla kattavaa, joten menetelmän tulee olla hyvin suunniteltu. Riskit voidaan esittää muun muassa taulukkomuodossa, jolloin riskiä voidaan kuvata riskin tyypin, riskin aiheuttaman vahingon, laadun, haitallisuuden, riskin käsittelyn, mahdollisten vastatoimien ja strategia- sekä politiikoiden kehittämisen kannalta. Keskeisimmät riskit voidaan määritellä muita riskejä tarkemmin. *Riskien todennäköisyyden seuranta* voi olla tilastollista tai laadullista riskin esiintymisen mahdollisuuden ja mahdollisten seurausten suhteen. Riskit voidaan lajitella seurausten suhteen esimerkiksi korkean tason-, keskitason- ja matalantason riskeihin. Riskit voidaan lajitella myös riskien todennäköisyyden mukaan. Riskianalyysiprosessin jälkeen on tarpeen arvioida arvioituja riskejä organisaation laatimien riskien tunnusmerkkien suhteen (Risk Evaluation). Riskien tunnusmerkit voivat sisältää esimerkiksi kustannukset ja hyödyt, lainsäädännölliset vaatimukset, sosio-ekonomiset tekijät ja ympäristötekijät. Riskien arviointi ohjaa päätösten tekoa pohdittaessa riskin merkitsevyyttä organisaa-

tiolle. Arvioinnissa määritellään, hyväksytäänkö riski tai käsitelläänkö sitä jollakin tavalla.

LIITE 10 HERÄTE - MUODOSTETTU RISKIEN ARVIOINNIN MALLI

HERÄTE -malli

Validoitu riskien arvioinnin malli

Kokkomäki Tuomas

Nortunen Mika

v1.1

Perusteet

Organisaatiolla on yksi strategia, jota kaikkien muiden prosessien tulee tukea. Riskienhallinta saa ohjauksen strategian kautta ja määrittää riskien arvioinnin perusteet. Riskien arviointi on osa organisaation kilpailukykyä, jolloin ketterät sekä dynaamiset toimintatavat ovat ratkaisevassa asemassa. Epävarmuus ja nopeat muutokset toimintaympäristössä tuovat mukanaan myös mahdollisuuksia. Laadukas riskien arviointi on keino erottua kilpailijoista, varmistaa osaltaan organisaation luotettavuus ja trendien tunnistamisen kautta löytää uusia mahdollisuuksia tulevaisuuden innovaatioille.

Yhä monimutkaistuva maailma luo organisaatiolle tarpeen tehdä tehokkaita toimenpiteitä yhä nopeammin. Organisaatioiden tulee pystyä reagoimaan nopeasti muuttuvan toimintaympäristön asettamiin haasteisiin. Riskien arvioinnin tulosten jakamisen avulla on mahdollisuus löytää uusia yhteistyömuotoja. Aikaisemmat riskien arvioinnin menetelmät ovat perustuneet riskienhallintaorganisaation keräämiin havaintoihin. Mallissa datan ja tiedon kerääminen perustuu aktiiviseen toimintaan. Aktiivinen tiedonhankinta tarkoittaa organisaation oma-aloitteista, proaktiivista, kanssakäymistä ympäröivän maailman kanssa ja muutosten tunnistamista tiedon joukosta. Tämä malli tarjoaa mahdollisuuden mahdollisimman monipuolisen tiedon keräämiseen. Tieto ja tilannekuva ovat aina jossain määrin puutteellisia ja tämän vuoksi on tärkeää, että riskien arvioinnin prosessi on joustava ja dynaaminen. Malli pyrkii esittämään riskien arvioinnin prosessina, jossa olemassa olevaa tietoa käytetään mahdollisimman tehokkaasti hyväksi ja sitä pyritään aktiivisesti täydentämään prosessin edetessä. Mallin tavoite on pyrkiä mahdollisimman kattavaan tietoon ja tilannekuvaan.

Organisaation riskien arvioinnin tulee perustua henkilöstöä osallistaviin riskitietojen raportointiin ja työpajoihin, joissa pyritään kattavasti ylläpitämään tilannekuvaa organisaation riskeistä. Toiminnan tulee olla hyvin organisoitua ja vastuutettua prosessin omistajalle, kuten turvallisuusjohtajalle tai muulle nimetylle henkilölle, joka käy keskustelua johdon ja henkilöstön välillä. Henkilöstön sitoutuminen on organisaatiolle mahdollisuus saada havaintoja erilaisilta ihmisiltä. Ihmiset tekevät havaintoja asioista erilaisista lähtökohdista ja aikaisempiin kokemuksiinsa verraten. Muun muassa henkilöstön koulutus ja harrastuneisuus tuovat uusia näkökulmia kokonaisvaltaiseen riskien arviointiin. Merkittävän, asioita ja tilanteita ratkaisevan, tiedon lähdettä on riskien arviointi prosessin alkaessa hankala tietää.

Riskien arvioinnin tuloksena, toimintana, organisaatio pyrkii käsittelemään riskejä esimerkiksi luomalla painopisteitä tietoturvaperiaatteiden kautta tai tekemällä taloudellisia investointeja organisaation tietoturva-arkkitehtuuriin. Mallin taustalla on ajatus uhkien sekä muiden herätteiden kattavasta tunnistamisesta, riskien arvioinnin nopeuttamisesta, yksinkertaistamisesta ja yhdenmukaistamisesta organisaation strategian mukaisesti. Malli on laadittu tieteellisen kirjallisuuden, standardien ja kaksivaiheisen laadullisen tutkimuksen synteesinä. Muodostettu malli on rakennettu finanssialan organisaatioiden riskien arvioinnin lähtökohdista. Mallissa ei ole kuitenkaan rakenteita, jotka tekisivät siitä ainoastaan finanssialaan soveltuvan. Näin ollen malli soveltuu käytettäväksi organisaatioihin ja dynaamisiin prosesseihin toimialasta riippumatta.

Suomalaisten finanssialan organisaatioiden edustajilla ja mallin validointiin osallistuneilla asiantuntijoilla on ollut mallin muodostumisessa merkittävä osuus. Kiitoksia yhteistyöstä ja avoimesta keskustelusta.

Riskien arvioinnin vaiheet

Mallin vaiheisiin on valittu organisaatioiden käytännön kokemuksia ja parhaita käytänteitä tehokkaan riskien arvioinnin toteuttamiseksi. Riskien arviointi koetaan nykyisessä muodossaan kankeaksi ja toimimattomaksi prosessiksi. Menetelmät koetaan perehtymistä vaativiksi ja niiden tulokset koetaan epätarkoiksi. Mallin muodostumisen taustalla on tarve prosessin yksinkertaistamiselle ja tehostamiselle. Prosessin tulee olla omaksuttavissa nopeammin ja ohjeiden tulee olla selkeämmät.

KUVA 1: Riskien arvioinnin prosessi

Mallin ei oleteta antavan tyhjentäviä vastauksia riskien arviointiin vaan ohjaavan prosessia oikeaan suuntaan. Mallia soveltamalla organisaatioiden on mahdollista laatia omista lähtökohdistaan ketterämpi menetelmä riskien arviointiin. Vaiheet on käsitelty seuraavissa luvuissa yleisesti. Tarkemmat kuvaukset ovat luettavissa Kokkomäen ja Nortusen Jyväskylän yliopistossa laaditusta pro gradu -tutkielmasta.

Riskien arvioinnin tulisi olla mahdollisimman joustava ja aktiivinen prosessi ja sen tulee kyetä reagoimaan nopeisiin muutoksiin. Arvioinnin vaiheet 1. - 3. menevät päällekkäin siten, että tiedonhankinnan tulee olla mahdollisimman monipuolista ja aktiivista. Tiedonhankinnan tulee jatkua koko ajan. Se ei ole irrallinen vaihe, joka lopetetaan sen suorittamisen jälkeen. Myös kerätyn tiedon analysoinnin tulee olla aktiivista ja jatkuvaa. Vaiheet määrittävät mallissa prosessin painopisteen eikä niinkään tiukasti vaiheesta toiseen etenevää kulkua.

	Vastuu	Suorittaja	Työtapa
1. Aktiivinen tiedonhankinta	Prosessin omistaja	Koko organisaatio	Tiedon aktiivinen kerääminen ohjatusti
2. Analyysi	Prosessin omistaja	Asiantuntijaryhmä	Työpajat ja asiantuntijaryhmät
3. Toimenpiteiden valmistelu	Prosessin omistaja	Valikoituu tilannekohtaisesti	Analysoidun riskin siirto asiasta vastaavalle toimijalle
4. Tiedon kertyminen ja oppiminen	Prosessin omistaja	Asiantuntijaryhmä	Vaiheiden 1-3 aikana kertynyt tieto ja palaute toiminnasta palaavat koordinoidusti joko uudeksi herätteeksi tai organisaation tietopääomaksi

TAULUKKO 1: Vastuunjako

Vastuunjako eri vaiheissa on riippuvainen organisaation rakenteesta. Olennaista on se, että toiminnan kokonaisuus on organisoitu ja johdettu selkeästi. Riskien arvioinnin prosessi ei saa olla kuitenkaan liian henkilökeskeinen. Koko organisaation ammattitaito tulee pyrkiä hyödyntämään arvioinnin suorittamisessa.

Heräte

Riskienhallinnassa pyritään löytämään kokonaisvaltaisesti organisaation strategiaa uhkaavia tekijöitä ja ilmiöitä sekä hallitsemaan niitä. Organisaatio etsii ja pyrkii tunnistamaan ympäröivästä maailmasta, erityisesti omasta toimintaympäristöstään, herätteitä, joiden avulla on mahdollista puuttua riskeihin ennalta. Organisaatioilla on oman toimialansa vaikutuksesta ja tiedon kertymisen kautta tiedossa riskejä, joiden herätteitä pyritään havainnoimaan. Herätteiden havainnointi ja aktiivinen tiedonhankinta menevät vaiheina osittain päällekkäin ja tästä syystä riskien arvioinnin prosessimallissa on huomioitava myös herätteiden vaikutus.

Organisaatio etsii ja pyrkii tunnistamaan ympäröivästä maailmasta, erityisesti omasta toimintaympäristöstään, herätteitä, joiden avulla on mahdollista puuttua riskeihin ennalta.

Riskien arvioinnin aloitukselle ei voi määrittää yhtä aloittavaa herätettä. Herätteiden merkityksellisyyttä arvioivat ihmiset. Ihmisten aiemmat kokemukset määrittävät, miten ihminen pystyy tunnistamaan kaikesta datasta ja olemassa olevasta tiedosta merkitykselliset herätteet. Organisaation tietoisuuden ja historiatiedon kasvaessa on mahdollista automatisoida siirtymistä herätteestä suoraan toimintaan, jolloin riskien arviointi voidaan jättää tekemättä tai prosessin kulkua voidaan nopeuttaa. Esimerkkinä herätteestä voivat olla tunnistetut hyökkäykset organisaation tietojärjestelmiä kohtaan, jolloin puolustusmekanismit voivat reagoida suoraan herätteestä (tunkeutumisyritys) ja estää vastapuolen yritykset.

Riskien arviointi tuottaa prosessin aikana uusia herätteitä, jolloin tiedon kertymisen ja oppimisen (mallin vaihe 4.) kautta organisaatiossa pyritään luomaan syvempi ymmärrys omasta toimintaympäristöstä ja sen riskeistä.

1 Aktiivinen tiedonhankinta

Organisaation tulee itse ymmärtää, mitä tietoa tarvitaan strategian toteutumiseksi. Nykyaikaiselle organisaatiolle on ominaista aktiivinen tiedon hakeminen eri lähteistä. Aktiivinen tiedonhankinta kuvaa organisaation jatkuvaa kanssakäymistä ympäröivän maailman kanssa. Keskeinen toiminta-ajatus on olla itse aloitteellinen osapuoli. Tietoa hallitsevien yksilöiden, ryhmien ja järjestelmien kanssa pyritään muodostamaan yhteistyöverkostoja. Tietoa tuottavat muun muassa oman organisaation henkilöstö, sidosryhmät, yhteistyöverkostot ja erilaiset käytössä olevat teknologiat. Organisaatiossa olevien projektien aikana kertyvän datan ja tiedon käyttöön tulee kiinnittää erityistä huomiota.

Aktiivinen tiedonhankinta kuvaa organisaation jatkuvaa kanssakäymistä ympäröivän maailman kanssa.

Tiedonhankinnan perustana tulee käyttää organisaation jo olemassa olevia varantoja. Toiminnan suuntaamisen ja kehittymisen kannalta on kuitenkin merkityksellistä havainnoida aktiivisesti mahdollisuuksia saada tietoa uusista lähteistä sekä uusia teknologioita käyttäen. Etua strategian toteuttamiseen on mahdollista hakea erilaisia muutoksia, trendejä, tunnistamalla. Trendien tunnistamisessa on mahdollista käyttää apuna julkisia sekä palveluntarjoajien maksullisia datavarantoja.

Riskien arvioinnin perusteena olevan tiedon hankinnan tulee olla koordinoitua. Organisaatiossa tehtyjen toimenpiteiden ja muiden tapahtumien jälkeen tieto tulee palauttaa uusien herätteiden ja oppimisprosessin perustaksi. Henkilöstöllä tulee olla mahdollisuus kirjata ylös mahdollisia havaintoja riskien arvioinnin perustaksi riskien arvioinnin analyysin tueksi.

Vastuuhenkilö tiedon hankinnalle on kyseisen prosessin omistaja. Organisaatiosta riippuen henkilön tehtävänimike voi vaihdella, mutta keskeistä on keskusteluyhteys johdon ja henkilöstön edustajien kanssa.

Organisaation riskien arvioinnin kannalta tärkeitä asioita ovat koko henkilöstön motivointi, riskitiedon ja trendien jakaminen sekä suunnitellusti toteutettu henkilöstön palkitseminen.

2 Analyysi

Analyysi kuvaa organisaation keräämän datan suodattamista tiedoksi. Organisaatiot keräävät tietoa aktiivisesti, jolloin riskien arvioinnin perusteena olevan jäsennellyn tiedon keräämiseksi tulee suorittaa erityisiä työpajoja, workshoppeja. Työpajoihin osallistuvat organisaation eri toimintayksiköiden nimetyt riskien arvioinnin vastuuhenkilöt. Vastuuhenkilöiden valinnassa tulee painottaa laajaa ymmärrystä riskien arvioinnin perusteena olevan tiedon hankinnassa ja koko henkilöstön näkemyksen esille tuomisessa. Työpajat ovat suunniteltuja ja valmisteltuja tilaisuuksia, joissa käydään läpi ennalta määriteltyjä asioita. Riskejä tuodaan esille laajasti organisaation toiminnan eri osa-alueilta, mutta työpajoissa pääpaino on kuitenkin suunniteltujen asioiden läpikäymisellä.

Analyysi kuvaa organisaation keräämän datan suodattamista tiedoksi. Päivittäistä operatiivista toimintaa ja riskien arviointia ei tule erottaa toisistaan.

Tiedon hankinnan ja analyysin välille ei voi määrittää yhtä tiettyä tekijää, joka määrittää siirtymisen vaiheesta toiseen. Kuvaava esimerkki on, että organisaatiot järjestävät suunnitelmien mukaisesti, omaan toimintaansa perustuen, neljännesvuosittain, puolivuosittain tai kerran vuodessa työpajoja. Analysointi tulee ymmärtää kuitenkin vuosittaisia työpajoja laajemmin. Organisaation havaitseman riskin arviointiprosessi saattaa olla hyvinkin nopea ja dynaaminen prosessi, jossa prosessin omistaja kerää toiminnan kannalta keskeiset henkilöt yhteen. Tällöin päätös tehdään olemassa olevan tiedon perusteella mahdollisimman nopeasti. Tällaisia tilanteita ovat muun muassa organisaation toiminnan kannalta kriittisten toimintojen suojaaminen ja toimintojen jatkuvuuden turvaaminen. Päivittäistä operatiivista toimintaa ja riskien arviointia ei tule erottaa toisistaan. Analyysi tehdään samalla tavalla riippumatta käytettävissä olevasta ajasta. Nopeasti eteen tulevassa tilanteessa analyysi suoritetaan sen hetkisen tiedon perusteella prosessin omistajan tai hänen erikseen määräämänsä henkilön johtaessa toimintaa.

Riskien arviointi on aina arvio, johon liittyy useita epävarmuustekijöitä. Analyysin perustana olevan materiaalin tulee sisältää mahdollisimman paljon mitattavissa olevia, kvantitatiivisia, arvoja. Tämä ei kuitenkaan tarkoita sitä, että riskille on mahdollista määrittää tarkka arvo ennalta määritellyllä asteikolla. Riskien arvioinnin tuloksen tulee olla sekä johdon että muun henkilöstön ymmärtämässä muodossa. Tämä tarkoittaa usein sitä, että arvo tulee esittää asteikon lukuarvoa monipuolisemmin käyttäen kvalitatiivisia, laadullisia, mittareita. Toisinaan riskin tuottama vahinko on varsin abstrakti ja tällöin on arvioitava käytettävissä olevan tiedon perusteella kuinka suuren vahingon riski toteutuessaan voi aiheuttaa ottaen huomioon niin konkreettiset fyysiseen omaisuuteen kuin maineeseen vaikuttavat tekijät.

Analyysin tulee tuottaa lopulta yhdenmukaista materiaalia, jota voidaan verrata toisiin riskeihin ja historiatietoihin. Vertailuaineiston eli formaalin, määrämuotoisen, historiatiedon puutteen vuoksi täysin kvantitatiiviseen menetelmään perustuvaa arviointia ei ole mahdollista tehdä. Jotta vertailua olisi mahdollista tehdä, tulisi organisaation kerätä tietoa tapahtumista ja pyrkiä jakamaan sekä vaihtamaan tietoa muiden samalla toimialalla toimivien ja toimialan ulkopuolisten organisaatioiden kanssa. Organisaation kehittyessä ja riskien arvioinnin materiaalin kertyessä on tulevaisuudessa mahdollista tehdä kvantitatiivisin arvoin perusteltavia arvioita.

Riskien arviointi on aina arvio, johon liittyy useita epävarmuustekijöitä.

Tiedon analysoinnista vastaa prosessin omistaja ja sen suorittaa asiantuntijaryhmä.

3 Toimenpiteiden valmistelu

Toimenpiteiden valmistelu kuvaa sitä, että toimenpiteet, joihin riskien arvioinnin perusteella tulee ryhtyä siirretään sille organisaation toimijalle, jolla on tosiasiallinen kyky suorittaa ne. Ennen siirtymistä varsinaiseen toimintaan tulee toimenpiteet suunnitella ja valmistella. Toiminnan tulee olla koordinoitua ja johdettua. Tätä kautta valituilla toimenpiteillä saadaan todennäköisemmin huomattavasti tehokkaampi vaikutus.

Riskien arvioinnin seurauksena löydettyjen, toimenpiteitä vaativien, riskien käsittely vaatii usein monia asiantuntijoita. Työn päällekkäisyyttä tulee välttää kaikessa toiminnassa.

Ihannetilanteessa valmisteltujen toimenpiteiden toteuttamiseen osallistuu useampi toimija organisaation sisällä, jolloin resursseja saadaan tehokkaampaan käyttöön. Tämä tarkoittaa niin henkilöresursseja kuin organisaation eri toimijoille budjetoituja varoja. Riskien arvioinnin seurauksena löydettyjen, toimenpiteitä vaativien riskien käsittely vaatii usein monia asiantuntijoita. Työn päällekkäisyyttä tulee välttää kaikessa toiminnassa. Työpajatyöskentely tukee sekä henkilöstön että muiden resurssien tehokasta käyttöä. Organisaatio voi siirtyä suoraan toimintaan ilman erillistä valmistelua, mikäli sillä on aiempaan kokemukseensa perustuen riittävät edellytykset siihen.

Toimenpiteiden valmistelusta vastaa prosessin omistaja. Toimenpiteiden suorittaja määräytyy analysoidun riskin tai riskien perusteella.

4 Tiedon kertyminen ja oppiminen

Organisaation tulee tietoisesti kerryttää riskien arvioinnista kertynyttä tietoa ja oppia suorittamastaan riskien arvioinnista. Riskien arvioinnin prosessi antaa organisaatiolle mahdollisuuden analysoida oman toimintansa vahvuuksia ja heikkouksia. Tämän tiedon jakaminen ja hyödyntäminen koko organisaation laajuudella auttaa sitä kehittämään toimintaansa. Riskien arvioinnin ei siis tulisi olla prosessi, joka suoritetaan kaavamaisesti suunnitelmassa määritettyyn aikaan, vaan sen tulisi olla jatkuva sykli, jonka kautta organisaatio voi muokata ja kehittää aktiivisesti toimintaansa.

Organisaation tulee tietoisesti kerryttää riskien arvioinnista kertynyttä tietoa ja oppia suorittamastaan riskien arvioinnista. Riskien arvioinnin prosessi antaa organisaatiolle mahdollisuuden analysoida oman toimintansa vahvuuksia ja heikkouksia.

Tiedon kertymisen ja oppimisen tulee olla koordinoitua ja johdettua toimintaa. Johdon lisäksi tätä vaihetta kohtaan tulee olla vahva sitoutuminen läpi koko organisaation. Riskien arvioinnin prosessin kautta kertynyttä tietoa tulee jakaa organisaatiossa sekä ylhäältä alas- että alhaalta ylöspäin. Prosessin aikana kertynyt tieto tulee dokumentoida systemaattisesti. Tätä kautta kaikki mahdollinen tieto on aina tarvitsijoiden käytössä.

Tiedon kertymisen ja oppimisen vaiheen suorittamisesta vastaa prosessin omistaja. Käytännön suorittajana ovat riskien arviointiin osallistuneet asiantuntijaryhmät. Tiedon kertymisen ja oppimisen tulisi noudattaa oppivan organisaation periaatteita. On oleellista, että tietoa vaihdetaan aktiivisesti joka suuntaan. Saavutetun syvemmän ymmärryksen kautta organisaatio voi kehittää toimintaa ja saavuttaa kilpailukykyä.

Toiminta

Riskien arvioinnin tuloksilla pitäisi olla konkreettista vaikutusta organisaation toimintaan. Organisaation strategian toteuttamisen kannalta oikein ajoitetut ja tehokkaat toimenpiteet luovat mahdollisuuden menestykseen. Ajan ja tilan hallinta omassa toimintaympäristössä ovat keskeisiä tekijöitä. Organisaatioiden tulisi pyrkiä olemaan aloitteellisia omassa toiminnassaan, jotta toiminta ei perustu eteen tuleviin tilanteisiin reagointiin vaan ennen kaikkea strategisten tavoitteiden toteuttamiseen ja oma-aloitteiseen toimintaan.

Organisaation strategian toteuttamisen kannalta oikein ajoitetut ja tehokkaat toimenpiteet luovat mahdollisuuden menestykseen. Organisaatioiden tulisi pyrkiä olemaan aloitteellisia.

Konkreettisia toimia, joilla riskeihin voidaan vaikuttaa ovat tietoturvallisuuden osalta esimerkiksi erilaiset turvallisuuteen vaikuttavat järjestelmät tai palvelut, henkilöstön koulutus tai organisaation tietoturvaperiaatteiden muokkaaminen. Oleellista on, että se toiminta, johon resursseja suunnataan perustuu oikeaan ja systemaattisella prosessilla saavutettuun kuvaan organisaation tilasta, eli havaituista riskeistä.

Riskien arvioinnin prosessi tarjoaa organisaatiolle tietoa sen toimintaan vaikuttavista riskeistä. Systemaattisen prosessin kautta organisaatiolla on mahdollisuus muodostaa riskeistään kattava kuva. Tämän tilannekuvan avulla organisaatio voi eri aktiviteettien kautta hallita havaittuja riskejä. Organisaatio tavoite on trendien tunnistaminen kerätystä tiedosta. Trendien tunnistamisen kautta organisaatioiden on mahdollista löytää uusia painopistealueita ja innovaatioita toiminnalleen.

LIITE 1: Mallin vaiheet ja vastuunjako

	Vastuu	Suorittaja	Työtapa
1. Aktiivinen tiedonhankinta	Prosessin omistaja	Koko organisaatio	Tiedon aktiivinen kerääminen ohjatusti
2. Analyysi	Prosessin omistaja	Asiantuntijaryhmä	Työpajat ja asiantuntijaryhmät
3. Toimenpiteiden valmistelu	Prosessin omistaja	Valikoituu tilannekohtaisesti	Analysoidun riskin siirto asiasta vastaavalle toimijalle
4. Tiedon kertyminen ja oppiminen	Prosessin omistaja	Asiantuntijaryhmä	Vaiheiden 1-3 aikana kertynyt tieto ja palaute toiminnasta palaavat koordinoidusti joko uudeksi herätteeksi tai organisaation tietopääomaksi

LIITE 11 HERÄTE - MUODOSTETTU RISKIEN ARVIOINNIN MALLI: ”POSTERI”

PERUSTEET

Riskienhallinta saa ohjauksen strategian kautta ja määrittää riskien arvioinnin perusteet. Riskien arviointi on osa organisaation kilpailukykyä, jolloin ketterät sekä dynaamiset toimintatavat ovat ratkaisevassa asemassa. Epävarmuus ja nopeat muutokset toimintaympäristössä tuovat mukanaan myös mahdollisuuksia. Laadukas riskien arviointi on keino erottua kilpailijoista, varmistaa osaltaan organisaation luotettavuus ja trendien tunnistamisen kautta löytää uusia mahdollisuuksia tulevaisuuden innovaatioille.
Mallissa datan ja tiedon kerääminen perustuu aktiiviseen toimintaan. Aktiivinen tiedonhankinta tarkoittaa organisaation oma-aloitteista, proaktiivista, kanssakäymistä ympäröivän maailman kanssa ja muutosten tunnistamista tiedon joukosta. Tämä malli tarjoaa mahdollisuuden mahdollisimman monipuolisen tiedon keräämiseen. Tieto ja tilannekuva ovat aina jossain määrin puutteellisia ja tämän vuoksi on tärkeää, että riskien arvioinnin prosessi on joustava ja dynaaminen. Mallin tavoite on pyrkiä mahdollisimman kattavaan tietoon ja tilannekuvaan. Mallin taustalla on ajatus uhkien sekä muiden herätteiden kattavasta tunnistamisesta, riskien arvioinnin nopeuttamisesta, yksinkertaistamisesta ja yhdenmukaistamisesta organisaation strategian mukaisesti.

HERÄTE-MALLI

VALIDOITU RISKIEN ARVIOINNIN MALLI

RISKIEN ARVIOINNIN VAIHEET

Mallin muodostumisen taustalla on tarve prosessin yksinkertaistamisella ja tehostamisella. Prosessin tulee olla nopeasti omaksuttava ja ohjeiden tulee olla selkeät.

KUVA 1: Riskien arvioinnin prosessi

Mallin ei oleteta antavan tyhjentäviä vastauksia riskien arviointiin vaan ohjaavan prosessia oikeaan suuntaan. Mallia soveltamalla organisaatioiden on mahdollista laatia omista lähtökohdistaan kettterämpi menetelmä riskien arviointiin.
Riskien arvioinnin tulisi olla mahdollisimman joustava ja aktiivinen prosessi ja son tulee kyetä reagoimaan nopeisiin muutoksiin. Arvioinnin vaiheet 1. - 3. menevät päällekkäin siten, että tiedonhankinnan tulee olla mahdollisimman monipuolista ja aktiivista. Tiedonhankinnan tulee jatkua koko ajan. Se ei ole irrallinen vaihe, joka lopetetaan sen suorittamisen jälkeen. Myös kerätyn tiedon analysoinnin tulee olla aktiivista ja jatkuvaa. Vaiheet määrittävät mallissa prosessin painopisteen eikä niinkään tiukasti vaiheesta toiseen etenevää kulkua.

	Vastuu	Suorittaja	Työtapa
1. Aktiivinen tiedonhankinta	Prosessin omistaja	Koko organisaatio	Tiedon aktiivinen kerääminen ohjatusti
2. Analyysi	Prosessin omistaja	Asiantuntijaryhmä	Työpajat ja asiantuntijaryhmät
3. Toimenpiteiden valmistelu	Prosessin omistaja	Valikoituu tilannekohtaisesti	Analysoidun riskin siirto asiasta vastaavalle toimijalle
4. Tiedon kertyminen ja oppiminen	Prosessin omistaja	Asiantuntijaryhmä	Vaiheiden 1-3 aikana kertynyt tieto ja palaute toiminnasta palaavat koordinoidusti joko uudeksi herätteeksi tai organisaation tietopääomaksi

TAULUKKO 1: Vastuunjako

Vastuunjako eri vaiheissa on riippuvainen organisaation rakenteosta. Olennaista on se, että toiminnan kokonaisuus on organisoitu ja johdettu selkeästi.

Riskien arviointi on osa organisaation kilpailukykyä, jolloin ketterät sekä dynaamiset toimintatavat ovat ratkaisevassa asemassa.

Tieto ja tilannekuva ovat aina jossain määrin puutteellisia ja tämän vuoksi on tärkeää, että riskien arvioinnin prosessi on joustava ja dynaaminen. Mallin tavoite on pyrkiä mahdollisimman kattavaan tietoon ja tilannekuvaan.

HERÄTE

Organisaatio pyrkii tunnistamaan toiminta-ympäristöstään herätteitä

Riskienhallinnassa pyritään löytämään kokonaisvaltaisesti organisaation strategiaa uhkaavia tekijöitä ja ilmiöitä sekä hallitsemaan niitä. Organisaatio etsii ja pyrkii tunnistamaan ympäröivästä maailmasta, erityisesti omasta toimintaympäristöstään, herätteitä, joiden avulla on mahdollista puuttua riskeihin ennalta.
Riskien arviointi tuottaa prosessin aikana uusia herätteitä, jolloin tiedon kertymisen ja oppimisen (mallin vaihe 4.) kautta organisaatiossa pyritään luomaan syvempi ymmärrys omasta toimintaympäristöstä ja sen riskeistä.

1 AKTIIVINEN TIEDONHANKINTA

Aktiivinen tiedonhankinta kuvaa organisaation jatkuvaa kanssakäymistä ympäröivän maailman kanssa. Keskeinen toiminta-ajatus on olla itse aloitteellinen osapuoli. Riskien arvioinnin perusteena olevan tiedon hankinnan tulee olla koordinoitua. Organisaatiossa tehtyjen toimenpiteiden ja muiden tapahtumien jälkeen tieto tulee palauttaa uusien herätteiden ja oppimisprosessin perustaksi.

2 ANALYYSI

Analyysi kuvaa organisaation keräämän datan suodattamista tiedoksi. Organisaatiot keräävät tietoa aktiivisesti, jolloin riskien arvioinnin perusteena olevan jäsennellyn tiedon keräämiseksi tulee suorittaa työpajoja. Työpajat ovat suunniteltuja ja valmisteltuja tilaisuuksia, joissa käydään läpi ennalta määriteltyjä asioita. Riskejä tuodaan esille laajasti organisaation toiminnan eri osa-alueilta.

Päivittäistä operatiivista toimintaa ja riskien arviointia ei tule erottaa toisistaan.

Tiedon hankinnan ja analyysin välille ei voi määrittää yhtä tiettyä tekijää, joka määrittää siirtymisen vaiheesta toiseen. Organisaation havaitseman riskin arviointiprosessi saattaa olla hyvinkin nopea ja dynaaminen prosessi, jossa prosessin omistaja kerää toiminnan kannalta keskeiset henkilöt yhteen. Tällöin päätös tehdään olemassa olevan tiedon perusteella mahdollisimman nopeasti. Päivittäistä operatiivista toimintaa ja riskien arviointia ei tule erottaa toisistaan. Riskien arviointi on aina arvio, johon liittyy useita epävarmuustekijöitä. Riskien arvioinnin tuloksen tulee olla sekä johdon että muun henkilöstön ymmärtämässä muodossa.

3 TOIMENPITEIDEN VALMISTELU

Toimenpiteiden valmistelu kuvaa sitä, että toimenpiteet, joihin riskien arvioinnin perusteella tulee ryhtyä siirretään sille organisaation toimijalle, jolla on tosiasiallinen kyky suorittaa ne. Riskien arvioinnin seurauksena löydettyjen, toimenpiteitä vaativien, riskien käsittely vaatii usein monia asiantuntijoita. Työn päällekkäisyyttä tulee välttää kaikessa toiminnassa.

4 TIEDON KERTYMINEN JA OPPIMINEN

Organisaation tulee tietoisesti kerryttää riskien arvioinnista kertynyttä tietoa ja oppia suorittamastaan riskien arvioinnista. Riskien arvioinnin prosessi antaa organisaatiolle mahdollisuuden analysoida oman toimintansa vahvuuksia ja heikkouksia. Riskien arvioinnin ei tulisi olla prosessi, joka suoritetaan kaavamaisesti suunnitelmassa määritettyyn aikaan, vaan sen tulisi olla jatkuva sykli, jonka kautta organisaatio voi muokata ja kehittää aktiivisesti toimintaansa. Saavutetun syvemmän ymmärryksen kautta organisaatio voi kehittää toimintaansa ja saavuttaa kilpailukykyä.

TOIMINTA

Riskien arvioinnin tuloksilla pitäisi olla konkreettista vaikutusta organisaation toimintaan. Organisaation strategian toteuttamisen kannalta oikein ajoitetut ja tehokkaat toimenpiteet luovat mahdollisuuden menestykseen.

Oikein ajoitetut ja tehokkaat toimenpiteet luovat mahdollisuuden menestykseen.

Organisaatioiden tulisi pyrkiä olemaan aloitteellisia omassa toiminnassaan, jotta toiminta ei perustu eteen tuleviin tilanteisiin reagointiin vaan ennen kaikkea strategisten tavoitteiden toteuttamiseen ja oma-aloitteiseen toimintaan. Riskien arvioinnin prosessi tarjoaa organisaatiolle tietoa sen toimintaan vaikuttavista riskeistä. Systemaattisen prosessin kautta organisaatiolla on mahdollisuus muodostaa riskeistään kattava kuva. Tämän tilannekuvan avulla organisaatio voi eri aktiviteettien kautta hallita havaittuja riskejä. Organisaatio tavoite on trendien tunnistaminen kerätystä tiedosta. Trendien tunnistamisen kautta organisaatioiden on mahdollista löytää uusia painopistealueita ja innovaatioita toiminnalleen.