Niko Takala

ULKOISTEN KYBERTURVALLISUUDEN RISKIEN ARVIOINTI FINANSSIALAN ORGANISAATIOSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Takala, Niko
Ulkoisten kyberturvallisuuden riskien arviointi finanssialan organisaatiossa
Jyväskylä: Jyväskylän yliopisto, 2019, 82+1 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Niemimaa, Marko

Riskienhallintaa ja riskien arviointia voidaan tarkastella useasta eri näkökulmasta ja sitä ohjaavat useat erilaiset tekijät. Ohjaaviksi tekijöiksi voidaan tunnistaa organisaation strategia, organisaatiokulttuuri, tietoturvapolitiikka sekä erilaiset riskienhallinnan mallit, kuten PMBOK, ISO31000 ja IRM. Näiden lisäksi tieto- ja kyberturvallisuuden prosesseja pyritään helpottamaan erilaisilla työkaluilla, kuten ISO27001, VAHTI ja Katakri. Riskienhallinnan mallit pitävät sisällään riskien arvioinnin, mutta käsittelevät arviointiprosessia hyvin pintapuolisesti. Riskien arvioinnin perustuminen arvioijan omien kokemusten ja ajatusten päälle pidetään jossain määrin ongelmallisena. Tutkimus toteutettiin toimeksiantona ja sen tarkoitus oli tarjota tukea riskien arvioinnin prosessin kehittämiseen. Tutkimuksessa pyrittiin paikantamaan toimeksiantajan riskien arviointiprosessin ongelmakohdat ja rakentamaan riskien arvioinnin malli niin, että sen voi yleistää käytettäväksi myös muihin organisaatioihin. Tutkimuksen tulokset osoittavat, että myös todennäköisyyksien ennustamiseen on mahdollista rakentaa sen uskottavuutta tukeva malli, joka ajan kuluessa tarjoaa vankan pohjan riskien arviointiprosessiin. Tutkimus toteutettiin kvalitatiivisena tapaustutkimuksena ja pääasiallinen empiirisen datan keräämiseen käytetty metodi oli kvalitatiivinen semi-strukturoitu haastattelu. Riskien arvioinnin mallista muodostui iteratiivinen malli, joka nojaa olemassa olevaan riskienhallinnan malliin. Mallin tavoitteena oli syventää riskienhallinnan henkilökunnan tietoa organisaation riskeihin liittyen ja sitä kautta intuition vaikutuksen vähentäminen riskien arvioinnissa.

Asiasanat: kyberturvallisuus, riskienhallinta, arviointi, finanssiala, ulkoiset riskit

ABSTRACT

Takala, Niko
External Cyber Security Risk Assessment in a Finance Sector Organization
Jyväskylä: University of Jyväskylä, 2019, 82+1 pp.
Cyber Security, Master's Thesis
Supervisor(s): Niemimaa, Marko

Risk management and risk assessment can be viewed from several different angles and they have multiple guiding factors. The organization's strategy, culture and information security policy, as well as risk management models like PMBOK, ISO31000 and IRM can all be seen as guiding factors. In addition to these, there are multiple toolboxes designed to make it easier to implement these models in everyday actions. Tools like these include ISO27001, VAHTI and Katakri. The models of risk management include risk assessment, but they handle it very superficially. Basing risk assessment on the intuition of the assessor can be seen as a problem. The study was conducted as an assignment and the aim of the study was to provide support for developing the risk assessment process inside the principal organization. The study sought to pinpoint the problems of the risk assessment process in the organization and to build a model that can be generalized outside the organization as well. The results of the study show that it is possible to build a model to support the estimation of the risk probabilities. In time, by using the model the organization is able to build a strong database considering its risks and to use the database as a justification for assigned probabilities. The study was conducted as a qualitative case study and the main data collection method was a qualitative semi-structured interview. The model for risk assessment formed to be an iterative model that bases itself on the existing model. The aim of the model was to provide a better foundation for the risk management professionals to do their work and estimate the risks' probabilities. Through this foundation it is possible to weaken the effect of intuition in the process or at least provide a good justification for the level of probability of the risks.

Keywords: cyber security, risk management, assessment, financial field, risks

KUVIOT

TAULUKOT

SISÄLLYSLUETTELO

1 Johdanto

Informaatioteknologiaan on panostettu eri alojen organisaatioissa jo pitkään. IT on integroitu organisaatioiden rakenteisiin sekä osaksi muita toimintoja (Fairbank, Labianca, Steensma & Metters, 2006). Tästä johtuen myös riskienhallinta ja riskien arviointi varsinkin IT-järjestelmissä ovat jokapäiväistyneet organisaatioissa. Riskienhallintaa ohjaa strategia (IRM, 2002), joka määrittää riskienhallinnan perusteet.

IT-järjestelmien lisääntyessä riskienhallinnasta sekä riskien arvioinnista on tullut merkittävä osa organisaatioiden kilpailukykyä. Teknologioiden ja menetelmien nopea ja jatkuva kehittyminen tuovat tullessaan epävarmuutta (Kotler & Keller, 2006). Riskienhallinta kokonaisuutena on nykypäivänä merkittävämmässä asemassa kuin koskaan ennen. Varsinkin kyberturvallisuuden osa-alueella haitalliset toimijat ovat lisääntyneet teknologioiden kehittymisen myötä ja myös valtiolliset toimijat ovat tulleet mukaan kuvioihin. (Lindström, 2012; Kotler & Keller, 2006)

Riskien arviointi lukeutuu osaksi riskienhallintaa (PMBOK, 2013; ISO, 2018; IRM, 2002). Riskienhallinnalle on luotu useampia standardeja, kuten esimerkiksi, PMBOK (2013), ISO 31000 (2018) ja IRM (2002). Tämän tutkimuksen tarkoitus on keskittyä riskienhallinnassa kyberturvallisuuden osa-alueeseen ja tarkemmin ulkoisten riskien arviointiin. Vaikka riskien arvioinnille ja riskienhallinnalle on mahdollista löytää useita erilaisia malleja ja tutkimuksia, mallintavat nämä tutkimukset enimmäkseen riskienhallintaa isona kokonaisuutena, eivätkä välttämättä keskity niin tarkasti nimenomaan riskien arviointiin, kuten luvussa 3 tullaan näkemään.

Toimeksiantaja aloittaa kyberturvallisuuden riskienhallinnan kehittämistyön vuonna 2019. Tätä kehittämistyötä varten ulkoisten kyberturvallisuuden uhkien ja niistä johtuvien riskien arvioinnin tueksi halutaan luoda malli, joka helpottaa kyseistä työtä ja tuo siihen enemmän tieteellistä pohjaa. Kuten jatkossa käy ilmi, perustuu riskienhallinta kuitenkin vahvasti myös intuitiolle. Tätä intuition määrää arviointiprosessissa halutaan pienentää.

1.1 Tutkimuksen tausta ja näkökulma

Tämä tutkimus toteutettiin laadullisena tapaustutkimuksena finanssialan organisaatiossa. Tarve tutkimukselle sai alkunsa loppuvuodesta 2018, kun toimeksiantaja näki tarpeelliseksi aloittaa kyberturvallisuuden riskienhallinnan ja erityisesti ulkoisten uhkien sekä näistä johtuvien riskien arvioinnin kehittämistyön. Työn pohjalle päätettiin toteuttaa pro gradu -tutkielma kyberturvallisuuden ulkoisten riskien arvioinnista finanssialan organisaatiossa. Tutkija itse toimii toimeksiantajalla tukitehtävissä.

Toimeksiantaja koki, että riskien todennäköisyyksien hahmottaminen on hankalaa. Vaikka riskienhallinnan prosessi itsessään on selkeä ja noudattaa informaatioturvallisuuden riskienhallinnan prosessimallia (PMBOK, 2013; ISO, 2018; IRM, 2002), joutuu todennäköisyyksiä ja riskejä käsittelemään liiaksi omien kokemusten ja ajatusten pohjalta (Baskerville, 2009). Omat kokemukset ja intuitio ovat isossa osassa riskienhallintaa, mutta toimeksiantaja on sitä mieltä, että mitä tarkemmin arviot nojaavat johonkin tiettyyn malliin tai tietoon, sitä tarkemmin riskejä pystytään arvioimaan. Kun arviointi tehdään huolella, vältytään suuremmilta virheiltä prosessin muissa vaiheissa sekä kerätään tietoa tulevaisuuden arvioinnin tueksi. Tutkimustuloksia voi hyödyntää kyberturvallisuuden riskienhallinnassa myös finanssialan ulkopuolella. Tarkoituksena on kuitenkin luoda malli, joka helpottaa riskien arviointia juuri tutkimuskohteen kaltaisessa organisaatiossa.

Aikaisempaa tutkimusta juuri tästä aiheesta on loppupeleissä hyvin vähän ja juuri spesifin lähdemateriaalin löytäminen oli jokseenkin hankalaa. Toisaalta riskienhallintaa on käsitelty laajasti useassa eri alan julkaisussa, joka itsessään taas helpotti tutkimuksen aloittamista. Mitä syvemmälle tutkimukseen uppouduttiin, sitä vähemmän materiaalia kuitenkin oli tarjolla. Varsinkin, kun informaatioturvallisuuden käsitteeseen lisätään kyberturvallisuus, joka käsitteenä on vasta viimeisen 10 vuoden aikana yleistynyt, on tutkimusten määrä varsin vähäinen.

Riskiksi gradun viivästymiselle oli tunnistettavissa heti alkuun organisaation henkilöstön kiireet, jotka juontavat juurensa useampaan yhtäaikaiseen lakiuudistukseen. Toisaalta uhkana tutkimukselle voitiin nähdä myös tutkijan kyky hahmottaa riskienhallinnan ja riskien arvioinnin periaatteet sekä haastattelurungon luominen tutkimuksen tueksi ja haastattelujen analysoinnin onnistumisen tutkimusongelman kannalta.

1.2 Tutkimuksen tavoitteet ja tutkimusongelma

Tämän tutkimuksen tavoitteena oli selvittää, miten kyberturvallisuuden ulkoisia riskejä arvioidaan riskienhallinnan prosessissa ja miten tätä prosessia voidaan parantaa. Tutkimusongelma muotoiltiin tutkimuskysymykseksi seuraavalla tavalla:

Millainen riskien arvioinnin malli tukee kyberturvallisuuden ulkoisten riskien arviointia?

Tutkimusongelman selvittämiseksi laadittiin yllä oleva tutkimuskysymys sekä apukysymyksiä, joihin tämä tutkimus pyrki vastaamaan. Apukysymykset muotoiltiin tutkimusongelman pohjalta seuraavasti:

Millaisia nykymalleja riskien arviointiin on olemassa?

Miten kyberturvallisuuden ulkoisia riskejä tulisi arvioida?

Tutkimuksen empiirinen osuus toteutettiin semi-strukturoituna kvalitatiivisena haastattelututkimuksena. Tutkittavaksi organisaatioksi valikoitui toimeksiantaja. Haastattelut järjestettiin alkuvuodesta 2019 ja haastateltaviksi valittiin organisaation riskienhallinnasta vastaavat tahot.

1.3 Tiedonkeruu ja tutkielman rakenne

Kirjallisuuskatsauksen materiaalia etsittiin verkosta löytyvistä tietokannoista sekä hakukoneista. Materiaalia etsittiin mm. Google Scholarista, JYX Digital Repositorysta, JYKDOKista, IEEE Xplore Digital Librarysta, Researchgatesta sekä muista vastaavista julkaisualustoista, joita tuli vastaan matkan varrella. Hakusanoina käytettiin riskienhallintaan liittyviä termejä ja tutkielman avainsanoja eri muodoissa sekä englanniksi että suomeksi. Hakutuloksia oli tuhansia ja niitä rajattiin niin, että ne vastasivat tutkimuksen tarkoitusta mahdollisimman tarkasti. Apuna rajaamisessa käytettiin myös tarkentavia hakusanoja, jotka liittyivät sillä hetkellä käsittelyssä olleeseen lukuun.

Hakutuloksista löytyneistä materiaaleista tehtiin nopea arvio abstraktin perusteella siitä, ovatko ne soveltuvia tukemaan tätä tutkimusta. Lähteiden valintaa tehdessä keskityttiin myös siihen, millaisia lähteitä ne olivat käyttäneet ja kuljettiin lähdepolkua syvemmälle, mahdollisimman lähelle alkuperäistä teosta. Alun perin lähteenä käytetyn materiaalin lähdeluettelosta voitiin paikantaa myös lisää tutkimusta tukevaa materiaalia.

Internetissä sijaitsevien hakukoneiden ja tietokantojen lisäksi lähteitä haettiin myös Jyväskylän yliopiston sekä Jyväskylän kaupunginkirjaston valikoimista niin internetissä e-kirjoina kuin paikan päälläkin fyysisinä painoksina.

Apuna tiedonhaussa käytettiin myös asiantuntijoita, jotka osasivat ohjata oikeaan suuntaan tutkimusmateriaalia etsimään. Esimerkiksi Suomen Pankin ja VTT:n, kuten muidenkin julkisten elinten, materiaaleja etsittiin heidän omista palveluistaan, kuten nettisivuilta ja julkaisuista. Osittain tietoa saatiin myös toimeksiantajalta sekä toimeksiantajan omasta kirjakokoelmasta. Toimeksiantaja on pyritty tutkimuksessa anonymisoimaan mahdollisimman hyvin. Materiaa-

linkeruu kirjallisuuskatsausta varten suoritettiin pääasiassa 2018 loppuvuodesta.

Empiirinen aineisto kerättiin kevään 2019 aikana. Empiirisen aineiston keräämiseen valittiin semi-strukturoitu haastattelu, joka on omiaan kvalitatiivisen tutkimusmenetelmän empiirisen aineiston keräämiseen. Monesti kvalitatiivisen aineiston ainut keräystapa on juuri haastattelu ja siksi semi-strukturoitu rakenne sopii tähän loistavasti. Haastattelu seuraa ennalta määrättyä runkoa, jonka tutkija tekee kysymyksillään, mutta se myös lähtee harhailemaan eri teille sitä mukaa, mitä haastattelun aikana keskustellaan ja mitä kysymyksiä tai aiheita keskustelun aikana nousee esiin. Tutkimuksen ollessa kvalitatiivinen, myös aineiston analyysi on kvalitatiivinen. (DiCicco-Bloom & Crabtree, 2006)

Pro gradun toinen luku käsittelee riskienhallintaa ja -arviointia yleisellä tasolla. Kolmannessa luvussa paneudutaan tarkemmin ulkoisten riskien arvioinnin menetelmiin ja käydään läpi toimeksiantajalla vaikuttavia malleja, kuten ISO31000, IRM, sekä tutkijan itsensä mielestä riskien arviointiin erinomaisesti soveltuvaa PMBOKia. Neljäs luku pyrkii esittelemään tarkemmin finanssialalla olevia kyberuhkia sekä työkaluja, joita toimeksiantaja hyödyntää omassa kyberturvallisuuden riskienhallinnassaan. Viidennessä luvussa esitellään tutkimusmenetelmät sekä tutkimuksen tapaus. Kuudes luku kattaa tutkimustulokset ja antaa ehdotuksen muokatusta riskien arviointiprosessin mallista. Viimeisessä luvussa pohdinnan ja johtopäätösten kautta vedetään tutkimusta yhteen ja tiivistetään se, mitä tutkimus on antanut.

2 Riskienhallinnan perustukset

Tässä luvussa määritellään riski, riskienhallinta ja riskienhallintaa ohjaavat tekijät yleisellä tasolla. Ensimmäisessä alaluvussa luodaan käsitys siitä, miten riski ja riskienhallinta määritellään. Luvuissa 2.2, 2.3 ja 2.4 tutustutaan riskien arviointia ohjaaviin tekijöihin. Tutkimuksessa käsiteltäviä ohjaavia tekijöitä ovat organisaation strategia, organisaatiokulttuuri sekä tietoturvapolitiikka. Luvussa 2.5 tehdään vielä selväksi ero tietoturvallisuuden ja kyberturvallisuuden välillä.

2.1 Riski ja sen hallinta

Riski

Riskin määritteleminen on yhtä hankala prosessi kuin riskienhallinta itsessään ja terminä riski voidaan mieltää useaksi eri asiaksi lukijasta tai kuulijasta riippuen. Douglas (1990) puhuu siitä, kuinka ajan kuluessa riskin määritelmä on muuttunut ja keskittynyt eri osa-alueisiin kuin nykyään. Nykymaailmassa riskit nähdään laajemmassa skaalassa kuin menneisyydessä, jolloin riskejä katsottiin aivan eri perspektiivistä. 1700-luvulla riski tarkoitti lähinnä sitä, kuinka pelatessa nopan heitolla on mahdollisuus tuottaa tuskaa ja tätä varten kehitettiin kaava todellisuuslaskelmaa varten. Riski terminä oli neutraali ja se otti huomioon ainoastaan mahdolliset hyödyt ja menetykset. Nykypäivänä riski mielletään yleiseksi, toimintaan vaikuttavaksi tekijäksi ja se on terminä ajautunut kauemmas todellisuuslaskelmista sekä heikentänyt laskelmien asemaa riskin määrittelyssä. Riski terminä onkin jopa korvannut terminologiassa vaaran (*engl. danger*). Suuri riski tarkoittaa suurta vaaraa. Tämä johtuu siitä, että riskillä on terminä paljon vahvempi tieteellinen pohja kuin vaaralla. (Douglas, M. 1990; Gerber & Von Solms, 2005)

Ahteensuu (2014) puhuu riskienhallinnasta filosofisella tasolla ja hänen mukaansa riskit syntyvät, kun tiettyyn tapahtumaan tai asiaintilan esiintymiseen liitetään negatiivisia arvoja. Riskit ovat arvosidonnaisia omalla tavallaan ja tietty riski voi esiintyä eri organisaatiolle eri mittakaavassa. Päätöksenteko pyri-

tään aina perustamaan mahdollisimman luotettavaan tietoon, jota pyritään tuottamaan riskien arvioinnin prosessissa. Tämä prosessi sisältyy myös riskienhallintaan. (Ahteensuu, 2014)

Yates & Stone (1992) ovat sitä mieltä, että riskin voi määritellä epävarmuuden, menetyksen ja menetyksen merkittävyyden mukaan. Riskit ovat subjektiivisia ja ne saavat merkityksensä vasta, kun riskinottaja päättää joko ottaa riskin tai olla ottamatta sitä. Riski määritellään enemmänkin psykologisena terminä kuin varsinaisena organisaatiota uhkaavana tekijänä. Myös Fischhoff (1992) näkee riskin subjektiivisena käsitteenä. Hänen mukaansa riski määritellään seuraamusten perusteella. Riski voi hänen mukaansa olla negatiivinen tai positiivinen ja sama riski voi tapahtua eri tavoilla. Joskus riskejä myös otetaan tietoisesti, kun halutaan välttää toinen, vielä suurempi riski. (Yates & Stone, 1992; Fischhoff, 1992)

ISO (International Organization for Standardization) määrittelee riskin omassa sanastossaan (ISO Guide, 2009) tavoitteeseen kohdistuvaksi epävarmuustekijäksi. Riski on poikkeama odotetusta lopputulemasta ja tämä voi ISO:n mukaan olla negatiivinen tai positiivinen poikkeama. Riski mielletään usein tapahtumaksi ja seuraamukseksi tai näiden yhdistelmäksi (ISO Guide, 2009).

Kuten ISO Guide (2009), myös Baccarini, Salm & Love (2004) määrittelevät riskin sellaiseksi todennäköisyydeksi, että jotain projektiin jollain tavalla negatiivisesti vaikuttavaa voi tapahtua. Vaikutus voi ilmetä lopputuloksessa tai itse prosessissa. Riskiä ei kuitenkaan tässä tapauksessa nähdä positiivisena asiana, vaan sitä tarkastellaan ainoastaan negatiivisena tapahtumana. (Baccarini ym., 2004)

Bannermanin (2008) mukaan riski on altistumista tietyille tekijöille, jotka ovat uhkana asetetun tavoitteen saavuttamiselle. Yksinkertaiseksi kaavaksi Bannerman (2008) esittelee seuraavaa: **R = P x I**, missä **R** on riski, **P** on todennäköisyys ja **I** on vaikutus, jonka riski toteutuessaan luo. Vaikutus on yleensä mitattavissa rahana tai aikana. (Bannerman, 2008)

Riski on terminä löytänyt tiensä myös Oxfordin (2018) tietosanakirjaan, jossa se määritellään sellaisena mahdollisuutena, että jotain ikävää tai epämukavaa tapahtuu – esimerkiksi sydän- ja verisuonisairauksien riski. Berg (2013) määrittelee riskin epävarmaksi lopputulemaksi, jolla on haitallisia vaikutuksia, mutta mainitsee myös, että riski voi olla neutraali. Bergin (2013) mukaan riski viittaa epävarmuuteen, joka ympäröi tulevaisuuden tapahtumia ja lopputulemia. Se ilmaisee todennäköisyyden sekä tapahtuman vaikutuksen organisaation asettamiin tavoitteisiin. (Berg, 2013)

Suomen Pankki (2018) luokittelee informaatioteknologiaan liittyvät riskit operatiivisiksi riskeiksi. Operatiivisella riskillä Suomen Pankin (2018) mukaan tarkoitetaan sellaista riskiä, jossa sisäisistä prosesseista, henkilöstöstä, järjestelmistä tai ulkoisista tekijöistä aiheutuu tappiota tai ylimääräisiä kustannuksia. Valtioneuvosto (2015) taas määrittelee riskin suuruuden koostuvaksi kahdesta eri osasta: tapahtuman todennäköisyydestä sekä sen seurausvaikutuksista. Riskien arvioinnissa on myös tarkoitus järjestää riskit jonkinlaiseen järjestykseen toisiinsa suhteutettuna. Arvioinnin perusteena käytetään Valtioneuvoston (2015)

mukaan riskilukua, todennäköisyyttä tai seurausvaikutuksia. (Suomen Pankki, 2018; Valtioneuvosto, 2015)

Tietoturvaan sekä tietojärjestelmiin kohdistuvat riskit määritellään ominaispiirteiden mukaan. Tietojärjestelmäriskit Salmela (2008), kuten muutkin ylempänä, määrittelee epävarmuustekijäksi. Tässä tapauksessa kuitenkin epävarmuustekijä kohdistuu tietokonepohjaiseen järjestelmään, jonka tarkoituksena on tarjota tietoa. Tietojärjestelmän riskit voivat olla tarkemmin tietojärjestelmän osioiden, kuten omaisuuden, laitteiston, ohjelmiston, datan, tallenteiden tai tiedostojen muokkaamista, tuhoamista, varastamista tai saatavuuden puutetta. Tietojärjestelmiin kohdistuvat riskit voivat lisäksi tulla joko sisältä tai ulkoa. Ne voivat olla luonnonkatastrofeja, vahinkoja tai tarkoituksenmukaisia toimia. (Salmela, 2008; Straub & Welke, 1998)

Tietojärjestelmiin kohdistuvat riskit ovat oma alueensa ja niiden lisäksi on riskejä, jotka kohdistuvat tietojärjestelmien turvallisuuteen. Straub & Welke (1998) määrittelee tietojärjestelmien turvallisuuteen liittyvät riskit organisaation tiedon tai tietojärjestelmän osan suojaamattomuudeksi tietynlaisia tapahtumia tai tietynlaista vahinkoa vastaan. Nykyteknologia tarjoaa hyvät, mutta monessa tapauksessa riittämättömät työkalut riskien pienentämiseen ja torjuntaan. Esimerkeiksi Whitman (2003) listaa salasanat, varmuuskopiot ja virusturvan. (Straub & Welke, 1998; Whitman, 2003)

Tietojärjestelmiin sekä tietojärjestelmien turvallisuuteen liittyvien riskien lisäksi voidaan tunnistaa myös tietoturvallisuuteen liittyviä riskejä. Gordon & Loeb (2002) mukaan tietoturvallisuudessa tärkeää on ylläpitää CIA-tasapainoa. Jos yksikin osa-alue tästä perusrakenteesta jää huomiotta, on tietoturvallisuus auttamatta vaarantunut. CIA on lyhenne englanninkielisistä termeistä, jotka tarkoittavat luottamuksellisuutta, eheyttä sekä saatavuutta (*engl. confidentiality, integrity, availability*). Tämä tarkoittaa sitä, että tiedon tai dokumenttien tulee olla luottamuksellisia, eli vain niiden saatavissa, joilla on tarve niille. Tiedon tulee olla eheää ja oikeellista, eli se ei voi muuttua missään vaiheessa vääränlaiseksi. Näiden kahden lisäksi tiedon täytyy olla saatavilla aina, kun sitä tarvitaan. Tietokoneiden kokonaisvaltainen rooli organisaatioissa on luonut uuden uhkan järjestelmille. Tietokoneet ovat vastuussa siitä, että tarjottu data vastaa tietoturvallisuuden määritelmää ja henkilöstön vastuulla on ylläpitää tätä kokonaisuutta. Kokonaisuuden oikeellinen ylläpito varmistaa sen, että tietoturvallisuuteen liittyvät riskit pienenevät. (Dhillon, 2004; Stewart, 2004)

Kuten ylläolevista määritelmistä voi nähdä, riskit voidaan kokea myös positiivisina riskeinä ja termin määrittely ei aina ole yksioikoista. Tässä tutkimuksessa riskejä lähestytään toimeksiantajan compliance-osaston näkökulmasta sekä pyritään luomaan malli, jonka avulla nimenomaan ulkoisten kyberturvallisuuden riskien arviointi olisi helpompaa. Kyberturvallisuuden riskejä käsitellään tässä tutkimuksessa tietenkin riskin perusmääritelmän mukaisesti, mutta kyberturvallisuuden riskit luokitellaan erityisesti tietojärjestelmiin, niiden turvallisuuteen sekä tietoturvallisuuteen kohdistuviksi riskeiksi (luku 2.5). Tutkimuksessa riskiä käsitellään ainoastaan negatiivisena, ulkoa kohdistuvana tapahtumana, joka voi vaikuttaa haitallisesti yrityksen toimintaan.

Ilmosen, Kallion, Kosken & Rajamäen (2010) mukaan riskit voidaan jakaa niiden tyypin tai lähteen mukaan. Riskityyppejä ovat strategiset, taloudelliset, operatiiviset sekä vahinkoriskit. Jokainen tyyppi voi olla sekä sisäinen, että ulkoinen. Tällöin täytyy riskien arvioinnin prosessissa miettiä sitä, mikä on riskin lähde. Riskin lähteen määrittelyn jälkeen saadaan ymmärrys siitä, onko riski ulkoinen vai sisäinen. Ilmonen ym. (2010) kategorisoivat finanssialan riskit kuvion 1 mukaisesti. Riskin lähde tarkoittaa sellaista tekijää, joka vaikuttaa riskin toteutumiseen. Riskin toteutumiseen vaikuttavia tekijöitä voi olla useita ja joskus se on seurausta pidemmästä ketjureaktiosta. Riskit voivat olla siis organisaation sisäisiä, kuten valintoihin ja toimintoihin liittyviä, tai organisaatiosta riippumattomia, ulkoisia tekijöitä. Ulkoinen riski voi olla esimerkiksi asiakkaisiin, markkinoihin, lainsäädäntöön tai luonnonmullistuksiin liittyvä riski. (Ilmonen ym., 2010)

Riskikategoriat

Strategiset riskit	Taloudelliset riskit	Operatiiviset riskit	Vahinkoriskit
1.Liiketoiminnan kehitykseen liittyvät riskit 2. Liiketoimintaympäristöön liittyvät riskit 3. Markkinariskit 4. Teknologiariskit 5. Poliittisen, taloudellisen ja kulttuurisen kehityksen riskit 6. Regulaatioriskit 7. Globaaleista ilmiöistä johtuvat riskit (ilmasto, ympäristö, jne.) 8. Viestintäriskit 9. M&A riskit	1. Likviditeettiriskit 2. Korkoriskit 3. Valuuttariskit 4. Vastapuoliriskit 5. Maariskit 6. Sopimusriskit 7. Veroriskit 8. Kirjanpidon ja talousraportoinnin riskit 9. Pääomarakenteen riskit	1. Organisaatioon ja johtamiseen liittyvät riskit 2. Informaatioteknologiaan liittyvät riskit 3. Tietoturvallisuusriskit 4. Tuotannolliset, toimintaprosesseihin ja tehokkuuteen liittyvät riskit 5. Liiketoiminnan keskeytysriskit 6. Tuottavuusriskit 7. Projektitoimintaan liittyvät riskit 8. Sopimus- ja vastuuriskit 9. Kriisitilanteisiin liittyvät riskit 10. Rikosriskit	1. Työterveys- ja työturvallisuusriskit 2. Henkilöstöriskit 3. Ympäristöriskit 4. Vahingoittumisriskit 5. Luonnonkatastrofeihin liittyvät riskit 6. Toimitilaturvallisuuden riskit

KUVIO 1 Riskikategoriat (Ilmonen ym. 2010)

Voidaan ajatella, että ulkoiset riskit ovat monesti sellaisia, joihin organisaatio itse ei pysty vaikuttamaan. Riskiin voidaan kuitenkin varautua ja siltä voidaan pyrkiä suojautumaan parhaalla mahdollisella tavalla. Silloin ulkoiset riskit eroavat sisäisistä riskeistä oleellisesti juurikin tältä osalta. Sisäiset riskit ovat normaalisti sellaisia, joihin organisaatio pystyy vaikuttamaan paremmin esimerkiksi kouluttamalla henkilöstöä tai luomalla kunnollisen dokumentaation henkilöstölle. Dokumentaatio voi sitten käsittää ohjeet sosiaalisesta mediasta aina USB-laitteiden käsittelyyn. Sisäiset riskit voivat toisaalta johtua piittaamattomuudesta, mutta voivat olla myös vahinkoja. Oleellista on, että organisaatio itse, omilla toimillaan kykenee vaikuttamaan näiden riskien toteutumisen todennäköisyyteen.

Riskienhallinta

Kuten aikaisemmin todettiin, myös riskienhallinta on moniulotteinen termi ja sen voi mieltää useammalla tavalla riippuen niin organisaation toimintaympäristöstä kuin käsittelevän henkilön taustoista. Berg (2010) jakaa riskienhallinnan kahteen erilaiseen tapaan hallita turvallisuutta. Ensimmäinen tapa on seurausperäinen hallinta. Seurausperäisessä hallinnassa keskitytään siihen, että pahimmallakaan mahdollisella lopputulemalla ei ole vaikutusta tietyn rajan toisella puolella. Tapahtuma pyritään rajaamaan pahimmassakin tapauksessa niin tehokkaasti, että se ei pääse karkaamaan muille osa-alueille. Toinen tapa on riskikeskeinen turvallisuuden hallinta. Tämä jälkimmäinen tapa mielletään perinteiseksi riskienhallinnaksi ja on myös se näkökulma, jota tässä tutkielmassa käsitellään riskienhallintana. Riskienhallinta tarkoittaa, että jäännösriski analysoidaan sekä todennäköisyyden että vaaran luonteen osalta. Näin saadaan paljon informaatiota riskin vaikutusten lieventämiseksi. Perinteinen riskienhallinnan malli myös ehdottaa, että jotkin erittäin epätodennäköiset tapahtumat voitaisiin myös hyväksyä sellaisenaan. (Berg, 2010; Lanne, 2007)

Bergin (2010) ja Project Management Body of Knowledgen (PMBOK, 2013) mukaan riskienhallinta on keskeinen osa hyvää hallintoa ja päätöksentekoa jokaisella organisaation osa-alueella, sillä jokainen organisaation taso vastaa tahollaan riskienhallinnasta jopa tietämättään. Riskienhallintaa onkin hyvä pyrkiä ohjaamaan koko organisaation kattavaksi toiminnaksi (IRM, 2002; ISO 31000, 2009).

Aivan kuten riski, myös riskienhallinta on vaikea määritellä yksioikoisesti, ja riskienhallinnalla on useampia erilaisia määritelmiä. Joissain tapauksissa riskienhallintaa kuvataan kokonaisena prosessina, joka sisältää riskien tunnistamisen, arvioinnin ja päätöksenteon riskien ympärillä. Yhtenä yleisesti hyväksyttynä määritelmänä Berg (2010) pitää ajatusta siitä, että riskienhallinta on systemaattinen lähestyminen päätöksentekoon, jossa pyritään asettamaan paras mahdollinen kurssi epävarmuustekijät huomioon ottaen. Epävarmuustekijöiden huomioiminen tarkoittaa sitä, että tunnistetaan, arvioidaan, ymmärretään, toimitaan ja kommunikoidaan riskin ympärillä tapahtuvat asiat mahdollisimman tehokkaasti. Tällöin vaaditut resurssit riskienhallintaan voidaan varata jo etukäteen. (PMBOK, 2013; Berg 2010)

Riskienhallinnan voi myös mieltää iteratiiviseksi ja jatkuvaksi prosessiksi, jossa ennakoivasti käsitellään asioita jo ennen kuin ne tapahtuvat. Riskienhallinta on tärkeä prosessi, jolla pyritään hallitsemaan organisaation kulurakennetta, aikatauluissa pysymistä sekä laadukasta toimintaa. Riskienhallinta voi olla muodollista tai epämuodollista toimintaa riippuen tilanteen, projektin tai yrityksen luonteesta (Rakos, Dhanraj, Kennedy, Fleck, Jackson & Harris, 2005). Tämä lisää aikaisemmin mainittua monikäsitteisyyttä ja hankaloittaa osaltaan termin määrittelyä. Koska riskienhallinta on iteratiivinen prosessi, se on myös jatkuva prosessi, joka ei pysähdy koskaan. Tutkimuksessaan Spears & Barki (2010) määrittelevät tietojärjestelmien (IS, *engl. Information Systems*) turvallisuuden riskienhallinnan jatkuvaksi riskien tunnistamisen sekä priorisoinnin, että kontrollien implementoinnin ja valvonnan prosessiksi. Turvallisuuden riskienhallinnan (SRM, *engl. Security Risk Management*) tarkoituksena on koota yhteen

strategiat, politiikat, toiminnot, roolit, toimenpiteet ja ihmiset, jotka hallitsevat turvallisuuden riskejä. Tästä kokonaisuudesta syntyvät ohjaimet alentavat riskien todennäköisyyttä sekä vaikutusta. SRM:n tarkoitus on pitää kasassa tietoturvallisuuden CIA, eli tiedon luottamuksellisuus, eheys ja käytettävyys (Spears & Barki, 2010).

ISO Guide (2009) määrittelee riskienhallinnan koordinoiduiksi toimiksi, joilla pyritään ohjaamaan ja kontrolloimaan organisaatiota riskeihin liittyvissä toimissaan. Riskienhallinnalle pyritään luomaan runko (*engl. framework*). Runko on työkalupakki, joka tarjoaa pohjan ja perustukset organisaatiolle luoda kunnolliset puitteet riskienhallinnan suunnitteluun, toteutukseen, valvontaan, arviointiin ja jatkuvaan parantamiseen koko organisaatiossa. ISO Guide (2009) on siis samoilla linjoilla Bergin (2010) sekä Rakosin ym. (2005) kanssa siitä, että riskienhallinta on jatkuva prosessi, jolla pyritään tuottamaan lisäarvoa yritykselle (ISO Guide, 2009; Berg, 2010; Rakos ym., 2005).

Riskienhallintaa ja riskianalyysiä ei välttämättä kannata tarkastella sisäkkäisinä prosesseina, vaikka ne usein sellaiseksi mielletäänkin. Gerber ja Solms (2005) toteavat riskienhallinnan olevan riskianalyysin jälkeinen toimenpide, joka koostuu heidänkin mukaansa riskianalyysiin perustuvista toimintaa ohjaavista toimenpiteistä. Toimenpiteiksi he luettelevat suunnittelun, valvonnan ja kontrolloinnin, kun taas riskianalyysi koostuu riskien tunnistamisesta. Riskien tunnistaminen pitää sisällään vakavuuden, vaikutusten sekä todennäköisyyden arvioinnin. Gerber & Solms (2005) lainaavat Scarffia (1993) sekä Frosdickia (1997) ja vetävät yhteen riskienhallinnan ja riskianalyysin kokonaisvaltaiseksi riskien hallitsemiseksi.

Kyberturvallisuuden riskien arviointi on hyvin samankaltaista kuin miksi riskien arviointi mielletään yleisesti tekniikan alalla tai esimerkiksi organisaatioiden toiminnan suojaamisessa ja jatkuvuuden suunnittelussa. Kyberturvallisuuden riskit ovat vain yksi osa-alue, johon informaatioteknologian riskienhallinnassa keskitytään. Youngin (2009) mukaan organisaatiot ovat hyvin riippuvaisi informaatioteknologiasta. Riippuvuussuhde johtaa siihen, että kuten tietoturvallisuutta, myös kyberturvallisuutta kannattaa lähestyä nimenomaan riskien kannalta.

Laajalti hyväksytyssä muodossa oleva esimerkki riskienhallinnan yleisestä prosessista löytyy mm. IRM:n (2002) ohjeistuksesta. Ohjeistuksessa riskienhallinta on kuvattu aikaisemmin mainittuna iteratiivisena ja jatkuvana prosessina, jonka perustaksi on sijoitettu organisaation strategiset tavoitteet. Kun strategiset tavoitteet ovat selvillä, voidaan siirtyä riskien arviointiin, joka pitää sisällään kaksi kokonaisuutta. Riskien arviointiin lukeutuvat IRM (2002) mukaan riskianalyysi, joka pitää sisällään riskien tunnistamisen, kuvaamisen ja estimoinnin. Analyysin lisäksi arviointiin kuuluu myös evaluaatio, joka nojaa analyysissa tuotettuun dataan. Vaikka nämä onkin sijoitettu samaan kokonaisuuteen, niitä tulisi tarkastellaan omina palikoinaan, jotka yhdessä muodostavat kokonaisuuden. Kun riskien arviointi saadaan valmiiksi, raportoidaan uhkat ja mahdollisuudet tarkasti koko ajan organisaation suuntaan kommunikoiden. Raportoinnin jälkeen tehdään päätöksiä siitä, mihin suuntaan riskien kanssa liikutaan ja

miten riskejä käsitellään. Riskien käsittelyn jälkeen jäännösriskit raportoidaan tarkasti jälleen organisaation suuntaan kommunikoiden. Prosessin lopussa siirrytään seurantavaiheeseen, jonka aikana arvioidaan tehtyjä toimenpiteitä ja niiden vaikutuksia riskeihin. Tätä prosessia toistetaan jatkuvasti ja sen aikana syntyy uusia näkökulmia sekä uusia tapoja torjua riskejä. Prosessia voidaan tukea jatkuvasti muodollisella auditoinnilla ja tehtyjä päätöksiä pyritään haastamaan. Riskienhallinta ei ole koskaan valmis, vaan pienimmätkin asiat kehittyvät ajan myötä. (IRM, 2002)

Kyberturvallisuuden riskienhallinta ja arviointi on hankala prosessi, jossa monesti turvaudutaan intuitioon. Baskerville (1991) käsittelee artikkelissaan riskien analysointia ja riskienhallintaa sekä pyrkii selittämään, miksi riskienhallinta on laajasti hyväksytty prosessi, vaikka sen yhtenä isona osa-alueena on vahva intuitio ja jopa tuuri. Baskervillen (1991) artikkelista saa käsityksen, että riskienhallinnan hyödyt työkaluna ja kommunikointivälineenä ovat ajaneet tieteellisen pohjan ohi. Riskienhallinta ei täytä kunnolla tieteellisen metodin ominaispiirteitä. Riskien vaikutukset ja epävarmuus nojaavat liikaa tuuriin ja mikäli onnettomuus ei toistu, johdolla ei ole mitään palautetta siitä, onnistuuko riskienhallinnan kehittäminen. Tästä syystä kehotetaankin keskittymään suurempiin kokonaisuuksiin eikä pelkästään yksittäisiin tapauksiin riskien arvioinnissa ja riskienhallinnan suunnitelmia laadittaessa. (Baskerville, R. 1991)

Esimerkkinä kyberturvallisuuden riskienhallinnan sekä yleisestä riskienhallinnan hankalasta tieteellisestä pohjasta Baskerville (1991) esittelee Popperin (1935) tieteelliset lait, jotka ovat hyviä teorioita, mutta ne ovat kuitenkin vain teorioita, joita ei käytännössä välttämättä kyetä hyödyntämään. Nämä teoriat pohjaavat olettamuksiin ja yleistyksiin, joissa oletetaan, että asioiden tila ei muutu ajan kuluessa. Todellisuus kuitenkin on, että Popperin (1935) lait eivät pidä riskienhallinnassa paikkaansa, mikäli yksikin ehto muuttaa muotoaan. Tämä tarkoittaa sitä, että riskien analysointi ja riskienhallinta eivät ole tieteellisesti täysin valideja metodeja. Toisaalta myöskään fundamentaaliset fysiikan laitkaan eivät saavuta Popperin lakia siitä, että mikään ei poikkea oletetusta (Baskerville, R. 1991).

Jotta riskienhallinta olisi riittävän tehokasta, tulee organisaation toiminnan täyttää tietyt uskomukset, käyttäytymismallit, kyvyt ja toiminnot. Kun nämä osa-alueet tulevat täytetyiksi, organisaatio samalla todistaa, että tietoturvallisuus on sille hallinnollisesti vakavasti otettu aihe (Allen, 2005; Whitman & Mattord, 2012). Allen (2005) sekä Whitman & Mattord (2012) jakavat nämä osa-alueet viiteen tarkempaan kokonaisuuteen:

- Turvallisuusperiaatteita sovelletaan koko organisaation tasolla.
- Turvallisuutta käsitellään, kuten mitä tahansa muuta liiketoimintaan vaikuttavaa kokonaisuutta.
- Turvallisuus otetaan huomioon päivittäisissä rutiineissa, suunnittelussa ja operationaalisissa toimissa.

- Turvallisuus integroidaan organisaation toimintoihin ja prosesseihin.
- Kaikki mukana olevat toimijat, joilla on pääsy organisaation verkkoon, ymmärtävät heidän yksittäisen vastuunsa. Toimijoiden tulee kunnioittaa turvallisuutta ja pyrkiä suojaamaan organisaation turvallisuus.

Vaikka riskienhallinnan määritelmä on monikäsitteinen ja se nojaa kovasti olettamuksiin ja alan tai toimijoiden asiayhteyksiin, voidaan ylläolevia määritelmiä hyödyntää erinomaisesti kyberturvallisuuden riskienhallinnassa sekä riskien arvioinnissa. Aivan kuin kyberturvallisuuden riskit, myös kyberturvallisuuden riskienhallinta kohdistuu tutkimuksessa samoille osa-alueille tietojärjestelmissä ja tietoturvallisuudessa. Tutkimuksessa tarkastellaan ulkoisia tekijöitä, joten riskienhallinnassakin keskistytään siihen, miten ulkoa tulevia kyberturvallisuuden riskejä voidaan arvioida. Aikaisemmin on todettu, että riskienhallinta prosessina on sellainen, mihin koko organisaation tulee ottaa osaa. Tiedottamisen organisaation suuntaan tulee olla hyvää ja siinä ei saa olla katkoksia. Näin turvataan riskienhallinnan suurempi onnistumisprosentti, kun kaikki ovat tietoisia siitä, mitä ollaan tekemässä ja miksi. Tästä päästäänkin riskienhallintaa ohjaaviin tekijöihin, jotka samalla toimivat tärkeänä tiedottamisen välineenä organisaation suuntaan.

2.2 Organisaation strategia

Riskien arviointia ohjaavia tekijöitä on useita. Niistä yksi, riskienhallinnan pohjankin luova tekijä on organisaation strategia (IRM, 2002). Kuten IRM:n (2002) mallista nähdään luvussa 3, on organisaation strategia lähtökohtana koko riskienhallinnalle ja näin ollen se on myös riskien arviointiin suuresti vaikuttava tekijä. Riskienhallinnan pohjan lisäksi strategia on yrityksen liiketoiminnalle tärkeä kulmakivi (Nieminen, 2016). Strategialla organisaatio kuvaa sen, miten se voi tuottaa arvoa nyt ja tulevaisuudessa yhteistyökumppaneilleen sekä sidosryhmilleen (Kaplan & Norton, 2004). Organisaation strategian kehittyminen tapahtuu pikkuhiljaa sekä suunnittelun kautta että erilaisten sisäisten toimintatapojen ohjaamana (Porter, 1980).

Yrityksen tavoitteena on sijoittua omaan toimintaympäristöönsä sopivalla tavalla, kilpailuedun saavuttamista, ja strategian tehtävänä on ohjata organisaatio tavoitteeseensa. Kilpailuedun saavuttamiseksi organisaatio havainnoi muuttujia toimintaympäristössään ja pyrkii vastaamaan toimintaympäristöä muovaaviin tarpeisiin. (Porter, 1980). Nieminen (2016) on Porterin kanssa samoilla linjoilla ja toteaa, että organisaatio määrittelee tavoitteet sekä ohjaa omaa toimintaansa huomioiden jatkuvasti muuttuvan toimintaympäristön sekä tarpeet, joita jatkuva muutos tuo tullessaan. Strategian ajantasaisuuden takaamiseksi organisaation täytyy kyetä myös muuttamaan strategiaa tarvittaessa (Nieminen, 2016). Strategiaa varten organisaation on kartoitettava resurssinsa ja päätettävä,

miten näiden voimavarojen tuottama arvo voidaan maksimoida (Kaplan & Norton, 2000).

Arvo ei ole yksiselitteinen käsite tässä tapauksessa, sillä se on riippuvainen yrityksen toimintaympäristöstä sekä strategiasta. Organisaation kokonaisarvo koostuu abstrakteista ja konkreettisista elementeistä. Konkreettisia esimerkkejä ovat mm. rahallinen omaisuus, kalusteet ja osakkeiden osuus. Abstrakteja elementtejä ovat mm. brändin tunnettavuus, hyvä tahto, julkinen hyöty ja tavaramerkki. (PMBOK, 2013; Kaplan & Norton, 2000)

Paras arvo sekä kilpailuetu organisaatiossa saavutetaan, kun strategiaa käytetään ohjaamisen lisäksi johdon ja työntekijöiden yhteisenä kommunikaatiovälineenä ja -kielenä, kuten Mantere, Tienari, Vaara & Välikangas. (2008) ehdottavat. Strategian luonne on pohtimista ja keskustelua. Strategia on osa organisaation kehittämistä, hyvinvointia ja johtamista. Strategia luo pohjan yritystoiminnalle sekä asettaa yhteisesti sovitun suunnan, jota organisaatio lähtee tavoittelemaan. (Mantere ym,. 2008).

Mauryn (2016) mukaan vaikka suomalaisissa organisaatioissa strategia on yleensä erinomaisesti suunniteltu ja raportoitu, niin sen ymmärtää sekä pystyy kuvaamaan vain 13 prosenttia organisaation ylimmästä johdosta ja vain kahdeksan prosenttia keskijohdosta. Vielä huolestuttavampaa on se, että Mauryn (2016) mukaan tavallisista työntekijöistä 98% ei tiedä, mihin suuntaan organisaatio on menossa ja mitä se tavoittelee. Strategian voidaan siis päätellä olevan merkityksellinen myös organisaation lopputuotteelle, sillä kaiken työn jälkeen organisaation lopputuote on se, mihin strategia vaikuttaa eniten.

Organisaation kyberturvallisuuden riskienhallinnalla pyritään suojaamaan niin organisaation omaisuus kuin organisaation toimintakin. Loppupeleissä organisaation lopputuote on se, joka tuo organisaatiolle kilpailuedun ja tekee organisaatiosta tuottavan sen sidosryhmien silmissä. Strategia ei ole organisaatioissa kuitenkaan niin hyvin ymmärretty asia, että siitä saisi kaiken mahdollisen hyödyn riskienhallintaan. Onkin helppo spekuloida, miksi organisaatioiden strategia ei välity työntekijöille asti. Onko kyse siitä, että työntekijöitä ei kiinnosta sisäistää strategiaa? Eivätkö he ymmärrä organisaation strategiaa esimerkiksi liian hankalan kielen tai epäselvän rakenteen takia? Onko strategiaa loppupeleissä edes jaettu työntekijöille asti vai onko se vain jokin abstrakti käsite, jonka olemassaolon työntekijät tiedostavat, mutta eivät ymmärrä asiasta sen enempää? Näistä kysymyksistä voisikin tehdä kokonaan uuden tutkimuksen liittyen organisaation strategian ymmärtämiseen sekä strategian ymmärtämisen vaikutuksen organisaation tuloskehitykseen sekä sen tuottavuuteen sidosryhmien silmissä.

2.3 Organisaatiokulttuuri

Organisaation strategian lisäksi riskien arviointia ohjaavana tekijänä voidaan tunnistaa myös organisaatiokulttuuri. Tsohou, Karyda, Kokolakis & Kiountouzis (2006) mukaan kulttuurilla on suora vaikutus organisaation riskienhal-

lintaan ja riskien arviointiin, koska kulttuuri määrittelee sen, miten yksilöt ja sitä myötä organisaatiot kokevat esimerkiksi riskin vaikuttavuuden. Kulttuuri on abstrakti käsite, jolla on vaikutusta yksilöiden käytökseen sosiaalisissa tilanteissa sekä voima ohjata organisaatiota oikeaan tai väärään suuntaan (Schein, 1985).

Organisaatiokulttuuria määritellessä tulee Scheinin (1985) mukaan ottaa huomioon kulttuurin syntyminen, joka vaatii suurta määrää yhteisiä kokemuksia sekä yhteistä historiaa. Nämä kokemukset, jotka synnyttävät organisaatiokulttuuria, ovat ongelmatilanteista selviämistä ja näiden kohtaamista yhdessä. Kulttuuria tarkasteltaessa Schein (1985; 1999) listaa kolme eri tasoa: organisaation näkyvät rakenteet ja prosessit, perusoletukset sekä organisaation arvot strategioineen, päämäärineen ja filosofioineen. Nämä kolme tekijää myös muokkaavat yksilöiden näkemyksiä sekä kykyjä arvioida riskejä (Tsohou ym., 2006). Vanhalan, Laukkasen ja Koskisen (2002) mielestä organisaatiokulttuurista puhuttaessa kulttuurin voi määritellä vain, jos organisaatiosta löytyy riittävästi yhteisiä piirteitä, jotka ovat kehittyneet ajan myötä. Kulttuuri itsessään koostuu Scheinin (1985) mukaan arvoista, uskomuksista, perinteistä, käytännöistä sekä tavoista. Jäsenet organisaatiossa jakavat nämä osaset keskenään jollain tavalla ja siirtävät ne eteenpäin uusille tekijöille sekä tuleville sukupolville.

Lämsä ja Hautala (2005) pitävät myös yllä esiteltyä Scheinin määritelmää yhtenä tunnetuimpana organisaatiokulttuurin kuvauksena. Heidän mukaansa kulttuuri voidaan jakaa kolmeen osaan:

1. organisaatiokulttuuri on yhteinen identiteetti, joka määrittelee sen mitä ja ketä organisaation jäsenet ovat
2. organisaatiokulttuuri sitouttaa jäsenet organisaation arkeen ja pyörittämiseen
3. organisaatio luo sekä selventää käyttäytymissääntöjä sekä yhteisiä pelisääntöjä työpaikalla.

Lämsä ja Hautala (2005) mainitsevat myös, että tarinat ja yhteiset tapahtumat kehittävät organisaatiokulttuuria jatkuvasti.

Organisaatiokulttuurin muuttaminen ei pidä olla ensimmäinen askel organisaation kehittämiseen, sillä se on erittäin hidasta. Organisaation kehittämiseksi kulttuurin muuttaminen on kuitenkin pakollista. Organisaatiokulttuurin muuttaminen auttaa kehityksessä, koska silloin työntekijät eivät asetu muutosta vastaan, vaan kokevat sen hyödylliseksi (Mattila, 2007). Kokkomäki & Nortunen (2016) listaavat Lämsää ja Hautalaa (2005) mukaillen organisaatiokulttuurin muutosta edistäviksi asioiksi seuraavat pääkohdat:

- organisaation jäsenten jatkuva kouluttaminen ja kehittäminen
- toimintatapojen muuttaminen sekä arkirutiineissa, että työympäristössä
- organisaation rakenteiden uudelleenjärjestely
- käsitteiden, tapojen sekä tarinoiden päivittäminen

- muutospaine, joka juontaa juurensa äkillisestä ja dramaattisesta ulkoisesta tapahtumasta
- organisaation jäsenten palkitseminen, arviointi ja kiittäminen
- esimiesten sekä muiden avainhenkilöiden vaihtuminen
- uusiin arvoihin sekä päämääriin tähtäävät ihanteet.

Selvää on se, että välinpitämättömässä organisaatiossa myös kulttuuri on välinpitämätön ja siellä kulttuuria on hankala, mutta ei mahdoton kehittää paremmaksi. Välinpitämättömässä kulttuurissa myös riskienhallinta on haastavaa. Mikäli ihmiset eivät välitä tekemisistään, vaikuttaa se tietenkin suoraan kyberturvallisuuden riskienhallintaan ja resursseja täytyy kohdistaa enemmän sisäisten uhkien tunnistamiseen ja näistä syntyvien riskien estämiseen kuin ulkoisista uhkista selviämiseen. Jotta voitaisiin saavuttaa kyberturvallisuuden ja tietoturvallisuuden kannalta ihanteellinen ympäristö, joka itsessään ylläpitää riskienhallinnan periaatteita, tulee organisaatiokulttuuria pyrkiä muuttamaan paremmaksi näiden tavoitteiden kannalta. Kuten yllä on kuvattu, organisaatiokulttuurin muuttaminen on hidas ja paljon resursseja syövä prosessi, mutta se on myös pakollinen prosessi. Mikäli organisaation halutaan päätyvän erinomaiseen kyberturvallisuuden riskienhallinnan prosessiin, tulee resurssit kohdistaa oikein ja ne tulee kommunikoida hyvin myös organisaation jäsenille. Aivan kuten kiteytyksessä mainitaan, myös Boehm (1991) sanoo, että muutokset käytänteisiin tulee aina ottaa käyttöön mieluummin askel askelelta kuin kaikki kerralla.

2.4 Tietoturvapolitiikka

Organisaation strategian ja organisaatiokulttuurin lisäksi riskien arviointia ohjaavana tekijänä voidaan pitää organisaation tietoturvapolitiikkaa. Tietoturvapolitiikka on riskienhallinnan työkaluna hyvä, sillä se pohjautuu organisaation strategiaan sekä toimintaympäristön tarpeisiin (Kokkomäki & Nortunen, 2016). Sanastokeskuksen sanakirjan mukaan tietoturvapolitiikalla tarkoitetaan sellaista organisaation hyväksymää kokonaisuutta, joka ohjaa tietoturvan päämääriä, periaatteita sekä toteutusta (Sanastokeskus TSK, 2004). Tästä syystä tietoturvapolitiikalla on suora vaikutus organisaation strategiaan, riskienhallintaan ja sitä myötä myös riskien arviointiin.

Tietoturvapolitiikkaa määritellessä voidaan tukeutua Bulgurcu, Cavusoglu & Benbasat (2010) rakentamaan määritelmään. Heidän mukaansa tietoturvapolitiikka on selvitys organisaatiossa olevista rooleista ja vastuista, joihin työntekijät on nimetty. Sen tarkoitus on pitää huoli, että kaikki organisaation toimijat noudattavat turvallisia tapoja tiedon, laitteiden ja tilojen käsittelyssä. Politiikassa erotellaan roolit sekä vastuut tiedon, datan sekä teknisten laitteiden ja muiden resurssien turvaamisessa (Bulgurcu ym., 2010). Tarkoituksena tietoturvapolitiikalla on tarjota ohjeita ja selkeyttä organisaation tietoturvan suojaamiseen, kuten riittävät käytänteet ja mekanismit (Wood, 1999).

Tietoturvapolitiikka on ohjeistus tai järjestely, joka on luotu ylläpitämään organisaation tietoturvaa ja tietoturvallisuutta. Tietoturva finanssialalla on tärkeä kokonaisuus, sillä finanssiala on tarkkaan säädeltyä. Yhtenä korkeamman tason valvojana Suomessa toimii Finanssivalvonta. Koska ala on niin tarkkaan valvottu, voidaan olettaa, että myös tietoturva alan organisaatioissa olisi oikealla mallilla. Kuten aikaisemmin tässä luvussa on todettu, tietoturva koostuu luottamuksellisuuden, eheyden ja käytettävyyden säilyttämisestä (*CIA*) (Gordon & Loeb, 2002; ISO/IEC 27000:2018). CIA:n lisäksi tietoturvassa pyritään kiinnittämään huomiota myös tunnistettavuuteen, kiistämättömyyteen, vastuullisuuteen sekä luotettavuuteen (ISO/IEC 27000:2018). Tietoturvallisuus varmistaa sen, että oikea tieto on saatavilla vain sitä tarvitseville, oikeudet saaneille tahoille (luottamuksellisuus, *engl. confidentiality*). Tiedon tulee olla sellaista, kuin se on alun perin tarkoitettu olevaksi (eheys, *engl. integrity*), eli tieto ei ole muuttunut tai jollain muulla tavalla vaarantunut. Tiedon tulee lisäksi olla aina saatavilla, kun sitä tarvitaan (käytettävyys, *engl. availability*) (Whitman & Mattord, 2010). CIA-periaate on saanut osakseen myös arvostelua. Dhillon & Backhouse (2000) arvostelevat CIA-periaatetta, koska heidän mukaansa teknologian kehitys aiheuttaa sen, että tietoturvallisuus on kaksiteräinen miekka. Samalla, kun tietoa pyritään suojaamaan, se pyritään myös saattamaan saataville mistä ja milloin tahansa sitä tarvitaan.

Hale & Swusten (1998) määrittelevät tieteen alalla käytetyt turvallisuussäännöt sellaiseksi järjestelmän ennalta määritetyksi tilaksi tai toimintatavaksi, joka on mahdollista ennakoidussa tilanteessa. Toimintatavat ja tila on määritelty tällöin ennen tapahtumaa sekä hyväksytty järjestelmään turvallisuutta parantavana järjestelmänä tai tapana saavuttaa vaadittu turvallisuuden taso.

Whitman & Mattordin (2010) näkemyksen mukaan tietoturvapolitiikkoja on organisaatioissa yleensä kolmentyylisiä: EISP, ISSP sekä SysSP. Enterprise Information Security Policy (*EISP*) on kokonaisuus, joka kuvaa yleistä tietoturvaa organisaatiossa. Lisäksi EISP kuvaa strategisen informaatioteknologian suunnitelman. Issue Specific Security Policy (*ISSP*) on sääntökokonaisuus, jonka avulla organisaation työntekijät osaavat käyttää sovelluksia, laitteita tai vaikkapa käyttäytyä sosiaalisessa mediassa tietoturvallisella tavalla. System-specific Policy (*SysSP*) on tekninen, hallinnollinen tai molempia kuvastava kokonaisuus. SysSP hallinnoi teknologioita tai käyttöoikeuksia erilaisten listojen avulla, kuten Access Control List (*ACL*). (Whitman & Mattord, 2010)

Tietoturvapolitiikka määrittelee organisaation tietoturvallisuuden sekä myös tietoturvapolitiikan itsessään. Tämä on tärkeä vaihe, sillä määritelmiä on useita ja tietoturvapolitiikassa tulee tehdä selväksi se, miten organisaatiossa tietoturva tulee ymmärtää ja miten sitä käsitellään (Höne & Eloff, 2002). Tietoturvapolitiikassa tulee ottaa huomioon organisaatiokulttuuri, organisaation strategia sekä organisaation työntekijät ja tahot, jotka tietoturvapolitiikkaa pyrkivät noudattamaan. Hönen ja Eloffin (2002) mukaan organisaatiolla tulee olla selkeä yhteinen kuva siitä, kuka hyväksyy tietoturvapolitiikan, kuinka kattava se on ja mitä se pitää sisällään. Tietoturvapolitiikka on lisäksi aina organisaa-

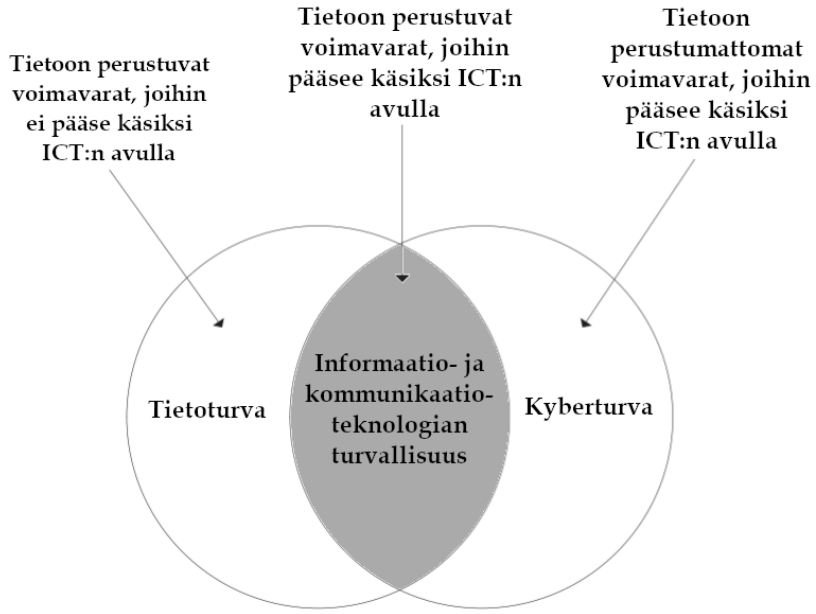
tiokohtainen ja millään organisaatiolla tietoturvapolitiikka ei voi olla samanlainen.

Tietoturvapolitiikka saattaa olla, kuten organisaation strategiakin, erittäin hyvin laadittu kokonaisuus, mutta haasteena on usein sen käyttöönotto. Kokkomäki & Nortunen (2016) puhuvat siitä, kuinka pelottavana tietoturvallisuuden keskiössä olevaa kybermaailmaa pidetään Suomessa. Ihmisten pelko on sinänsä aiheellista, sillä kyberturvallisuus ei ole pelkkää teknistä tietokoneiden leikkikenttää. Yksi suurimmista tekijöistä tietoturvallisuuden rikkoontumisessa on inhimillinen virhe tai ajattelemattomuus. Inhimillistä tekijää (*engl. human factor*) voi pienentää erilaisilla koulutuksilla ja organisaation onkin hyvä panostaa henkilökunnan kouluttamiseen sekä listata tämä strategiassaan (Kokkomäki & Nortunen, 2016).

Sen lisäksi, että tietoturvapolitiikka listaa organisaation tietoturvakäytänteet sekä määrittelee tietoturvan organisaatiossa, se myös listaa seuraamuksia tietoturvarikkomuksista sekä tietenkin tietoturvapolitiikan mukana vaikuttavat liitteet (Hakala, Vainio & Vuorinen, 2006). Tietoturvarikkomukset tässä tapauksessa ovat tietoturvapolitiikan vastaisia toimia, jotka altistavat organisaation uhille ja näistä aiheutuville riskeille. Kuten aikaisemmin on todettu, tietoturvan yksi suurimpia ongelmakohtia ovat inhimilliset tekijät. Inhimillisiä tekijöitä vähentääkseen organisaation tulee luoda tietoturvapolitiikasta sellainen, että kuka tahansa voi sen lukea ja ymmärtää. Tietoturvapolitiikat ovat usein julkisia, joten niissä ei saa käyttää sellaista tietoa, mikä lisää hyökkäysvektoreiden määrää (Miettinen, 1999). Yleensä tietoturvapolitiikan liitteet luokitellaan salaisiksi ja niistä löytyvä tieto tulee pitää organisaation sisällä (Hakala ym., 2006). Tietoturvapolitiikka on olemassa, jotta organisaation strategia tietoturvallisuuden osalta sekä organisaation suhtautuminen tietoturvaan välittyisi myös organisaation työntekijöille. Tietoturvapolitiikka itsessään on hyvä pitää lyhyenä ja ytimekkäänä (Miettinen, 1999).

2.5 Kyberturvallisuutta vai tietoturvallisuutta

Luvussa aikaisemmin esiteltyyn riskienhallinnan laajempaan viitekehykseen mahtuu pienempiä kokonaisuuksia, joista seuraavaksi käsitellään kyberturvallisuutta sekä tietoturvallisuutta. Nämä osittain päällekkäin menevät termit koetaan monesti samaksi asiaksi, mutta Von Solms & Van Niekerk (2013) huomauttavat, että ne ovat vain osittain päällekkäisiä termejä. Kyberturvallisuus kattaa myös tietoturvallisuuden, mutta on laajempi kokonaisuus, jossa turvataan tiedon lisäksi muutkin organisaatiolle arvoa tuovat voimavarat, kuten työntekijät (kuvio 2). Tietoturvallisuudessa inhimilliseen tekijään viitataan yleensä, kun tarkoitetaan henkilön osallisuutta turvallisuusprosessissa, mutta kyberturvallisuus laajentaa käsitteen myös mahdolliseksi hyökkäysvektoriksi. Tämä tarkoittaa sitä, että turvallisuusprosessin osana yksilöt ovat myös mahdollisia kohteita, joita vastaan pahantahtoinen toimija voi hyökätä. (Von Solms & Van Niekerk, 2013).



KUVIO 2 Tietoturvallisuuden ja kyberturvallisuuden suhde (Von Solms & Van Niekerk, 2013 mukaillen)

Kyberturvallisuus on saavuttanut viime aikoina kansainvälistä huomiota ja yli 50 valtiota on julkaissut kyberturvallisuusstrategian, jossa ne ottavat kantaa kybertilaan (*kyberavaruus, kybertoimintaympäristö*), kyberrikoksiin ja kyberturvallisuuteen (Klimburg, 2012). Näiden 50 valtion joukossa on myös 33 valtiota, jotka sisällyttävät kybersodan armeijansa suunnitteluun ja organisointiin (Lindström, 2012). Valtiot panostavat merkittäviä summia oman kyberturvallisuutensa säilyttämiseen (Von Solms & Van Niekerk, 2013).

Kyberturvallisuus ymmärretään usealla eri tavalla ja onkin tärkeää, että se pyrittäisiin määrittelemään mahdollisimman yhtenäisesti. Yksi määritelmistä on esimerkiksi Oxfordin (2018) sanakirjasta löytyvä tietokoneiden tai järjestelmien suojaaminen luvatonta pääsyä tai hyökkäystä vastaan. Von Solms & Van Niekerk (2013) määrittelevät kyberturvallisuuden ITU:a (*The Internationam Telecommunications Union*) mukaillen:

- työkalupakiksi
- käytänteiksi
- turvallisuuskäsitteiksi
- turvatoimiksi
- ohjeistuksiksi
- riskienhallinnan lähestymistavoiksi
- toimenpiteiksi
- kouluttamiseksi ja harjoitteluksi
- parhaiksi käytänteiksi
- luottamukseksi
- teknologioiksi.

Tätä koko pakettia käytetään organisaation kybertilan puolustamiseen. Puolustuskohteita ovat organisaation sekä yksilöiden voimavarat, jotka pitävät sisällään:

- tietokoneet ja ICT-laitteet
- henkilöstön
- infrastruktuurin
- sovellukset
- palvelut
- telekommunikaatiojärjestelmät
- organisaation koko datan. (Von Solms & Van Niekerk, 2013)

Kyberturvallisuus pyrkii samaan kuin aikaisemmin esitelty tietoturvallisuus, eli säilyttämään sekä organisaation että henkilöstön voimavarojen luottamuksellisuuden, eheyden ja käytettävyyden. Eheyteen liitetään myös kiistämättömyys (*engl. non-repudiation*) sekä datan oikeellisuus (*engl. authenticity*). (Von Solms & Van Niekerk, 2013; ITU, 2018)

Kyberturvallisuuden käsite on saanut jalansijaa myös Suomessa (Limnéll, 2014). Suomalainen määritelmä kyberturvallisuudelle löytyy mm. Lehdon ja Kähkösen (2015) artikkelista, jossa he määrittelevät kyberturvallisuuden kybertilan puolustamiseksi kyberhyökkäyksiä vastaan. Kyberturvallisuus on heidän mukaansa toimenpiteiden sarja, jotka pyrkivät suojaamaan organisaation kyberhyökkäysten vaikutuksilta. Kyberturvallisuus tarjoaa työkalut kyberhyökkäysten vastaisiin toimiin aivan kuin riskienhallinta tarjoaa työkalut riskejä vastaan toimimisessa. Kyberturvallisuus pohjautuu organisaation tekemälle uhkaanalyysille, joka on osa riskienhallintaa ja tarkemmin osa riskien arviointia ja tunnistamista (Lehto & Kähkönen, 2015).

Monen muun maan tavoin myös Suomella on oma kyberturvallisuusstrategiansa. Siinä Turvallisuus- ja puolustusasiain komitea määrittelee kyberturvallisuuden sellaiseksi tavoiteltavaksi tilaksi, jossa kybertila on luotettava ja turvattu. Tätä tavoitetilaa avataan kyberturvallisuusstrategiassa hieman enemmän toteamalla, että tavoitteen toteutuessa kybertilasta ei aiheudu mitään ongelmia tiedon käsittelylle. Luottamus kybertilaan pohjautuu toimijoiden (*yhtei-*

sön) riittävään tietoturvallisuusmenettelyyn. Nämä menettelyt johtavat tavoitetilassa siihen, että riskien toteutuessa järjestelmä on kykenevä estämään, lieventämään ja sietämään syntyviä vaikutuksia. Kyberturvallisuusstrategian mukaan kyberturvallisuus on toimenpiteitä, jotka pyrkivät ennakoimaan, sietämään ja suojaamaan Suomen yhteiskuntaa sekä infrastruktuuria näihin kohdistuvilta toimilta, jotka aiheuttaisivat ongelmia Suomelle tai yhteiskunnalle. (Turvallisuus- ja puolustusasiain komitean sihteeristö, 2013)

3 Riskienhallinnan mallit

Tässä luvussa esitellään riskienhallinnan menetelmiä, jotka kaikki käsittelevät myös riskien arviointia osana koko mallia. Riskienhallinnan kannalta riskien tunnistaminen ja luokittelu ovat tärkeitä toimenpiteitä, mutta vielä tärkeämpiä ne ovat riskien arvioinnin kannalta. Riskienhallintaa varten on kehitetty useampi malli, joista tässä tutkielmassa käsittelyyn otetaan Project Management Body of Knowledge (PMBOK), ISO-standardi 31000 sekä Institute of Risk Managementin 2002 julkaisema riskienhallinnan standardi. Lisäksi myöhemmin luvussa 4 luodaan katsaus ISO 27001-standardiin, kansalliseen turvallisuusauditointikriteeristöön (Katakri) ja Suomen valtiovarainministeriön julkaisemaan VAHTI-ohjeeseen. Mitä tarkemmin riskit on tunnistettu ja luokiteltu, sitä varmemman arvion niistä pystyy tekemään. Huomionarvoinen seikka on kuitenkin se, että riskien arviointi on aina subjektiivista. Mallit ja työkalut valittiin tutkimukseen käsiteltäviksi, koska ne ovat tunnettuja sekä standardoituja kokonaisuuksia ja myös tutkittava organisaatio hyödyntää niitä riskienhallinnan työssään lukuun ottamatta PMBOKia, joka on yleisluonteensa takia tutkijan mukaan ottama malli.

3.1 Project Management Body of Knowledge

Vaikka PMBOK (2013) onkin kehitetty alun perin projektinhallintaa ohjaavaksi työkaluksi, on siinä esitelty malli myös erittäin yleispätevä kokonaisuus kyberturvallisuudenkin riskienhallintaan. PMBOK (2013) on alallaan erittäin hyvin tunnettu teos, joka määrittelee riskin epävarmuuden tilaksi tai tapahtumaksi, joka vaikuttaa projektiin ennalta-arvaamattomalla tavalla. Tässä tapauksessa PMBOKin (2013) mukaan riski voi olla siis myös positiivinen. Tutkimuksessa positiiviset riskit jätettiin tarkastelun ulkopuolelle, sillä ne ovat kyberturvallisuuden kannalta erittäin harvinaisia. Negatiivinen riski nähdään aina uhkana organisaation toiminnalle eri osa-alueilla ja se voi vaikuttaa lopputuotteen laatuun, kehittämisen aikatauluihin tai esimerkiksi synnyttää

lisää kustannuksia. Riski voi olla yksittäinen tekijä tai useamman tapahtuman tai tekijän summa ja riski on läsnä kaikessa, mitä organisaatio tekee. PMBOK (2013) jakaa riskienhallinnan pieniin palasiin, joita noudattamalla organisaatio kykenee luokittelemaan ja torjumaan riskejä.

Riskienhallinnan pohja luodaan PMBOKin (2013) mukaan riskienhallinnan suunnittelutyöllä. Suunnitteluvaiheessa kuvataan, miten riskienhallinnan toimenpiteitä tai aktiviteetteja tullaan toteuttamaan projektissa tai organisaation päivittäisissä toimissa. Jo suunnitteluvaiheessa on hyvä kommunikoida tehty työ koko organisaatiolle, jotta organisaation työntekijät pysyvät tietoisina riskienhallinnasta alusta asti.

Suunnitelman jälkeen on PMBOKin (2013) mukaan aika riskien tunnistamiselle. Tässä prosessissa määritellään kaikki riskit, joilla on mahdollisuus vaikuttaa organisaation toimintaan tai projektin valmistumiseen. Tärkein vaihe riskien tunnistamisessa on riskien dokumentointi. Kunnolla tehty dokumentointi auttaa riskienhallinnan työryhmän ulkopuolellakin olevia organisaation työntekijöitä ymmärtämään riskien vakavuutta. Riskien tunnistamisen prosessin on tarkoitus selvittää kaikki mahdolliset riskit, jotka vaikuttavat projektiin jollain tavalla. Tähän vaiheeseen palataan usein, sillä kaikkia riskejä ei pysty tunnistamaan kerralla. Kuten mainittu, riskienhallinta on kokonaisuutena iteratiivinen prosessi. Dokumentoinnin aikana riskit tulee jollain tavalla saattaa sanalliseen muotoon. Dokumentoinnin tärkein virka on riskien tunnistamisen selkeyttäminen ja pohjan luominen jatkotoimenpiteille sekä riskien arvioinnille. Riskien tunnistamiseen voivat osallistua organisaation työntekijät sekä sidosryhmät ja usein työryhmässä on esimiesten lisäksi avainhenkilöitä, jotka ovat erikoistuneet riskien tunnistamiseen. (PMBOK, 2013)

PMBOKin (2013) määritelmän mukaan tehty riskien tunnistaminen jakaantuu kolmeksi kokonaisuudeksi. Ne nimetään syötteeksi (input), työkaluiksi ja tekniikoiksi sekä tulosteeksi (output). PMBOKin (2013) mallin mukaiset syötteet ovat:

1. riskienhallinnan suunnitelma
2. kustannusten hallintasuunnitelma
3. aikataulun hallintasuunnitelma
4. laadunhallintasuunnitelma
5. henkilöstöresurssien hallintasuunnitelma
6. ulottuvuuden tai laajuuden hallintasuunnitelma
7. toimenpiteiden kustannusarvio
8. toimenpiteiden keston arviointi
9. sidosryhmistä luotu rekisteri
10. projektin (tässä tapauksessa organisaation) dokumentit
11. hankintoihin liittyvät dokumentit
12. organisaation ympäristötekijät
13. organisaation voimavarat (*engl. assets*).

Työkaluiksi ja menetelmiksi PMBOK (2013) määrittelee seuraavat kokonaisuudet:

1. dokumenttien katselmointi
2. tiedonkeräysmenetelmät
3. tarkistusluettelojen analysointi
4. olettamuksien analysointi
5. kaavioiden luominen ja graafiset tekniikat
6. SWOT-analyysi
7. asiantuntijoiden arviot.

Kaikesta tästä työstä ja analysoinnista syntyy ihanteellisessa tilanteessa hyvin jäsennelty ja selkeä lopputuotos, johon PMBOK (2013) viittaa tulosteena. Riskien arviointia tehdessä tulee huomata se, että mikäli jokin PMBOKin määritelmässä esitellyistä dokumenteista tai suunnitelmista on puutteellinen tai sitä ei ole, vaikeutuu riskien arviointiprosessi huomattavasti, koska lopputuotos perustuu puutteelliselle datalle. Vaikka tämä määritelmä on suunnattu erityisesti projektityöskentelyyn, on hyvä huomata, miten kokonaisuutena se on yleistettävissä koskemaan koko organisaation riskienhallintaa sekä kyberturvallisuuden riskienhallintaa. (PMBOK, 2013)

Riskianalyysin ja riskien arvioinnin PMBOK (2013) jakaa kahteen osaan, kvalitatiiviseen sekä kvantitatiiviseen riskianalyysiin. Kvalitatiivisessa riskianalyysissa riskit priorisoidaan jatkokäsittelyä varten. Priorisoinnissa riskit laitetaan vakavuusjärjestykseen arvioimalla niiden todennäköisyyksiä sekä riskien vaikutuksia, jos ne toteutuvat. Kvantitatiivinen riskianalyysi taas tarkoittaa sitä, että riskit analysoidaan numeerisesti. Kvantitatiivisessa riskianalyysissa pyritään arvioimaan, miten tunnistetut riskit vaikuttavat projektin tai organisaation eri osa-alueisiin.

Kvalitatiivinen riskianalyysi tarkoittaa laadullista riskien analysointia (PMBOK, 2013). Siinä riskit priorisoidaan myöhempiä vaiheita varten ja keskitytään riskien toteutumisen todennäköisyyteen sekä riskin toteutuessa tämän vaikutuksen voimakkuuteen ja laajuuteen. Tällöin riskien järjestäminen tärkeysjärjestykseen voidaan tehdä edellä mainituin kategorioin. Näiden mainittujen kategorioiden lisäksi riskit voidaan järjestää tärkeysjärjestykseen sen mukaan, miten hyväksyttävissä riskin toteutuminen on organisaation silmissä tai millaisen reaktioajan riskin vastatoimenpiteet vaativat. Kvalitatiivisen riskianalyysin yhdeksi tärkeäksi työkaluksi PMBOK (2013) ehdottaa riskimatriisia (kuvio 3). Riskimatriisissa on todennäköisyysasteikko sekä vaikutusasteikko ja näiden prioriteetti määritellään numeerisesti. Kuten useampaan otteeseen on todettu, riskejä tarkastellaan organisaation osa-alueittain useammasta eri näkökulmasta ja käsitellään todennäköisyyden sekä vaikutuksen mukaan. PMBOK (2013) käyttää riskimatriisissa kolmea eri värikoodia kuvastamaan riskin tasoa ja vakavuutta. Nämä värit ovat korkea, keskitaso ja matala. Jokaisesta osa-alueesta luodaan oma matriisi liittyen samaan riskiin, organisaation osa-alueet voivat olla esimerkiksi lopputuotteen laatu, kehittämisen aikataulu tai kustannusrakenne.

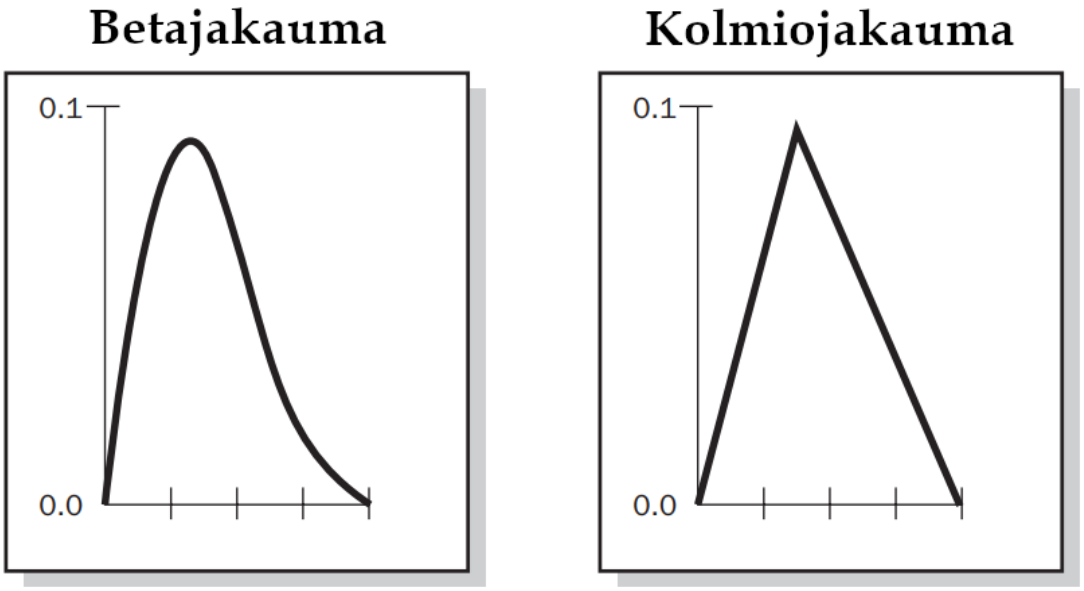
Todennäköisyys ja vaikutus
Riskimatriisi

Todennäköisyys	Uhka					Mahdollisuus				
0.90	0.05	0.09	0.18	0.36	0.72	0.72	0.36	0.18	0.09	0.05
0.70	0.04	0.07	0.14	0.28	0.56	0.56	0.28	0.14	0.07	0.04
0.50	0.03	0.05	0.10	0.20	0.40	0.40	0.20	0.10	0.05	0.03
0.30	0.02	0.03	0.06	0.12	0.24	0.24	0.12	0.06	0.03	0.02
0.10	0.01	0.01	0.02	0.04	0.08	0.08	0.04	0.02	0.01	0.01
	0.05/ Erittäin matala	0.10/ Matala	0.20/ Keskitaso	0.40/ Korkea	0.80/ Erittäin korkea	0.80/ Erittäin korkea	0.40/ Korkea	0.20/ Keskitaso	0.10/ Matala	0.05/ Erittäin matala

Vaikutus (*numeerinen arvo*) osa-alueeseen (*lopputuotteen laatu, kehittämisen aikataulu, kulurakenne*)
Jokainen riski luokitellaan sen toteutuessa todennäköisyyden sekä vaikutuksen mukaisesti osa-alueeseen nähden. Organisaation riskin tason alaraja matalalle, keskitasolle sekä korkealle näkyvät matriisissa ja määräävät, mille tasolle riski asettuu osa-alueeseen nähden.

KUVIO 3 Riskimatriisi (PMBOK, 2013 mukaillen)

Kvantitatiivinen riskianalyysi on prosessi, jossa numeerisesti arvioidaan riskien vaikutusta. Kuten kvalitatiivisen analyysin, myös kvantitatiivisen analyysin tarkoituksena on antaa työkaluja riskien määrän ja vaikutuksen minimointiin. Kvantitatiivinen riskianalyysi suoritetaan sellaisille riskeille, jotka on tunnistettu aikaisemmassa kvalitatiivisessa prosessissa. Mikäli dataa ei ole riittävästi saatavilla, kvantitatiivisen analyysin tekeminen ei ole mahdollista. Riskien priorisoinnissa hyödynnetään sekä aikaisempia dokumentteja, että kvalitatiivisessa riskianalyysissä syntynyttä dataa. Kvantitatiivisen riskianalyysin tulokset esitetään graafisina kokonaisuuksina, kuten taulukoina tai kuvioina. Kvantitatiivinen riskianalyysi pyörittelee numeerisia arvoja, kuten todennäköisyysprosentteja, rahallisia arvoja sekä vaikutuksen voimakkuutta. Todennäköisyysjakauma on yksi erittäin yleinen tapa esittää simulaatio todennäköisyyksien jakautumista (kuvio 4). Tämä jakauma esittää epävarmuustekijöitä beetajakaumana tai kolmiojakaumana. Esimerkissä X-akselilla esitetään mahdollista ajan tai kustannuksen arvoa ja Y-akselilla suhteellista todennäköisyyttä. Nämä jakaumat ovat yleensä yhteensopivia kvalitatiivisessa riskianalyysissä tunnistettujen riskien kanssa. (PMBOK, 2013)



KUVIO 4 Todennäköisyysjakauma (PMBOK, 2013 mukaillen)

Kvantitatiivisen riskianalyysin dataa on hyvä tulkita asiantuntijatahon kanssa, sillä he kykenevät tunnistamaan datasta huomionarvoisia kohtia ja ohjaamaan organisaation huomion näihin. He kykenevät myös arvioimaan käytettyjen työkalujen relevanttiuden ja ehdottamaan mahdollisesti uusia tai korvaavia käytänteitä. (PMBOK, 2013)

Kun riskianalyysi saadaan valmiiksi, aloitetaan toimenpiteet riskien neutralisoinnin suunnittelussa. Negatiivisten riskien käsittelyyn PMBOK (2013) listaa neljä erilaista strategiaa. Riskin välttäminen on strategia, jossa organisaatio pyrkii suojelemaan voimavarojaan riskiltä kokonaisuudessaan tai eliminoimaan riskin. Yleensä strategia vaatii sen, että organisaatio muuttaa toimintasuunnitelmaansa välttääkseen riskin toteutumisen. Riskin siirtämisen strategia tarkoittaa sitä, että organisaatio siirtää vastuun ja vaikutuksen kolmannelle osapuolelle. Tällöin organisaation ei itse tarvitse käsitellä riskin vaikutuksia – tämä strategia ei eliminoi riskiä. Riskin lieventämisen (*engl. mitigation*) strategia pyrkii lieventämään riskin vaikutusta tai todennäköisyyttä. Tässä strategiassa toimitaan proaktiivisesti ja pyritään suunnittelemaan toiminta niin, että riskin toteutuessa sen vaikutus jää mahdollisimman pieneksi, mielellään organisaation sietokyvyn (*engl. treshold*) alarajalle. Neljäntenä strategiana PMBOK (2013) listaa riskin hyväksymisen. Tämä strategia ei koskaan ole ideaali, mutta joissain tapauksissa riski on niin pieni tai sen varalta suunnitellut toimenpiteet syövät niin paljon varoja, että riskin eliminointi ei ole kannattavaa. Näitä vastareaktioiksikin (*engl. responses*) kutsuttuja toimenpiteitä ja vaihtoehtoisia reittejä suunnitellaan sen varalta, että riski saattaa toteutua. Samalla pyritään pienentämään uhkia, jotka vaikuttavat organisaatioon. Viimeinen vaihe PMBOKin (2013) mukaan on kontrollivaihe. Kontrollivaiheessa toteutetaan vastareaktiot, jotka on suunniteltu aikaisempien vaiheiden pohjalta. Kontrollivaiheen aikana seurataan jo aikaisemmin tunnistettuja riskejä, kontrollitoimenpiteiden tehokkuutta ja

tunnistetaan riskejä, joita ei aikaisemmin osattu tunnistaa. Kontrollivaihe on myös riskienhallintaprosessin tarkastelua kokonaisuutena sekä tuon kokonaisuuden tehokkuuden arviointia. Riskienhallinta on kuitenkin prosessi, joka ei pääty koskaan, vaan kehittyy iteratiivisen mallin mukaan jatkuvasti. Tärkeää on, että koko prosessi dokumentoidaan mahdollisimman hyvin ja tiedotetaan muulle organisaatiolle. (PMBOK, 2013)

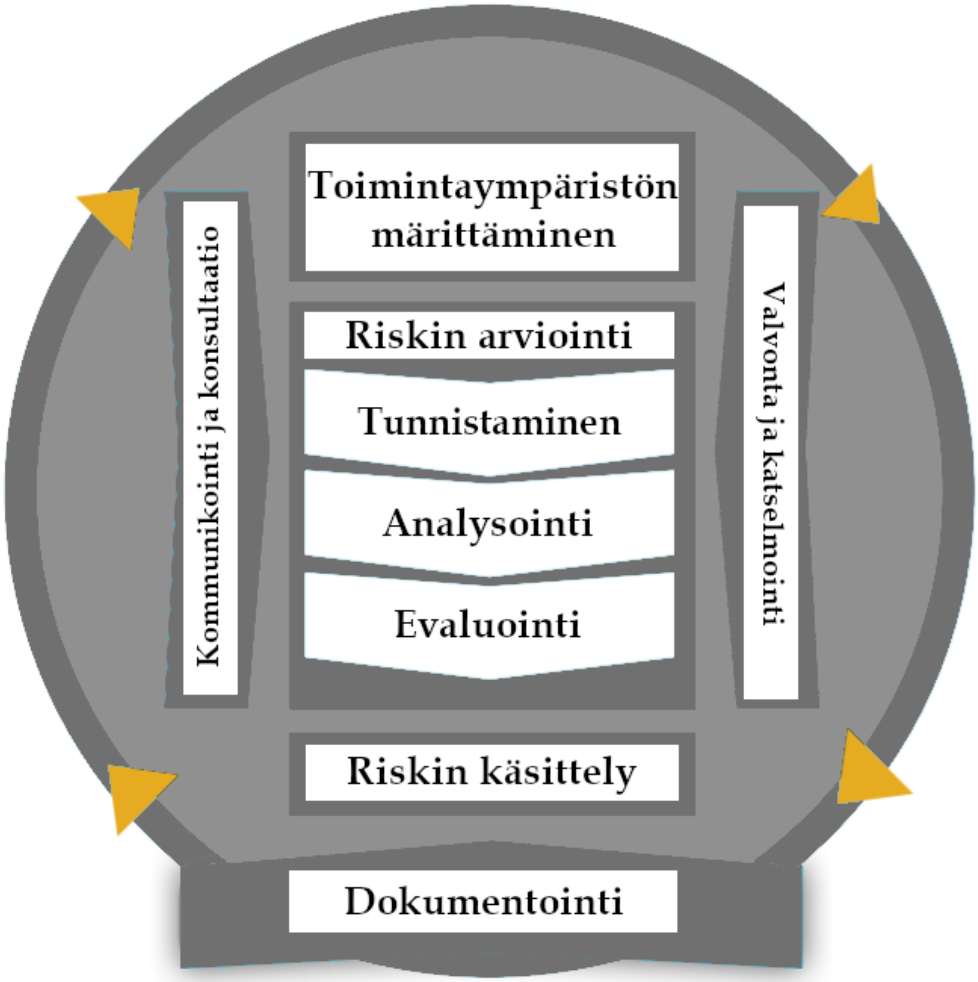
Koska tässä tutkimuksessa on kyse riskien arvioinnista, voidaan riskienhallinnan suunnittelu, vastareaktioiden suunnittelu sekä kontrollivaihe jättää pienemmälle tarkastelulle. Nämä kolme vaihetta eivät ole suoraan riskien arvioinnin menetelmiä, vaan tukityökaluja, jotka auttavat riskienhallinnan kokonaisuudessa ja siksi niitä ei käsitellä esittelyä syvemmin.

3.2 International Organization for Standardization

Riskienhallintaan liittyviä ISO-standardeja on useampia, joista ISO 31000 ja ISO 27001 ovat soveltuvimmat käsiteltäväksi tässä tutkimuksessa. ISO 31000 käsittelee koko riskienhallintaa ja ISO 27001 keskittyy siihen, miten organisaation tulisi järjestää tietoturvallisuutensa. ISO 27001 perustuu kuitenkin riskienhallinnan periaatteille. Tämä tarkoittaa sitä, että ISO 27001 mukaan organisaation tulee turvautua suojakeinoihin vain, jos tunnistetaan hyväksymiskelvottomia riskejä, joihin tulee reagoida. Tässä luvussa keskitytään kuitenkin koko riskienhallintaan ja ISO 31000 -standardiin. ISO 27001 esitellään myöhemmin luvussa 4. Tässä luvussa huomataan, miten samankaltaisia asioita ISO 31000 esittelee PMBOK (2013) kanssa ja tästä syystä projektin riskienhallinnan ohjekirja soveltuu yleistettäväksi myös koko organisaation toimintaan.

ISO, eli International Organization for Standardization on itsenäinen organisaatio, joka on edustettuna 162 maassa. ISO pyrkii standardisoimaan malleja ja käytänteitä usealla eri alalla. Standardoimalla ISO tavoittelee yhtenäistä toimintamallia, joka omalta osaltaan helpottaa haasteiden ratkaisua globaalisti. Tähän mennessä ISO on julkaissut 22654 standardia lähes jokaiselle teollisuuden alalle aina teknologiasta maatalouteen. (ISO, 12/2018)

ISO (2018) määrittelee 31000:2018-standardissaan riskienhallinnan käsitteet ja prosessin. Riskienhallintaa kuvataan standardissa päättymättömäksi, dynaamiseksi ja iteratiiviseksi prosessiksi, joka tapahtuu proaktiivisesti. ISO (2018) kuvaa riskien arviointia kolmen eri kokonaisuuden avulla. Kokonaisuudet ovat riskien tunnistaminen (*engl. identify*), analysointi (*engl. analyse*) sekä merkityksen arviointi (*engl. evaluate*). Kuviossa 5 riskienhallinnan prosessi on esitetty graafisena mallina, joka asettaa riskien arvioinnin riskienhallinnan keskiöön. (ISO, 2018)



KUVIO 5 Riskienhallinnan prosessi 1 (ISO, 2018 mukaillen)

Kuten kuviosta 5 nähdään, dokumentointi, katselmointi ja kommunikointi kulkevat arvioinnissa vahvasti mukana koko prosessin ajan ja mikään kohta ei poikkea tästä. Riskien tunnistaminen riskien arvioinnin pohjana on samalla tavalla tärkeä prosessi ISO 31000:2018 -standardin mallissa kuin mitä se on PMBOK (2013) mallissa. ISO 31000:2018 määrittelee riskien tunnistamisen niiden löytämiseksi, tunnistamiseksi sekä dokumentoinniksi. Riskien tunnistamisessa hyödynnetään montaa erilaista datan lähdettä, kuten historiaa, analyysejä, asiantuntijoiden lausuntoja ja sidosryhmiä. Riskien tunnistaminen tapahtuu aina tarpeen ja toimintaympäristön mukaan. Riskien tunnistaminen tulee dokumentoida riskienhallinnan prosessiin, organisaation strategiaan sekä tietoturvapolitiikkaan niin, että se toimii yhteistyössä organisaation muiden dokumenttien kanssa. Riskien dokumentointi tulee ISO 31000:2018 -standardin mukaan olla hyvin jäsenneltyä ja siinä tulee selkeästi riskien identifioinnin lisäksi esitellä riskien syyt ja lähteet, riskitapahtumat, riskien vaikutukset, riskeistä johtuvat seuraamukset sekä riskin omistaja. Riskin omistajan vastuulla on koko riskin hallitseminen ja, jotta riskiä voitaisiin hallita, tulee sillä olla erikseen nimetty vastuuhenkilö. (ISO, 2018)

Riskianalyysi on ISO 31000:2018 -standardin mukaan riskien ymmärtämistä laajemmalla skaalalla sekä riskien vakavuuden määrittämistä. Analyysivaiheessa riskien seuraamukset sekä todennäköisyydet määritellään tarkemmin ja dokumentoidaan selkeästi. Organisaatio hyödyntää analyysissä syntyviä arvoja riskien tasojen määrittämisessä ja priorisoinnin muodostamisessa. Riskianalyysi voidaan tehdä ISO 31000:2018 -standardin mukaisesti kvalitatiivisena tai kvantitatiivisena, mutta eroten PMBOK-mallista (2013), myös semi-kvantitatiivisena. Riskimatriisi on ISO 31000:2018 -standardissakin mainittu työkalu, jota hyödyntämällä riskit voidaan asettaa eri tasoille organisaation sietokyvyn mukaan. Organisaatio valitsee riskianalyysin muodon sen perusteella, mitkä ovat organisaation tarpeet, millaista dataa sillä on käytettävissä ja kuinka luotettavaa tuo data on. Metodit tulee määritellä riskienhallinnan ja riskien arvioinnin määritelmää tehtäessä. Baskervillenkin (1991) kritisoima riskien arviointi ja tulokset eivät koskaan ole tieteellisen tarkkoja, vaan aina pelkkiä olettamuksia ja arvioita. Riskianalyysia tehdessä tulee ottaa huomioon myös olemassa olevat keinot riskien lieventämiseen ja torjuntaan. Riskien torjunnan keinot vaikuttavat aina riskien tasoon. (ISO, 2018)

Riskien evaluointi, toisaalla myös riskien merkityksen arviointi, on vaihe, jossa pyritään arvioimaan riskin merkitys ottaen huomioon organisaation tavoitteet, toimintaympäristö ja konteksti. Riskien evaluoinnissa tulee ottaa kantaa siihen, mihin riskeihin kehitetään vastatoimia ja millaiset ovat riskien prioriteetit. Riskianalyysi tukee riskien merkityksen arviointia ja riskien evaluointi tukee lopullista päätöksentekoa. Tästä syystä riskien merkityksen arviointi tulee dokumentoida erittäin huolellisesti, selkeästi ja helposti ymmärrettävillä termeillä. Dokumentoinnin selkeys tukee myös helppoa ylläpitoa ja päivittämistä tulevaisuudessa. (ISO, 2018)

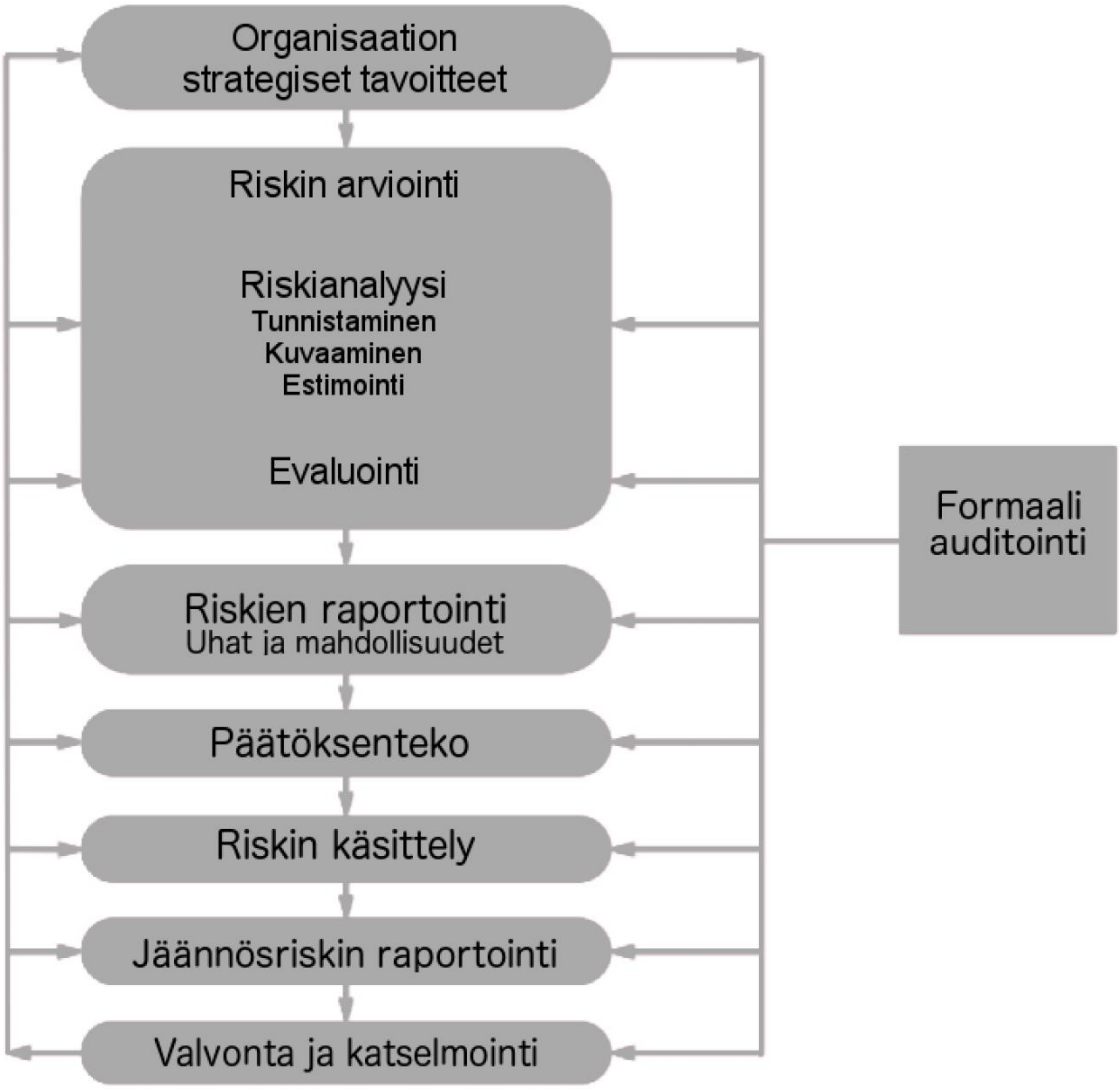
3.3 The Federation of European Risk Management Association ja The Institute of Risk Management

FERMA perustettiin vuonna 1974 ja se on kansallisten riskienhallintayhdistysten kattojärjestö. Järjestöä Suomessa edustaa Suomen riskienhallintayhdistys (SRHY, 2018). FERMA on Euroopan johtava riskienhallintaorganisaatio. FERMAN riskienhallinnan standardi julkaistiin ensimmäisen kerran IRM:n standardina vuonna 2002 ja se hyväksyttiin myöhemmin FERMAN standardiksi (IRM, 12/2018a).

IRM on toinen yritysten riskienhallintaan voimakkaasti vaikuttava järjestö, joka pyrkii kokoamaan ammattilaiset ja osaamisen yhteen paikkaan. IRM:n tehtävä on tarjota koulutuksia ja tutkimustuloksia sekä laatia standardeja riskienhallinnan helpottamiseksi (IRM, 12/2018b).

Molemmat järjestöt siis käyttävät samaa riskienhallinnan standardia, jonka IRM kehitti vuonna 2002. Tästä eteenpäin standardista puhuttaessa viitataan alkuperäiseen IRM:n standardiin. IRM:n (2002) standardi kuvaa käsitteet sekä riskienhallinnan prosessin. IRM (2002) standardi pyrkii myös neuvomaan lukijaa riskienhallinnan tekniikoissa esittämällä esimerkkejä. Standardi on monialainen kokonaisuus, jota ei ole sidottu yhteen asiayhteyteen. Riskienhallinnan tiedostetaan olevan yläkäsite, jota kaikki organisaatiot, julkiset sekä yksityiset, tulevat hyödyntämään toiminnoissaan (IRM, 2002). Kuten aikaisemmat standardit, (ISO 31000:2018 ja PMBOK) myös IRM (2002) eriyttää riskien arvioinnin yhdeksi erilliseksi kokonaisuudeksi riskienhallinnan sisällä. (IRM, 2002)

IRM (2002) jakaa riskien arvioinnin kahteen isompaan kokonaisuuteen, riskianalyysiin ja riskien merkityksen arviointiin (*engl. evaluate*). Riskianalyysi jaetaan edelleen kolmeen pienempään kokonaisuuteen, jotka ovat riskien tunnistaminen, riskien kuvaaminen ja riskien estimointi. Kuviossa 6 IRM-standardin mukainen riskienhallinta ja siihen sisältyvä riskien arvioinnin prosessi on esitetty graafisesti.



KUVIO 6 Riskienhallinnan prosessi 2 (IRM, 2002 mukaillen)

IRM (2002) lainaa riskien arvioinnin määritelmän suoraan ISO Guide (2009) dokumentista. Riskianalyysi on kokonaisuus, josta saatavat tulokset auttavat riskien omistajia ja vastuuhenkilöitä riskien hallitsemisessa sekä resurssien jakamisessa oikeisiin kohteisiin. Lisäksi riskianalyysin tuloksia käytetään tässäkin standardissa riskien ja riskejä vastaan tehtävien toimenpiteiden priorisoinnissa. (IRM, 2002)

Riskien tunnistamisen prosessi pyrkii tunnistamaan organisaation altistumisen epävarmuustekijöille. Epävarmuustekijöiden tunnistaminen vaatii erittäin hyvää tietämystä organisaatiosta ja organisaation toimintaympäristöstä. Toimintaympäristöksi IRM (2002) listaa lakipykälät ja sosiaalisen-, poliittisen- sekä kulttuurisen ympäristön, jossa organisaatio vaikuttaa. Toimintaympäristön lisäksi riskien arviointi vaatii, että organisaation strategiset ja operationaaliset tavoitteet mukaan lukien näihin vaikuttavat tekijät, ovat erittäin hyvin tunnettuja. Että nämä tekijät tunnettaisiin, tulee organisaatiolla olla selkeä strategia, kulttuuri sekä tietoturvapolitiikka. (IRM, 2002)

Riskien tunnistamista tulisi IRM:n (2002) mukaan lähestyä menetelmällisesti, että voidaan varmistua kaikkien organisaatioon vaikuttavien merkittävien riskien tunnistamisesta ja määrittelystä. Kaikki riskien tunnistamisen aikana kerätty data tulee luokitella ja kategorisoida tarkasti – kuten aikaisemmissakin standardeissa, myös IRM (2002) painottaa dokumentoinnin tärkeyttä. Organisaation liiketoimintaan liittyvät aktiviteetit, joihin riskit kohdistuvat, tulee määritellä ja ne voidaan luokitella monella eri tavalla. IRM (2002) luokittelee ne esimerkissään seuraavasti: ”

- **Strategiset** – Organisaation pitkäaikaisiin strategisiin tavoitteisiin. Vaikutus voi tulla esimerkiksi pääomasta, poliittisista riskeistä, laki- ja sääntömuutoksista, maineesta tai fyysisen toimintaympäristön muutoksista.
- **Operationaaliset** – Organisaation päivittäiset operatiiviset, strategian mukaiset toiminnot.
- **Taloudelliset** –Organisaation taloushallinto. Ulkoisina tekijöinä. Esimerkiksi luoton myöntö, valuuttakurssien muutokset, korkojen muutokset ja muut markkinoilla tapahtuvat liikkeet.
- **Tietohallinnolliset** – Organisaation tehokkaaseen tiedon hallinnointiin ja kommunikointiin liittyvät toiminnot. Esimerkiksi ulkoisia riskitekijöitä ovat tiedon luvaton käyttö, sähkökatkokset ja kilpaileva teknologia. Sisäisiä tekijöitä ovat esimerkiksi järjestelmän virheellinen toiminta tai avainhenkilön menettäminen.
- **Määräystenmukaisuus** (*engl. compliance*) – Organisaatiota koskevien määräysten noudattaminen. Esimerkkiriskejä terveyden ja turvallisuuden, ympäristön, kuluttajasuojan, datan suojaamisen ja säännösten sisältämien ongelmien vaikutus.” (IRM, 2002)

IRM (2002) myös toteaa, että riskien tunnistaminen voidaan teetättää ulkoisella asiantuntijataholla, mutta sisäinen, hyvin kommunikoitu yhteistyö on yleensä tehokkaampaa. Joka tapauksessa riskin vastuuhenkilön tulee olla organisaation sisältä. (IRM, 2002)

Riskin kuvaamisen tarkoitus on jäsennellä tunnistettu riski rakenteeltaan selkeään muotoon, kuten taulukkoon. Hyvin ennalta suunniteltu rakenne riskin kuvaamiseen on tärkeää, että voidaan taata lukijan ymmärrys riskin tunnistamisen, kuvaamisen ja arvioinnin prosessista. Oikein taulukkoon kuvattuna avainriskien löytämisen ja riskien priorisoinnin tulisi olla yksinkertainen prosessi. Riskit, jotka vaikuttavat organisaation toimintoihin, voidaan IRM (2002) mukaan kategorisoida strategisiksi, projektiin liittyviksi/taktisiksi tai operationaalisiksi. IRM (2002) esittelee esimerkkitaulukon riskien kuvaamiseen (taulukko 1). (IRM, 2002)

TAULUKKO 1 Riskien kuvaamisen esimerkki (IRM, 2002 mukaillen)

1. Riskin nimi	Kuvaus
2. Riskin vaikutus	Kvalitatiivinen kuvaus tapahtumista, mittakaavasta, tyypistä, määrästä ja riippuvuussuhteista
3. Riskin luonne	Esimerkiksi strateginen, operationaalinen, taloudellinen, tietohallinnollinen tai määräyksiin liittyvä
4. Sidosryhmät	Sidosryhmät ja heidän odotuksensa
5. Riskin numeerinen kuvaus	Merkittävyys ja todennäköisyys
6. Riskin toleranssi / halu	Tappion mahdollisuus ja taloudellinen vaikutus Mahdollisten hyötyjen ja haittojen koko ja todennäköisyys Riskin kontrolloinnin tavoitteet ja niiden haluttu tehokkuus
7. Riskin käsittely ja hallintamekanismit	Ensisijaiset riskienhallinnan keinot tällä hetkellä Luotto nykyisin riskienhallinnan keinoihin Käytänteiden tunnistaminen seuraamis- ja katselmointitarkoituksia varten
8. Mahdolliset toiminnot kehittämiselle	Riskin pienentämisen suositukset
9. Strategian ja politiikan kehittäminen	Strategian ja politiikan kehittämisestä vastuussa olevan toiminnon tunnistaminen

Riskin estimointi on kolmas palanen IRM (2002) esittelemästä riskianalyysistä. Estimaatio voi olla kvantitatiivinen, semi-kvantitatiivinen tai kvalitatiivinen, kuten ISO 31000:2018 -standardissakin. Nämä tavat kuvaavat riskin toteutumisen todennäköisyyttä ja mahdollista seuraamusta riskin toteutumisesta. Esimerkiksi uhkien seuraamukset voivat olla tasoltaan korkeita, keskitasoisia tai matalia. Myös todennäköisyydet voidaan määritellä samalla mittarilla, mutta se vaatii hieman tarkempaa määrittelyä, että todennäköisyys voidaan erotella seuraamuksen tasosta. IRM (2002) luokittelee uhkat sekä positiivisiksi, että negatiivisiksi. Tutkimuksessa käsitellään ainoastaan negatiivisia uhkia ja niistä syntyviä riskejä. Tasot ovat organisaatiokohtaisia ja toisen mallinen ryhmittely voi sopia toiselle organisaatiolle paremmin kuin toiselle. Suurimmalle osalle organisaatioista korkea, keskitaso ja matala ovat riittäviä ja toiset vaativat tarkemmat tasot, kuten erittäin korkea, korkea, keskitaso, matala ja erittäin matala. Seuraavissa taulukoissa (taulukko 2 ja 3) kuvataan IRM:n antama esimerkki todennäköisyyksien ja seuraamusten arvioinnista. (IRM, 2002)

TAULUKKO 2 Seuraamusten taso (IRM, 2002 mukaillen)

Korkea	Korkea taloudellinen vaikutus Merkittävä vaikutus organisaation strategiaan tai operationaalisiin toimintoihin Merkittävä vaikutus sidosryhmiin
Keskitaso	Kohtalainen taloudellinen vaikutus Kohtalainen vaikutus organisaation strategiaan tai operationaalisiin toimintoihin Kohtalainen vaikutus sidosryhmiin
Matala	Matala taloudellinen vaikutus Matala vaikutus organisaation strategiaan tai operationaalisiin toimintoihin Matala vaikutus sidosryhmiin

TAULUKKO 3 Todennäköisyyksien taso (IRM, 2002 mukaillen)

Arvio	**Kuvaus**	**Indikaattori**
Korkea (Todennäköinen)	Esiintyy mahdollisesti vuosittain tai 25% todennäköisyydellä.	Mahdollisuus esiintyä useasti annettuna ajanjaksona (kymmenen vuotta). Esiintynyt hiljattain.
Keskitaso (Mahdollinen)	Esiintyy todennäköisesti kymmenen vuoden ajanjaksolla tai alle 25% todennäköisyydellä.	Voi esiintyä useammin kuin kerran annettuna ajanjaksona. Voi olla hankala hallittava ulkoisten vaikutusten seurauksena. Onko esiintynyt aikaisemmin?
Matala (Epätodennäköinen)	Ei todennäköistä, että esiintyy kymmenen vuoden ajanjaksolla tai alle 2% todennäköisyys esiintymiselle.	Ei ole esiintynyt aikaisemmin. Epätodennäköistä, että esiintyy.

Riskianalyysin jälkeen suoritetaan riskien arvioinnissa seuraava vaihe, joka on riskien evaluointi. Evaluointi tukeutuu täysin riskianalyysissä tuotettuun dataan. Riskianalyysin dataa verrataan organisaation kehittämään riskikriteeristöön. Kriteeristöön organisaatio on listannut esimerkiksi ”kulut, hyödyt, lainmukaiset vaatimukset, sosioekonomiset- ja ympäristötekijät sekä sidosryhmien huolet ja toiveet”. Riskien evaluointiprosessin lopputuotoksena päätetään riskien merkittävyys organisaatiolle sekä se, hyväksytäänkö riski vai aiheuttaako se muita toimenpiteitä. (IRM, 2002)

3.4 Yhteenveto

Kuten tässä luvussa esitellyistä standardeista voidaan tulkita, ne kaikki käsittelevät riskien arviointia samalla tyylillä, joskin hieman eri termeillä. Sisällöltään riskien arvioinnin standardit ovat samankaltaisia ja ne voidaan yleistää myös kyberturvallisuuden riskien arviointimenetelmiksi. Riskien arviointi pitää sisällään useita eri kokonaisuuksia, joita ovat analyysi, tunnistaminen, kuvaaminen, estimointi sekä evaluointi.

Tutkimus pyrkii selvittämään, mikä toimeksiantajalla riskien arviointiprosessissa on ongelmana. Riskien arviointia käsitellään sen laajuudesta huolimatta hyvin pintapuolisesti. Tästä syystä arviointiosiota pyritään tutkimuksessa rakennetulla arviointimallilla parantamaan. Arviointimalli kohdistetaan juuri toimeksiantajan ongelmakohtiin, mutta sitä voidaan käyttää myös muissa organisaatioissa riskienhallintaa täydentävänä työkaluna. Standardit kuvaavat riskiä ja riskin vaikutusta sekä positiivisena että negatiivisena epävarmuustekijänä. Tässä tutkimuksessa kuitenkin keskitytään ainoastaan negatiivisiin epävarmuustekijöihin.

Jokainen standardi korostaa dokumentoinnin tärkeyttä kommunikointivälineenä sekä riskeistä syntyvän datan välittämisen muotona. Riskienhallinta ja -arviointi nähdään iteratiivisena mallina, johon organisaation tulee suhtautua proaktiivisesti jokaisella organisaation tasolla eikä vain ylimmän johdon tai tietoturvahenkilöstön kesken. Jokainen standardi kokee, että riskejä tulee käsitellä sekä kvantitatiivisesti, että kvalitatiivisesti. IRM (2002) ja ISO (2018) molemmat myös lisäävät semi-kvantitatiivisen arviointitason. Riskien arviointi malleissa ei ota kantaa esimerkiksi estimoinnin vaikuttavuus- ja todennäköisyysarvion tietopohjaan. Amara (1981) kuvaakin ajatuksiaan tulevaisuuden ennustamisesta ja on sitä mieltä, että sitä ei voida ennakoida, mutta siihen voidaan vaikuttaa. Tämä korostuu riskien arviointiprosessissa, koska se on kuitenkin aina jossain määrin pyrkimys tulevaisuuden ennakointiin.

Jokainen standardi suosittelee käyttämään numeerista arvoasteikkoa sekä matriisia riskien vaikutusten ja todennäköisyyksien arvioinnissa. Matriisien avulla on helppo priorisoida riskit ja paikantaa avainriskit, jotka vaativat normaalia rajumpia toimenpiteitä. Mallit ovat kattavia, mutta jokainen malli käsittelee riskien arvioinnin taustalla olevaa tietoa hyvin yleisellä tasolla. Mallit eivät vastaa kunnolla esimerkiksi sellaiseen kysymykseen kuin, mistä riskien arvioinnin taustalla vaikuttava tieto riskeistä on peräisin tai millä perusteella iteratiivisessa mallissa riskiarvioita tulisi muuttaa. Kuten Baskervillekin (1991) toteaa, tieto ja arviointi ovat liian paljon riippuvaisia arvioijan omasta intuitiosta. (PMBOK, 2013; ISO, 2018; IRM, 2002)

Luku vastaa itsessään ensimmäiseen tutkimuksen apukysymyksistä **(Millaisia nykymalleja riskien arviointiin on olemassa?)**. Malleja on ehdottomasti olemassa enemmänkin, mutta tutkimukseen valikoidut mallit ovat sen takia relevantteja, että tutkittava organisaatio osittain nojaa kahteen malliin kolmesta esitellystä. Kolmas, PMBOK, on erittäin tunnettu julkaisu ja tutkijan näkökul-

masta hyvä malli yleistettäväksi koko riskienhallintaan mukaan lukien tieto- ja kyberturvallisuus. Luvussa käsiteltiin laajasti myös riskien tunnistamiseen liittyviä tekijöitä, sillä kuten aikaisemmin todettu, epäonnistunut riskin tunnistaminen johtaa väärään arvioon.

4 Tieto- ja kyberturvallisuuden työkaluja

Tässä luvussa tutustutaan ISO 27001 -standardiin sekä kahteen kotimaiseen ohjeistukseen, joiden avulla pyritään ratkomaan tieto- ja kyberturvallisuuden ongelmakohtia organisaation sisällä (VAHTI ja Katakri). ISO 27001 -standardi sekä kotimaiset ohjeistukset ovat erinomaisia ohjenuoria, joita seuraamalla organisaation tietoturvallisuus sekä tietojärjestelmäympäristö voidaan suojata. Nämä ohjenuorat ovat tärkeä lisä riskienhallinnan ja riskien arvioinnin malleille, sillä niiden pohjalta organisaatio kykenee jalkauttamaan riskienhallinnan sekä riskien arvioinnin lopputuloksena saadut dokumentit koko organisaation jokapäiväisiin toimintoihin. Lisäksi luodaan lyhyt katsaus kyberturvallisuuden rikollisuuden luonteeseen, että ymmärretään paremmin, millaisia asioita vastaan organisaatio pyrkii kybertilaansa suojaamaan.

Työkalut ovat erittäin kattavat tieto- ja kyberturvallisuuden ohjeistukset, mutta ne eivät ota kantaa riskien arviointiprosessiin. Kokonaisuudet käydään tutkimuksessa läpi, koska ne ovat luvussa 3 esiteltyjen standardien tapaan toimeksiantajan käytössä ja ohjaavat osaltaan riskienhallintaa lakeihinkin perustuvine määräyksineen. Lisäksi ohjeistukset antavat konkreettisia esimerkkejä siitä, millaisia riskejä kybertilassa toimiva organisaatio saattaa kohdata, jolloin ymmärrys kyberturvallisuuden ulkoisten riskien arviointiprosessin tärkeydestä korostuu.

4.1 VAHTI-ohje

VAHTI-ohje on enemmänkin kansallinen julkaisusarja kuin yksi iso julkaisu. Jokainen VAHTI-ohjeen julkaisu löytyy Valtiovarainministeriön verkkosivuilta (Valtiovarainministeriö, 1/2019). Kyberturvallisuuden ja tietoturvallisuuden kannalta VAHTI-ohje on hyvä ohjeistus ja näin ollen työkalu sekä tilojen suunnitteluun että henkilöstön kouluttamiseen.

Valtiovarainministeriö on luonut VAHTI-elimen (*Valtionhallinnon tietoturvallisuuden johtoryhmä*) valtionhallinnon sekä julkishallinnon tietoturvallisuuden

sekä kyberturvallisuuden, ohjaamisen, kehittämisen ja koordinaation vastuunkantajaksi. VAHTIn työnä on käsitellä tieto- ja kyberturvallisuuden linjauksia sekä toimenpiteisiin liittyviä ohjausasioita. Sen toiminta tukee tietoturvallisuuden päätöksenteossa ja valmisteluissa valtioneuvostoa ja valtionhallintoa. Valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista on tarkoitus vahvistaa tietoturvallisuuden kehittämistyöllä. Lisäksi kehitystyön tavoitteena on vahvistaa tietoturvallisuuden asemaa hallinnon toiminnassa, johtamisessa ja tulosohjauksessa. (VAHTI, 5/2013)

Finanssialan organisaation ulkoisten riskien arvioinnin näkökulmasta johtuen VAHTI-ohjeesta otetaan tarkasteluun vain osa sen useasta julkaisusta. Julkaisuja, jotka tarjoavat työkaluja ulkoisten riskien arviointiin ja riskienhallintaan on useita ja ne rajataan kirjoittajan harkinnan mukaan niihin julkaisuihin, jotka käsittelevät riskienhallintaa sekä ulkoisilta riskeiltä suojautumista. VAHTI-ohje tarjoaa hyvin laajan ohjeistuksen tietoturvallisuuden parantamiseksi ja tiedon suojaamiseksi. Toisin kuin Katakri (2015), VAHTI-ohje on hyvin tarkka määräyksistään ja perustaa ohjeistukset suoraan lainsäädäntöön. VAHTI-ohjetta käytetään Katakrissa (2015) usein viitteenä.

Julkaisussa 4/2013 Henkilöstön tietoturvaohje käsitellään tietoturvallisuutta henkilöstön näkökulmasta. Toimitilojen turvallisuus -osiossa luetellaan hyvin kohteet, jotka voivat aiheuttaa ulkoisia riskejä organisaatiolle. Kokonaisuuksien ollessa kunnossa ulkoisten riskien todennäköisyys laskee huomattavasti. Nämä kokonaisuudet ovat kulunvalvonta, tekninen valvonta, vartiointi, palo-, vesi-, sähkö-, ilmastointi- ja murtovahingot sekä lähettipalvelut ja tietoaineistoja sisältävät lähetykset. Ohjeistuksessa käydään myös läpi henkilökunnan toimintaohjeet riskien minimoimiseksi. (VAHTI, 4/2013)

VAHTI-ohjeen osio 5/2013 Päätelaitteiden tietoturvaohje käsittelee niin ikään yleisellä tasolla sitä, millaisia hyökkäyksiä päätelaitteisiin voi kohdistua. Tämä osio käsittelee hyvin paljon ulkoisia riskejä, jotka kohdistuvat päätelaitteisiin ja osiossa on erittäin hyvät ohjeet henkilökunnalle näiltä riskeiltä suojautumiseen ja riskien vaikutuksen minimointiin. VAHTI (5/2013) listaa seuraavat ulkoa kohdistuvat tekniset riskit:

- Houkuttelemalla käyttäjä asentamaan haitallisia ohjelmistoja tai muodostamaan takaportti päätelaitteelle.
- Houkuttelemalla käyttäjä kytkemään päätelaitteeseen toinen laite (esimerkiksi oheislaite, vaihdettava apumuisti, älypuhelin tai muu laite), ja sen avulla suorittamalla haittaohjelmia tai varastamalla tai muokkaamalla laitteen sisältämiä tai sen kautta käsiteltäviä tietoja.
- Tartuttamalla haittaohjelma käyttäjän vieraillessa sivustolla, jossa on haittaohjelma (drive-by-download).
- Kuuntelemalla päätelaitteen tietoliikennettä tai esiintymällä yhdyskäytävänä tai muuna päätelaitteen tarvitsemana palveluna.

- Lähettämällä käyttäjälle haittaohjelman sisältävä tiedosto esimerkiksi sähköpostin, pikaviestiohjelman tai sosiaalisen median palvelun kautta. Kun käyttäjä avaa tiedoston, haittaohjelma asentuu päätelaitteeseen.
- Kalastelemalla tietoja (phishing) esimerkiksi sähköpostin, pikaviestiohjelman tai sosiaalisen median palvelun avulla. Hyökkääjä voi pyrkiä saamaan käsiinsä esim. uhrin salasanan tai organisaation salassa pidettäviä tietoja.
- Ottamalla laitteeseen etäyhteys esimerkiksi varastettujen ylläpitotunnusten, haavoittuvuuden tai (laitteisto tai ohjelmisto) takaportin avulla.
- Kohdistetulla hyökkäyksellä, jossa hyökkääjällä on tietoa organisaation IT-ympäristöstä ja henkilöistä.

Organisaation riskienhallintaan luodaan katsaus osiossa 4/2001 Sähköisen asioinnin tietoturvallisuuden yleisohje. VAHTI-ohjeen (4/2001) mukaan sähköisiin palveluihin kohdistuvat riskit muuttuvat monipuolisemmiksi todella nopealla tahdilla ja se on jopa nopeampaa kuin perinteisissä palveluissa. Koska finanssialan organisaatioiden toimintaympäristö on siirtynyt kehityksen myötä internetiin, sähköiseen muotoon, koskee tämä osio erittäin hyvin näitä organisaatioita. VAHTI-ohjeen (4/2001) mukaan riskienhallintaan tulee suhtautua kuten perinteistenkin palveluiden riskienhallintaan. Riskejä välttelemällä ja niiden minimoinnilla voidaan välttyä useilta tieto- ja kyberturvallisuuteen kohdistuvilta riskeiltä. VAHTI-ohje (4/2001) painottaa laaja-alaista, ennakoivaa ja aktiivista riskeihin varautumista osana riskienhallintaa tieto- ja kyberturvallisuuden kohdalla. Tästä johtuen tieto- ja kyberturvallisuusratkaisut on hyvä mitoittaa nykyhetkeä paremmiksi. Tällöin voidaan jossain määrin varautua myös tulevaisuuden riskeihin, kun tieto- ja kyberturvallisuusympäristö ovat nykyhetkeä paremmin rakennettuja ja laajemmin mitoitettuja. Tietoturvallisuuden uhkakuvaksi VAHTI-ohje (4/2001) näkee sähköisten kanavien hyödyntämisen ulkoa kohdistuvissa riskeissä. Suurimmaksi riskiksi se mainitsee organisaation palvelimien sekä tietoverkkojen avautumisen ulkoverkkoon. Tämä avaa suuren määrän hyökkäysvektoreita, joita rikolliset voivat hyödyntää. Kuten kirjallisuuskatsauksessa on aikaisemmin mainittu, useat riskit ovat aikaisemmin toteutuneiden riskien johdannaisia. Tässäkin tapauksessa sisäisestä riskistä sen toteutuessa aukeaa tilaisuus usealle ulkoiselle riskille.

VAHTI-ohje on kokoelma ohjeistuksia ja teoriaa sellaisena pakettina, että sitä seuraamalla voi organisaatio suojata oman tieto- ja kyberturvallisuusympäristönsä erittäin hyvin. VAHTI-ohjeen perustuessa vankasti lainsäädäntöön, on se jo pelkästään tämän takia hyvä työkalu organisaatiolle tietoturvallisuuden ja kyberturvallisuuden kehittämiseksi. Kuten voidaan myös todeta, perehtyy VAHTI-ohje hyvin paljon tekniseen tieto- ja kyberturvallisuusympäristön toteutukseen sekä henkilöstön ohjeisiin.

4.2 Kansallinen turvallisuusauditointikriteeristö

Kansallinen turvallisuusauditointikriteeristö (Katakri) on työkalu, jota Suomen viranomainen voi käyttää auditoidessaan organisaatioita ja arvioidessaan organisaation kykyä olla yhteistyössä julkisen hallinnon kanssa. Katakri auttaa viranomaista arvioimaan, miten hyvin kohteena oleva organisaatio kykenee suojaamaan viranomaisen salassa pidettävää tietoa. (Katakri, 2015)

Katakri ei aseta suoria, ehdottomia vaatimuksia tietoturvallisuudelle, vaan se pyrkii valvomaan (*engl. enforce)*, että lainsäädäntöön kirjatut vaatimukset täyttyvät ja toiminta on Suomen kansainvälisten tietoturvavelvoitteiden mukaista. Lisätietolähteinä ja isona osana vaatimuksia Katakrissa viitataan ISO 27001 -standardiin sekä VAHTI-ohjeeseen. Lisäksi Katakri (2015) jakaa vaatimukset kolmeen erilaiseen kokonaisuuteen.

Turvallisuusjohtaminen (T) pyrkii varmistamaan, että organisaatiolla on riittävät turvallisuusjohtamisen valmiudet sekä kyvykkyys. Fyysinen turvallisuus (F) kuvaa salassa pidettävän tiedon fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset. Tekninen tietoturvallisuus (I) jakautuu edelleen kolmeen käsiteltävän tiedon mukaiseen kokonaisuuteen, joita kutsutaan suojaustasoiksi (ST IV, ST III ja ST II). Tekninen tietoturvallisuus kuvailee teknisen ympäristön turvallisuusvaatimukset. (Katakri, 2015)

Katakria voidaan käyttää useampaan tarkoitukseen. Päätarkoitus on kuitenkin työkalu organisaation turvallisuusjärjestelyjen toteutumisen selvittämiseksi yritysturvallisuusselvityksessä sekä viranomaisen käyttämien tietojärjestelmien turvallisuuden kartoittamisessa. Näiden lisäksi Katakria voidaan käyttää myös muussa turvallisuustyössä ja sen kehittämisessä mm. organisaatioissa, yhteisöissä ja virastoissa. NSA (*Kansallinen turvallisuusviranomainen*) on hyväksynyt työkalun käyttöön 26.03.2015. (Katakri, 2015)

Turvallisuusjohtaminen osa-alueena käsittelee niitä kaikkia menetelmiä, mitä tarvitaan turvallisuuden ja sen hallinnan siirtämiseksi osaksi koko organisaation toimintaa. Turvallisuusjohtamisen kokonaisuudessa käsitellään hallinnollisen- ja henkilöstöturvallisuuden vaatimuksia. Nämä vaatimukset pyrkivät varmistamaan sen, että organisaatiolla on riittävät työkalut turvallisuuden hallintaan ja henkilöstön ohjeistamiseen ulkoistenkin kyberturvallisuuden riskien varalta. Katakri (2015) esittelee turvallisuusjohtamisen osa-alueessa toteutusesimerkkejä, joita seuraamalla voidaan useimmissa organisaatioissa ja ympäristöissä saavuttaa riittävä suojauksen taso. Esimerkkejä voidaan muuttaa ja soveltaa sopiviksi omassa organisaatiossa, kunhan vaatimukset täyttyvät. Jotta turvallisuusjohtamisen kokonaisuus olisi tarkoituksenmukainen, tulee arviointi kohdentaa oikeaan osaan organisaatiosta. Tarkastelun kohteeksi tulee ottaa se osa organisaatiota, joka on suorassa tai epäsuorassa yhteydessä tiedon hallinnointiin. Esimerkiksi tarkoituksenmukaisesta kohdentamisesta Katakri (2015) mainitsee tietojenkäsittely-ympäristöä hallinnoivan organisaation osan, joka voi olla esimerkiksi tytäryhtiö. Katakri (2015) ei sanele tiukkoja vaatimuksia, mistä kertoo myös dokumentin muoto. Katakrissa (2015) puhutaan hyvin yleisellä

tasolla vaatimusten täyttämisestä ”riittävinä”. Riittävä toteutustapa voi Katakrin (2015) mukaan vaihdella kohdekohtaisesti. Eri suojaustasojen ohjeistukset eroavat yleisestä, koko organisaatiota koskevasta henkilöstön ohjeistuksesta. (Katakri, 2015)

Toinen iso kokonaisuus, fyysinen turvallisuus, käsittelee tilojen suojaustasoa ja pyrkii varmistamaan, että kaikki tieto on sellaisessa paikassa, johon eivät ulkopuoliset pääse käsiksi. Tarkoituksena on Katakrin (2015) mukaan estää tunkeutuminen, ehkäistä sekä estää ja havaita luvattomat toimet ja lisäksi mahdollistaa tiedon saatavuus henkilöstölle tarpeen ja luokituksen mukaan. Nämä turvatoimet pitää olla kirjattuna organisaation riskienhallintaprosessissa. Fyysinen ympäristö jakaa tilat useampaan eri osa-alueeseen. Nämä osat ovat hallinnollinen alue, turva-alue ja tekninen turva-alue. Organisaation tarve jakaa tilansa alueisiin riippuu salassa pidettävän tiedon luokituksesta. Tämä aluejako perustuu Katakrin (2015) mukaan EU:n turvallisuussääntöihin sekä kansallisiin turvallisuussääntöihin. Kuten turvallisuusjohtamisen kokonaisuudessa, myös fyysisen turvallisuuden kokonaisuudessa Katakri (2015) esittelee esimerkkejä toteutustavoista. Katakrin (2015) mukaan fyysinen turvallisuus nojautuu suunnittelutyöhön, joka luo perustan fyysiselle turvallisuudelle. Katakri (2015) listaa suunnittelun tueksi kahdeksan kohtaa, jotka on hyvä pitää mukana suunnittelun aikana. Nämä kohdat ovat:

1) Missä tiloissa suojattavia tietoja käsitellään ja minkä suojaustason tiedoista on kyse.
2) Missä ympäristössä ja rakennuksen osassa suojattavia tietoja käsitellään.
3) Rakennuksen tai tilan turvajärjestelyt ja rakenteet.
4) Salassa pidettävien tietojen suojaaminen tilassa (luominen, vastaanottaminen, käyttäminen, säilyttäminen ja hävittäminen).
5) Millä tietojenkäsittelyvälineillä ja järjestelmillä tietoja tilassa käsitellään.
6) Tietojen määrä; suojattavien tietojen kasautuminen saattaa edellyttää tiukempien turvallisuusvaatimusten soveltamista (esimerkiksi suuri määrä suojaustason IV tietoa saattaa muodostaa suojaustason III kokonaisuuden).
7) Tietoja käsitellään muuten kuin satunnaisesti sellaisissa tiloissa, joiden turvallisuus on käsiteltävän tiedon suojaustason huomioon ottaen riittävä.
8) Suunnittelu- ja ylläpito-organisaation kanssa on sovittu rakennuksen turvallisuusdokumentaation luottamuksellisuudesta. (Katakri, 2015)

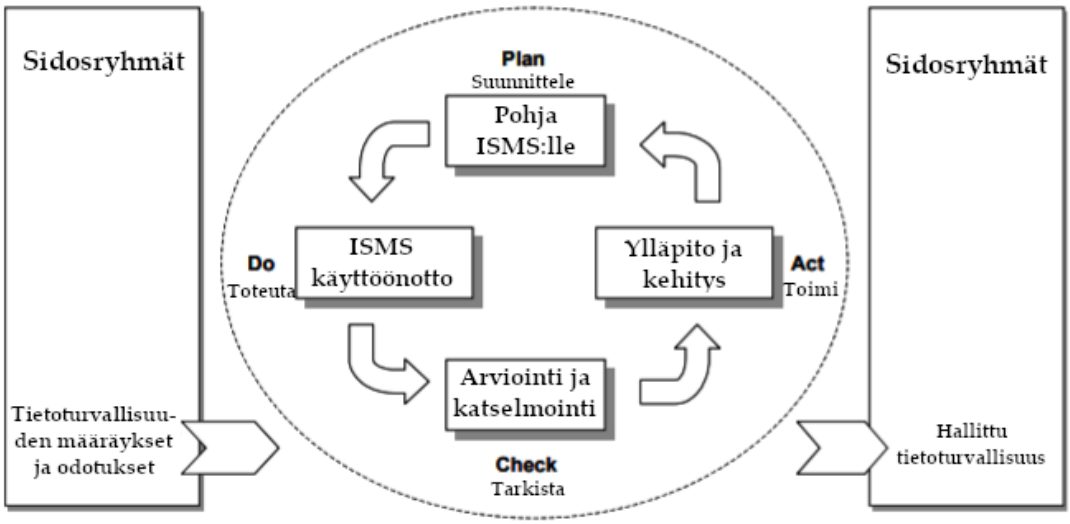
Viimeisenä kokonaisuutena Katakri (2015) käsittelee teknistä tietoturvallisuutta. Tutkijan mielestä tämä osa-alue on ulkoisille kyberturvallisuuden riskeille otollisin osumapiste. Kuten kahdessa aikaisemmassakin kokonaisuudessa, myös teknisen tietoturvallisuuden osuus esittelee esimerkkejä toteutustavoista. Tek-

nisen tietoturvallisuuden osa-alue myös täydentää aikaisempia osa-alueita fyysisen tiedon säilyttämisestä. Teknisen tietoturvallisuuden kokonaisuus pyrkii varmistamaan salassa pidettävän tiedon sähköisen käyttöympäristön turvallisuuden. Katakri (2015) jakaa vaatimukset useampaan osa-alueeseen, joita ovat tietoliikenne-, tietojärjestelmä-, tietoaineisto-, ja käyttöturvallisuus. Jokainen osa-alue pitää sisällään vaatimukset, toteutusesimerkit ja muut lisätiedot, kuten viittaukset ISO 27001 -standardiin. Teknisen tietoturvallisuuden tarkoituksenmukaisuus nojaa organisaation riskienarvioinnin pohjalta tehtävään tulkintaan vaatimuksista. Teknisen tietoturvallisuuden kokonaisuus ei ota kantaa huippusalaiseen aineistoon (ST I), vaan ainoastaan suojaustasojen II-IV vaatimuksiin. (Katakri, 2015)

Katakria voidaan käyttää myös yleisesti organisaation tietoturvan suojaamisen työkaluna, vaikka se on alun perin tarkoitettu viranomaisen auditointityökaluksi. Koska dokumentti on julkisesti saatavilla, voidaan sitä hyödyntää myös silloin, kun organisaation tarkoituksena ei ole hakea Katakrin mukaista luokitusta viranomaiselta, vaan suojata omaa arkaluontoista tietoaan.

4.3 ISO 27001 -standardi

ISO 27001 -standardi on International Organization of Standardizationin (*ISO*) ohjeistus ISMS:n (*Information Security Management Systems*), eli informaatioturvallisuuden hallintajärjestelmän, implementointiin organisaatiossa. Ohjeistuksen avulla pyritään rakentamaan järjestelmä, joka kykenee suojaamaan organisaation tietoa sekä kyberympäristöä. Standardi ajaa organisaation tilaan, jossa se suunnittelee, toteuttaa, ylläpitää ja kehittää keinoja uhkien hallintaan. ISO 27001:n ajatuksena on, että organisaatiosta tulee ennakoiva eikä reagoiva. Tällöin kaikki pyritään suunnittelemaan etukäteen ja riskien toteutumiseen voidaan varautua ennen kuin ne oikeasti toteutuvat. Standardia noudattamalla organisaatio voi myös todeta, että sillä on nykyaikaiset ja tehokkaat prosessit riskeihin varautumiseen. ISO 27001 pohjautuukin ennakoivaan malliin, jota kutsutaan Plan-Do-Check-Act -malliksi. (ISO 27001, 2005) Kuten aikaisemmin riskienhallintaa käsitellessä, tämäkin malli on iteratiivinen kokonaisuus, joka ei tule koskaan päätökseen, vaan käy läpi useita pisteitä, jotka parantavat käytettyjä prosesseja entisestään. ISO 27001 (2005) esittelee ISMS-kehitykseen tähtäävän mallinsa iteratiivisena, jatkuvasti kehittyvänä pakettina, jossa keskiössä on neljä kohtaa. Plan-Do-Check-Act (*PDCA*) -mallia (kuvio 7) noudattamalla organisaatio pystyy rakentamaan hyvän tietoturvallisuuden hallintajärjestelmän, joka on aina ajan tasalla.



KUVIO 7 PDCA-malli (ISO 27001, 2005 mukaillen)

Ensimmäisessä suunnitteluvaiheessa organisaatio perustaa hallintajärjestelmän. Tämä tarkoittaa sitä, että organisaatio määrittelee järjestelmän politiikan, tavoitteet, prosessit ja toimintatavat, jotka ovat jollain tavalla relevantteja riskienhallintaan ja tietoturvallisuuden parantamiseen liittyen. Järjestelmän osien tarkoitus on yhdessä organisaation omien käytäntöjen ja tavoitteiden kanssa tuoda tulosta tiedon suojaamisessa. Toisessa vaiheessa organisaatio tekee, eli implementoi ja operoi ISMS politiikkoja, ohjaimia, prosesseja ja toimintatapoja. Kolmannessa vaiheessa käydään läpi ensimmäinen arviointi. Arvioinnissa keskitytään siihen, miten prosessin tehokkuus rinnastuu tietoturvallisuuden hallintajärjestelmään. Tässä vaiheessa on erittäin tärkeää dokumentoida kaikki havainnot ja raportoida kaikki havainnot eteenpäin. Arvioinnin aikana katselmoidaan kaikki dokumentit ISMS:n liittyen. Viimeisessä iteratiivisessa vaiheessa toimitaan havaintojen ja järjestelmän pohjalta. Tarkoitus on tehdä korjaavia sekä ennakoivia liikkeitä, joiden avulla ISMS-kokonaisuutta voidaan parantaa. Tämän viimeisen vaiheen jälkeen polku alkaa alusta ja korjausliikkeiden jälkeinen ISMS aloittaa elämänsä kyseisellä polulla. PDCA-mallin ympärillä pyörii lisäksi sidosryhmien odotuksia, jotka vaikuttavat omalta osaltaan mallin lopputulokseen ja näkevät myös tietoturvallisuuden hallitun kokonaisuuden (ISO 27001, 2005). Huomionarvoista kuitenkin on, että vaikka PDCA-malli on uusimmasta standardin iteraatiosta poistettu, se vaikuttaa selkeästi edelleen standardin taustalla.

4.4 Toimintaympäristö ja kyberrikollisuus

Voidakseen ryhtyä toimiin kyberympäristön suojaamiseksi, organisaation tulee tuntea oma toimintaympäristönsä, siihen liittyvät riskitekijät ja toimintaympäristöä muovaavat tekijät. Tässä luvussa käydään läpi toimintaympäristön vai-

kutusta organisaation kohtaamiin riskeihin sekä kyberrikollisten motiiveja ja hyökkäystapoja. Näkökulmaksi tutkimuksessa valikoituivat ulkoiset riskit ja niiden arviointi, joten luvussa ei oteta kantaa sisäisiin riskeihin.

Porterin (1980) mukaan toimintaympäristö on se alue, jolla organisaatio toimii ja kilpailee muiden organisaatioiden kanssa. Se, millaista kilpailu on ja millaisia strategioita organisaatioilla on, riippuu täysin toimintaympäristön rakenteesta. Kilpailuedun saavuttamiseksi organisaatio havainnoi muuttujia toimintaympäristössään ja pyrkii vastaamaan toimintaympäristöä muovaaviin tarpeisiin. Toimintaympäristön ollessa jatkuvassa muutoksessa, tulee organisaation sopeutua muuttuvaan tilaan. Esimerkiksi sovellukset tai palvelut saattavat uuden teknologian myötä lakata olemasta kokonaan (Kotler & Keller, 2006).

Finanssialan organisaatio herättää kiinnostusta kybertilassa ja toimintaympäristössään jo sen takia, että yleensä alalla toimivissa organisaatioissa liikkuu paljon rahaa ja raha on motiivina epäilyttäville toimille todella usein, kuten taulukossa 4 voidaan nähdä. Finanssialan organisaatioita ovat mm. pankit, sijoitusrahastoyhtiöt, maksunvälityslaitokset, vakuutusyhtiöt, rahoitusyhtiöt ja arvopaperien välittäjät.

Finanssialan toimintaympäristö on myös kaikkien organisaatioiden tapaan riippuvainen yhä enemmän informaatioteknologiasta (Lindström, 2012). Tämä riippuvuussuhde aiheuttaa sen, että tietoturvallisuuteen ja kybertilan suojaamiseen tulee paneutua vuosi vuodelta enemmän. Lindström (2012) listaa viisi syytä, miksi päättäjien pitäisi välittää kyberturvallisuudesta. Myös Turvallisuuskomitea (2015) on Lindströmin kanssa samoilla linjoilla. Nämä samat tekijät ovat myös sellaisia kyberturvallisuuden haasteita, jotka yleisesti vaikuttavat informaatio- ja viestintäteknologiaa (*ICT*) käyttäviin organisaatioihin:

1. Internetin käyttäjien määrä on jatkuvasti kasvussa ja kybertila on, kuten aikaisemmin luvussa 2.4 todettu, jopa pelottava asia uusille käyttäjille ympäri maailman. Esimerkiksi vuonna 2000 käyttäjiä oli 361 miljoonaa, kun taas vuoden 2011 loppuun mennessä käyttäjiä oli jo 2,27 miljardia. Käyttäjät eivät myöskään tunne kybertilaa ja siihen liittyviä riskejä niin hyvin kuin pitäisi, sillä suurin osa uusista käyttäjistä tulee kehittyvistä maista.
2. Yhä useampi sovellus ulottaa itsensä internetiin tietämättömien käyttäjien keskuuteen ja sovellusten määrä kasvaa jatkuvasti tasaiseen tahtiin. Sovellusten määrän mukana kasvaa myös niiden käyttäjien määrä, jotka luottavat verkkokauppoihin ja -pankkeihin liittyviin sovelluksiin. Verkossa tehtävien ostosten ja rahan liikkumisen myötä myös rikollisuus lisääntyy verkossa ja kyberrikolliset etsivät uusia tapoja ansaita rahaa. Lindströmin (2012) mukaan kyberrikollisuus vastaa rahalliselta arvoltaan maailmanlaajuista huumekauppaa.
3. Kriittinen infrastruktuuri on kehityksen mukana aina vain haavoittuvampi kyberhyökkäyksille. Monet vanhat järjes-

telmät suunniteltiin aluksi irrallisiksi palikoiksi, jotka eivät olleet mukana lähiverkossa tai internetissä, mutta ajan myötä vanhatkin järjestelmät ovat tulleet osaksi kybertilaa. Tästä seuraa se, että nämä järjestelmät ovat avoinna erilaisille haittaohjelmille ja hakkeroinnille. Jälleen yksi hyvä syy organisaatiolle keskittyä kybertilan suojaamiseen.

4. Haitalliset toiminnot kybertilassa muuttuvat hienostuneemmiksi ja helpommiksi käyttää. Haitallisten toimijoiden ei tarvitse enää olla asiantuntijoita, vaan he voivat ostaa rikokset tai niihin tarvittavat valmiit työkalut (*Crime-as-a-service, CaaS).* Esimerkiksi Lindström (2012) mainitsee Zeus-työkalut, joiden hinta on alle 1000 dollaria.
5. Harrastelijahakkerit (*engl. script kiddies*), haktivistit (*internetissä toimivat aktivistit, jotka tuovat esiin omaa propagandaansa*) ja bottiverkkoja rakentavat toimijat ovat vain osa niistä useasta erilaisesta ryhmästä tai yksilöstä, jotka pyrkivät käyttämään kybertilaa epäilyttäviin tarkoituksiin, rahan ansaitsemiseen ja oman asiansa ajamiseen. Kybertilan epäilyttävät toimijat on listattu motiiveineen ja hyökkäystapoineen taulukossa 4. (Lindström, 2012)

TAULUKKO 4 Kyberrikollisuuden toimijat (Lindström, 2012 mukaillen)

Ryhmä	**Motivaatio**	**Hyökkäystapa**
Harrastelijahakkerit	Uteliaisuus / maine	Valmiiksi tarjolla olevat sovellukset
Hakkerit	Haasteet ja taloudellinen hyöty	Automaattiset työkalut, mahdolliset koordinoidut hyökkäykset
Sisäpiiritoimijat	Kosto / kiristäminen	Useita mahdollisuuksia
Haktivistit	Propaganda, omien aatteiden ajaminen	Sama kuin harrastelijahakkereilla ja hakkereilla
Rikolliset toimijat	Taloudellinen hyöty	Kalastelu, sosiaalinen manipulointi, spämmi, haittaohjelmat
Bottiverkkojen operaattorit	Taloudellinen hyöty ja palveluiden estäminen	Etäohjattavat bottiverkot
Terroristit	Propaganda, palveluiden estäminen, vahingon aiheuttaminen	Useita eri mahdollisuuksia mukaan lukien kriittiseen infrastruktuuriin kohdistuvat hyökkäykset
Valtiolliset toimijat	Palveluiden estäminen, vahingon aiheuttaminen, vakoilu, tiedonkeruu	Useita mahdollisuuksia

Turvallisuuskomitea (2015) sekä Turvallisuus- ja puolustusasiainkomitean sihteeristö (2013) huomauttavat, että Suomen kybertila ei ole rajattu ainoastaan Suomeen, vaan se on osa koko maailman globaalia kybertilaa, johon on pääsy

kaikkialta. Tämän takia organisaatioihin kohdistuvia riskejä tulee tarkastella Suomea laajemmassa mittakaavassa ja pyrkiä ymmärtämään niitä mahdollisuuksia, joita globaalisti toimivilla haitallisilla toimijoilla on. Turvallisuuskomitea (2015) listaa haasteita, joiden hoitamiseen organisaatioiden tulee keskittyä omassa kybertilassaan.

Nyky-yhteiskunta on digitalisoitunut todella nopeasti ja yhteiskunnan toiminnot ovat riippuvaisia tietoteknisistä toteutuksista. Digitalisaation edetessä myös kybertilaan kohdistuvat riskit muuttuvat vaikutuksiltaan yhä vaarallisemmiksi ja hyökkäyksien tarkoitukset monipuolistuvat. Digitalisaation lisäksi globaalissa kybertilassa vaikuttavat myös niin suurvaltojen kuin pienempienkin valtioiden voimasuhteet ja arvojärjestelmät, jotka ovat jatkuvassa murroksessa. Kaikki tämä vaikuttaa yksittäiseen organisaatioon, jonka toimintaympäristö on globaalissa tietoverkossa. Turvallisuuskomitea (2015) arvioi, että kyberrikollisuuden määrä lisääntyy samalla, kun rikollisten pakoilutavat kehittyvät. Tämä tarkoittaa, että kyberrikollisilla on tulevaisuudessa enemmän keinoja rikosten tekemiseen, mutta samalla myös enemmän keinoja suojautua virkavallalta. (Turvallisuuskomitea, 2015)

Edellä luetellut rikolliset toimet ovat ulkoisia riskejä, joihin organisaatio ei voi sinällään vaikuttaa suoraan. Vaikutusmahdollisuudet rajautuvat organisaation omaan varautumiseen riskienhallinnan kautta. Organisaation tulee selvittää, miten se reagoi riskeihin ja miten se pyrkii nollaamaan riskien vaikutuksen.

5 Tutkimusmenetelmät

Tässä luvussa käydään läpi tutkimuksen eteneminen aina kirjoitusprosessin alusta tutkielman palautukseen asti. Luvussa kuvataan, miten tutkimusprosessin suunnittelu ja toteutus tehtiin. Prosessin lisäksi luvussa kuvataan tutkimuksen tekemiseen käytetyt työkalut sekä mahdolliset ongelmat, joita tutkimuksen aikana ilmeni.

5.1 Tutkimusprosessi

Tutkimuksen suunnittelu aloitettiin graduseminaarin yhteydessä loppuvuodesta 2018. Tutkimuskysymys tarkentui matkan varrella useampaan otteeseen ja ensimmäinen kysymys sekä tutkimusongelma olivatkin aluksi suuntaa antavia. Tutkimuksen aiheen laajuuden takia olikin tärkeää, että tutkimus rajattaisiin mahdollisimman tarkasti koskemaan ainoastaan kyberturvallisuuden ja tietoturvallisuuden ulkoisia riskejä. Myös positiiviset riskit, jotka ovat mahdollisia, rajattiin tutkimuksen ulkopuolelle, sillä tutkimuksen tarkoituksena oli luoda pohja organisaation kyberturvallisuuden riskienhallinnan kehitystyölle. Toimeksiantaja toivoi, että riskejä käsiteltäisiin tutkimuksessa nimenomaan ulkoisina uhkina ja näistä syntyvinä riskeinä.

Lähdeaineistoa tallennettiin tutkijan tietokoneelle sekä useampaan pilvipalveluun (Google Drive ja Microsoft OneDrive), jotta ne eivät missään vaiheessa pääsisi katoamaan tutkimuksen aikana. Myös tutkimus itsessään tallennettiin useammalle kovalevylle sekä pilveen siltä varalta, että jokin laite hajoaisi. Tutkimus sekä lähteet olivat koko tutkimuksen ajan saatavilla pilvestä uusimmassa versiossa käytetystä laitteesta riippumatta.

Tutkimuksen aikataulua seurattiin yhdessä ohjaajan kanssa. Gradun valmistuttua materiaalit tuhottiin sillä oletuksella, että itse tutkimusraportti tuo esille tärkeimmät kohdat ja raporttia voidaan käyttää jatkotutkimusten pohjana, jolloin pilveen tallennettu tutkimusmateriaali on turhaa dataa.

Tutkimuksen dokumentointi tapahtui tallentamalla väliversioita tutkimuksesta ja kommentoimalla niitä suoraan PDF-tiedostoon, joka sisälsi sen hetkisen tutkimusvaiheen. Myös nämä väliversiot tallennettiin useampaan pilvipalveluun. Microsoftin OneDrive valittiin tutkimuksen pääasialliseksi säilytyspaikaksi tutkijan aikaisempien hyvien kokemusten takia sekä siitä syystä, että tutkimuksen kirjoittamiseen käytetty Microsoft Word osaa tallentaa tekstin pilveen reaaliaikaisesti, jolloin ei tarvinnut pelätä, että tietokoneen hajoaminen hävittäisi tiedon. Microsoft Word valikoitui kirjoitusalustaksi, koska tutkijalla oli jo vankka osaaminen ohjelman käytöstä ja aikaisemmin vaihtoehtoisella LaTeX-ohjelmalla kirjoitettujen töiden ohjelmasta johtuvaan ongelmanratkomiseen kului liikaa aikaa. Google Drivesta oli myös aikaisempia hyviä kokemuksia ja se valittiin tutkimuksen varmuuskopiointia varten siltä varalta, että primääri tallennusalusta olisi poissa käytöstä.

Tutkimusasetelma, tutkimusmenetelmä ja tutkimusstrategia muotoutuivat kirjallisuuskatsauksen edetessä tarkemmiksi ja tutkimuksesta pystyttiin yksilöimään selkeitä piirteitä ajan kuluessa. Tutkimuksen lopullinen tavoite oli kvalitatiivisen tapaustutkimuksen yksi tunnusmerkeistä – tutkittavan ilmiön syvällisen ymmärryksen kautta tehty tulkinta, jonka lopputuloksena on entistä syvempi ymmärrys ilmiön luonteesta ja tämän uuden ymmärryksen avulla tuotettu uusi tulkinta ilmiöstä.

Tutkimus noudatti perinteistä, Eisenhardtin (1989) tapaustutkimuksen mallia teorian rakentamiseen, jossa on kahdeksan askelta ja jokaiseen askeleeseen on määritelty toiminnot sekä syyt näille toiminnoille (Taulukko 5). Tutkimuksen ollessa laadullinen, ei perinteisen mallista hypoteesia muodostettu tutkimuksen aluksi.

TAULUKKO 5 Tapaustutkimuksen teoria (Eisenhardt, 1989 mukaillen)

Askel	**Toiminto**	**Syy**
Aloitus	Tutkimuskysymysten määrittely	Suuntaa voimavarat ja tarjoaa pohjan
Tapauksen valinta	Ennalta määritelty, teoriaan nojaava otanta	Rajaa vaihtelua Keskittää voimavarat hyödyllisiin tapauksiin
Mittareiden ja käytänteiden määrittely	Aineistonkeruumenetelmät	Vahvistaa teoriapohjaa
Kentälle siirtyminen	Päällekkäistä aineiston keräämistä sekä analyysia Joustavia aineistonkeräysmenetelmiä	Nopeuttaa analyysia ja auttaa säätämään aineistonkeruumenetelmiä
Datan analysointi	Within-case analyysi Cross-case analyysi	Tuo datan ja ensisijaisen teorian tutuksi Pakottaa tarkastelemaan ilmiötä monelta eri suunnalta
Hypoteesin muodostaminen	Rakenteiden iteratiivista taulukointia Vastaa kysymykseen ”miksi” suhteiden takana	Vahvistaa, laajentaa sekä selkiyttää teoriaa
Kirjallisuuden käsittely	Ristiriitaisen sekä samanhenkisen kirjallisuuden käsittely	Sisäinen validiteetti vahvistuu Selkeyttää yleistettävyyttä
Ratkaisun saavuttaminen	Teoreettinen saturaatio, kun mahdollista	Päättää prosessin, kun marginaalinen parantuminen on vähäistä

5.2 Kvalitatiivinen tutkimusmenetelmä

Kvalitatiivinen (*engl. qualitative*), eli laadullinen tutkimusmenetelmä on toinen kahdesta yleisimmästä tutkimusmenetelmästä. Toinen yleinen menetelmä on kvantitatiivinen, eli määrällinen tutkimusmenetelmä. Tutkimusmenetelmä valikoituu sen mukaan, miten tutkimusprosessi etenee. Tieteellinen ajattelu on Staken (2010) mukaan aina yhdistelyä näistä kahdesta menetelmästä, mutta ero näiden kahden menetelmän välillä on selvä. Tästä syystä täytyy aina valita jompikumpi päämenetelmäksi (Metsämuuronen, 2008).

Hirsijärven & Huttusen (1995) mukaan kvalitatiivinen menetelmäsuuntaus pyrkii ymmärtämään tutkittavaa ilmiötä tarkemmin. Tutkimusmenetelmä selvittää ilmiön merkityksen tai tarkoituksen ja luo kokonaisvaltaisen ja syvemmän käsityksen ilmiöstä. Kvalitatiivinen tutkimus myös antaa tilaa tutkittavien henkilöiden omille kokemuksille, näkökulmille, ajatuksille ja tunteille tutkittavan ilmiön ympärillä (Hirsijärvi & Huttunen, 1995). Kvalitatiivisessa menetelmässä muuttujat ilmaistaan sanallisesti toisin kuin kvantitatiivisessa

menetelmässä ja tutkimus pohjautuu ihmisten havaintoihin ja kokemuksiin (Hirsijärvi & Huttunen, 1995; Stake, 2010).

Laadullisessa tutkimuksessa tutkittavia yksilöitä ei tule valita liian montaa ja valitut yksilöt tutkitaan perusteellisesti, jolloin määrää tärkeämpää on aineiston laatu. Aineiston määrä toki nojaa siihen, millaista analyysia ja tulkintaa aineistosta pyritään tekemään. Tästä syystä aineisto yleensä valitaankin teoriaan nojaten ja tarkoituksenmukaisesti. (Eskola & Suoranta, 1998)

DiCicco-Bloom & Crabtreen (2006) mukaan yleisesti käytettyjä tiedonkeruumenetelmiä kvalitatiivisessa tutkimuksessa ovat mm. haastattelut, jotka voidaan jakaa esimerkiksi strukturoituihin, semi-strukturoituihin ja strukturoimattomiin haastatteluihin (DiCicco-Bloom & Crabtree, 2006). Vaikka määritelmiä on useita, riippuen lähdekirjallisuudesta, tämä on hyväksi havaittu jako. Strukturoidut haastattelut tuottavat kuitenkin yleensä kvantitatiivista dataa (DiCicco-Bloom & Crabtree, 2006), joten kyseistä mallia ei käytetä tässä tutkimuksessa. Strukturoimattomaan haastatteluun valitut kohteet valitaan heidän roolinsa mukaan ja valintaan vaikuttavat myös heidän kykynsä toimia tutkijan tulkkina, mentorina ja opettajana haastattelun aikana, joka tapahtuu jokapäiväisten toimien lomassa. Semi-strukturoitu haastattelu taas on usein tutkimuksen ainut aineisto, joka kerätään sovittuna ajankohtana jokapäiväisten toimintojen ulkopuolella ja haastattelu rakentuu osittain ennaltamääritetyn kaavan mukaisesti kysymysten ympärille, joita tutkija esittää haastateltavalle. Haastattelun aikana voidaan kuitenkin keskustella myös kysymysten ulkopuolisista asioista, joita saattaa tulla mieleen (DiCicco-Bloom & Crabtree, 2006). Tästä syystä tutkimuksen haastattelutavaksi valikoituikin semi-strukturoitu haastattelutapa, josta kerättiin kokonaisuudessaan tutkimuksessa käytettävä data. Kvalitatiivinen tutkimus valittiin myös sen takia, että tapauksesta ei ole saatavilla kvantitatiivista dataa, koska data ja tietämys ovat vain haastateltavien henkilöiden päässä. Tutkimalla olemassa olevaa kirjallisuutta ja haastattelemalla organisaation edustajia päädyttiin malliin, joka kehittyi tutkimuksen edetessä.

5.3 Tapaustutkimus

Tutkimuksen tarkoitus oli luoda pohja toimeksiantajan kyberturvallisuuden riskienhallinnan kehitystyölle ja tutkielman lopputuotokseksi valittiin yleistettävissä olevan mallin luominen sen pohjalta, millaista kyberturvallisuuden riskienhallinta on organisaatiossa tällä hetkellä ja miten se suhteutuu aikaisemmin luotuihin riskienhallinnan ja riskien arvioinnin standardeihin. Tästä syystä tutkimus on käytäntöön suuntautunut tutkimus, jonka tutkimusasetelmaksi valittiin yleistävä (*generalisoiva*) tutkimusasetelma. Niiniluodon (1997) näkemyksen mukaan yleistävä tutkimusasetelma kartoittaa järjestelmää koskevat säännönmukaisuudet. Näiden säännönmukaisuuksien pohjalta voidaan tehdä ennustuksia ja voidaan löytää tai jopa parantaa tavoitetilaan johtavia keinoja. Tutkimus itsessään ei pyri ennustamaan tulevaa, vaan pyrkii luomaan sellaisen mal-

lin, jonka avulla tulevaisuudessa on helpompi tehdä johtopäätöksiä menneisyyden perusteella. Säännönmukaisuus (*engl. regularity*) tarkoittaa Krimsleyn (1995) mukaan, että ilmiö esiintyy aina, kun jotkin tietyt ehdot täyttyvät. Toisena vaihtoehtona Niiniluodon (1997) mukaan oleva kuvaileva (*deskriptiivinen*) asetelma jätettiin pois, koska se pyrkii ainoastaan tarkastelemaan tutkimuksen kohteen nykyistä tilaa ja historiaa sekä Heikkilän (2014) mukaan vaatii laajan aineiston, jota ei tällaisessa pieneen organisaatioon kohdistuvassa tapaustutkimuksessa ole mahdollista kerätä. Lisäksi deskriptiivinen ote on enemmän kvantitatiivisen tutkimuksen empiriaa tukeva tutkimusasetelma (Heikkilä, 2014).

Yksi kvalitatiivisen tutkimusmenetelmän yleisimpiä tutkimusstrategioita on tapaustutkimus (*engl. case study*) (Darke, Shanks & Broadbent, 1998). Tapaustutkimuksessa pyritään laajan, edustavan aineiston ja tilastollisen tutkimuksen sijaan keskittymään ainoastaan muutamiin tapauksiin tai yhteen tapaukseen perusteellisesti, eri puolilta tarkastellen. Perusteellinen tarkastelu on tärkeää, koska tapaustutkimuksen tarkoitus ei ole löytää tyypillisiä piirteitä tai syyseuraussuhteita. Tapaustutkimuksen tarkoitus on kuvailla ilmiötä ja tehdä ilmiöstä uusia havaintoja sekä vastata kysymyksiin, kuinka ja miksi. (Colorado State University, 2019; Gillham, 2010; Yin, 2003)

Tapauksen terminologinen määrittely voi olla hankalaa, mutta Gillhamin (2010) mukaan se on ihmisten toimintojen kokonaisuus, jota voi tutkia, ymmärtää sekä käsitellä vain kontekstissaan, missä sille on hankala määritellä tarkat rajat. Hankalan tapauksen määrittelystä tekee se, että tapaus voi olla mitä vain, kuten yksilö, ryhmä, osasto tai kuten nyt, riskienhallinta (Metsämuuronen, 2008).

5.4 Aineiston keruu ja analysointi

Aineiston keräämistä varten luotiin semi-strukturoitu haastattelurunko (liite 1), jossa kysymykset olivat mahdollisimman avoimia, jotta haastateltavien henkilöiden omat ajatukset pääsisivät esiin. Kysymyksiä, joihin oli mahdollista vastata lyhyesti, vältettiin mahdollisimman paljon. Tarkoituksena oli, että haastateltava henkilö vastaisi kysymykseen kuvailevasti ja mahdollisimman laajasti. Tällöin aineistosta tuli riittävän laadukas ja sitä voitiin hyödyntää tutkimusongelmaan vastaamisessa. Empiirinen aineisto kerättiin vuoden 2019 ensimmäisellä kvartaalilla ja haastattelut järjestettiin haastateltavien henkilöiden aikataulujen puitteissa, tutkijan valitsemassa paikassa yksittäishaastatteluina. Tutkimuksen hyväksymisen jälkeen haastattelumateriaali tuhottiin kaikista tallennuskohteista.

Aineiston analysoinnin helpottamiseksi kaikki haastattelut nauhoitettiin ja tärkeimmistä kohdista tehtiin muistiinpanot haastattelun aikana. Nauhoitetut haastattelut litteroitiin, eli kirjoitettiin puhtaaksi luettavaan muotoon. Tutkimuksen luonteen takia todettiin, että peruslitterointi riittää, jolloin enimmät täytesanat suodatettiin tekstistä pois. Yhteiskuntatieteellinen tietoarkisto (2019) määrittelee peruslitteroinnin seuraavasti:

> ”Puhe litteroidaan sanatarkasti puhekieltä noudattaen, mutta siitä jätetään pois täytesanat (esim. tota, niinku), toistot, keskenjäävät tavut ja yksittäiset äännähdykset. Myös selvästi kontekstiin liittymätön puhe voidaan harkitusti jättää litteroimatta. Puheen lisäksi litteroidaan merkitykselliset tunneilmaisut (esim. nauru, liikuttuminen, tms.).”

Puhtaaksikirjoitettu aineisto käsiteltiin, jaettiin haastattelurungon mukaisesti ja hyväksytettiin vielä erikseen haastatelluilla henkilöillä siltä varalta, että joitain asioita ei saisi julkaista tutkimuksessa tai heillä olisi jotain lisättävää vastauksiinsa. Kommenttikierroksen jälkeen materiaaliin ei tehty muutoksia. Haastateltavat olivat tyytyväisiä ulosantiinsa ja totesivat, että ovat sanoneet kaiken oleellisen omasta näkökulmastaan. Aineiston analyysi suoritettiin haastattelurungon mukaisissa teemoissa, joita olivat taustatieto, tietoturvallisuus, riskikategoriat ja prosessi. Analyysin aikana haastatteluista pyrittiin paikantamaan samankaltaisuudet, eroavaisuudet sekä hyvät ja huonot puolet, joita haastateltavat toivat esiin. Haastattelut myös koodattiin niin, että pääkohdat jäisivät selkeästi muistiin. Näiden pohjalta alettiin työstää ehdotusta organisaation riskien arvioinnin malliksi.

5.5 Tutkimuksen tapaus: Finanssiyritys Oy

Tutkimuksen tarkoituksena oli selvittää Finanssiyritys Oy:n (nimi muutettu) riskienhallinnan mallia ja luoda paranneltu malli ulkoisten kyberturvallisuuden riskien arviointiin. Organisaatiossa koettiin, että riskien arviointi ei sellaisenaan ollut riittävän tieteellinen ja tarkka prosessi, vaan arviointi perustui liikaa omaan kokemukseen, intuitioon ja niin sanottuun Harrisonin–Stetsonin menetelmään, valistuneeseen arvaukseen. Kuten kirjallisuusosiossakin mainittiin, on riskien arviointi saanut kritiikkiä myös tutkijoilta juuri samasta syystä ja esimerkiksi Baskerville (1991) toteaa, että riskienhallinta ei ole tieteellinen menettelytapa. Omien kokemusten, intuition ja valistuneen arvauksen vaikuttavuutta Finanssiyritys Oy:n arviointiprosessissa haluttiin pienentää.

Finanssiyritys Oy:n suunnitelmissa oli aloittaa kyberturvallisuuden riskienhallinnan kehitystyö vuoden 2019 aikana. Tätä kehitystyötä varten ulkoisten kyberturvallisuuden riskien todennäköisyyksien arvioinnin tueksi haluttiin luoda malli, joka helpottaisi riskien arviointia ja toisi siihen vankemman, tietoon perustuvan pohjan. Riskienhallinta tutkittavassa organisaatiossa on tärkeä osa-alue organisaation menestyksessä finanssialalla ja tämä johtaa siihen, että mitä varmemmin riskien vaikutus sekä todennäköisyys arvioidaan, sitä paremmin organisaation toiminta finanssialalla turvataan.

Finanssiyritys Oy:n riskienhallinnassa ovat vahvimmin mukana tietosuojajohtaja sekä compliance-osaston toimijat. Heidän työnsä lisäksi emoyhtiöltä tulee tavoitetila, johon organisaation tulisi pyrkiä riskien vaikutusten lieventämisessä tai poistamisessa. Tavoitetila perustuu emoyhtiön suorittamaan arvi-

oon siitä, millaisella tasolla organisaation riskien todennäköisyys ja vaikuttavuus voisi parhaassa tapauksessa olla.

Haastateltavat henkilöt sekä haastatteluissa esiin tulleet yritykset on anonymisoitu. Kokonaisuutena puhutaan konsernista, joka silloin tarkoittaa emoyhtiötä ja tämän alla toimivia yksikköjä, kuten haastateltujen edustama Finanssiyritys Oy. Finanssiyritys Oy on finanssialan toimija, joka vastaa verkkomaksujen välittämisestä verkkokauppojen ja kuluttajien välillä. Organisaation asiakkaita ovat verkkokauppiaat ja heidän kauttaan kuluttajat. Organisaatio toimii Suomen Finanssivalvonnan tarkkailevan silmän alla ja sitä koskevat samat säädökset kuin pankkejakin. Finanssiyritys Oy työllisti tutkimushetkellä noin 55 henkilöä ja se on ison, pääasiassa pohjoismaissa, mutta myös Euroopassa vaikuttavan, konsernin tytäryhtiö.

Finanssiyritys Oy seuraa pääpiirteittäin tässäkin tutkimuksessa käsiteltyjä riskienhallinnan malleja sekä hyödyntää esiteltyjä työkaluja. Olemassa olevista malleista sekä työkaluista on otettu käyttöön ne osat, jotka organisaatio kokee soveltuviksi omaan ympäristöönsä ja kokoonsa.

Finanssiyritys Oy:stä valikoitiin haastateltavaksi henkilöt, jotka työskentelevät riskienhallinnan parissa (taulukko 6). Haastatelluista A ja B toimivat organisaatiossa yleisen riskienhallinnan parissa. A on organisaation riskienhallinnan vastuuhenkilö, B tekee usein omien sanojensa mukaan raakatyön, eli riskien kirjaamisen ja dokumentoinnin ennen ensimmäistä katselmointia ja C on organisaatiossa teknisen tietoturvallisuuden asiantuntija ja tietoturvavastaava, joka toimii riskienhallinnassa A:n ja B:n tukena. C vastaa myös organisaation tietosuojasta sekä on vastuussa siitä, että organisaatio on tietoturvallinen paikka ja tietoturvadokumentaatio on oikeellinen sekä ajantasainen. C on lisäksi vastuussa emoyhtiölle siitä, että emoyhtiön määräämät auditoinnit ja muut tietoturvatoimenpiteet hoituvat. A ja B kuljettavat tietoturvallisuuteen liittyviä asioita mukana organisaation riskimatriisissa ja pitävät huolen, että C:n esittämät asiat päätyvät sinne, sekä tukevat C:tä hänen työssään tietoturvallisuuden, tietosuojan ja kyberturvallisuuden parissa. C on kyberturvallisuuden osalta organisaation asiantuntija.

TAULUKKO 6 Haastatellut henkilöt ja heidän roolinsa

Haastateltava A	Yleisen riskienhallinnan vastuuhenkilö	On vastuussa riskienhallinnasta emoyhtiön suuntaan ja omistaa Finanssiyritys Oy:n riskit. Tekee riskiarviot yhdessä B:n kanssa.
Haastateltava B	Yleisen riskienhallinnan ammattilainen	Kirjaa ja dokumentoi tunnistetut riskit sekä hoitaa riskimatriisia. Tekee riskiarviot yhdessä A:n kanssa.
Haastateltava C	Tietosuojan sekä tieto- ja kyberturvallisuuden asiantuntija	Vastuussa tieto- ja kyberturvallisuuden riskien arvioinnista sekä tietoturvadokumentaation oikeellisuudesta. Varmistaa, että emoyhtiön järjestämät auditoinnit hoituvat.

Haastatelluilla on kaikilla oma roolinsa Finanssiyritys Oy:n riskienhallinnassa, mutta riskienhallinta toimii silti yksikkönä sekä yhteistyössä emoyhtiön riskienhallintaelimen kanssa. Finanssiyritys Oy pyrkii osallistamaan koko henkilöstön riskien tunnistamiseen, arviointiin sekä hallintaan siinä määrin, että ajatushautomoita järjestetään säännöllisen epäsäännöllisesti, mutta kuitenkin vähintään noin kahden vuoden välein.

Empiirisessä osiossa tutkimus paneutuu Finanssiyritys Oy:n riskien arvioinnin menetelmiin ja käsittelee riskienhallinnan johtohenkilöiden ajatuksia riskien arvioinnista organisaatiossa. Semi-strukturoitujen haastattelujen pohjalta kerättyä dataa verrattiin olemassa oleviin malleihin ja pyrittiin hahmottamaan sellaisia uusia tai erilaisia tapoja riskien arviointiin, jotka helpottaisivat organisaation kyberturvallisuuden riskien arviointia.

6 Tutkimustulokset

Tämä luku käsittelee tutkimuksen tulokset. Luvussa esitellään tulosten yhteydessä ehdotus ulkoisten kyberturvallisuuden riskien estimoinnin mallista, jota Finanssiyritys Oy voi käyttää osana riskienhallintaansa sekä vastataan tutkimuksen alussa esitettyyn päätutkimuskysymykseen haastattelun pohjalta. Haastattelujen purussa on nostettu esiin ne tekijät, jotka vaikuttivat mallin rakentumiseen, ja haastattelun purku perustelee mallissa esitellyt lisäykset ja tarkennukset IRM:n (2002) riskienhallintamalliin.

Haastattelujen pohjalta esiin nousivat tavoitellusti käytössä olevan riskien arvioinnin mallin ongelmakohdat, joihin organisaatio toivoo parannusta. Pääasiallisena ongelmakohtana Finanssiyritys Oy kokee ulkoisten kyberturvallisuuden riskien todennäköisyyden arvioinnin. Ongelmat paikantuvat siis riskien arviointiprosessissa estimointivaiheeseen. Tästä syystä ehdotettu malli pureutuukin estimaatioon ja nimenomaan todennäköisyyden arvioimiseen, joka on osa estimointiprosessia. Sama ajatus on yleistettävissä myös vaikuttavuuden arviointiin, joka on myös osa estimointia, kuten luvussa 3 käsitellystä IRM:n (2002) riskienhallinnan mallista näkee. Haastattelussa selvisi, että ulkoisten kyberturvallisuuden riskien arviointi organisaatiossa tapahtuu saman mallin mukaisesti kuin minkä tahansa muun riskin arviointi sillä poikkeuksella, että arviointia eivät tee pelkästään yleisen riskienhallinnan ammattilaiset, vaan mukana on Finanssiyritys Oy:n oma tieto- ja kyberturvallisuuden asiantuntija.

> *" - - niinku sanottu, niin meidän kannalta ne on kaikki riskit kategoriasta riippumatta siellä samassa kehikossa. Siitä sitten koostetaan jälleen ihan riippumatta mihin kategoriaan ne on luokiteltu ne sellaset ihan meidän mielestä keskeiset top 10 sanotaan." (haastateltava B)*

Finanssiyritys Oy noudattaa mm. ISO 31000- sekä IRM:n (2002) standardeja riskien arvioinnissaan niiltä osin kuin ne soveltuvat organisaation toimintaympäristöön sekä kokoon. Luvussa 3 avataan näiden standardien riskien arvioinnin malleja tarkemmin. Standardit on toteutettu hyvin, mutta ne koetaan puutteellisiksi riskien estimoinnin ja siihen kuuluvan todennäköisyyden arvi-

oinnin osalta. Tutkimustulosten yhteydessä esitellyssä malliehdotuksessa lisätään olemassa olevaan malliin asioita, jotka oikeassa kohdassa vaikuttavat positiivisesti organisaation ulkoisten riskien arviointiin. Malli on siis yhdistelmä tutkimusdatan perusteella tehtyjä päätelmiä sekä olemassa olevia malleja. Muokkauksen pohjana käytetään luvussa 3.3 esiintyvää IRM:n (2002) riskienhallinnan mallin arviointiosiota.

Haastattelun ensimmäinen osio käsitteli riskien arviointia ohjaavia tekijöitä Finanssiyritys Oy:ssä. Haastattelussa korostuivat tietoturvapolitiikan sekä strategian osuus koko riskienhallintaa ohjaavina tekijöinä ja näin ollen tutkimuksessakin luvussa kaksi esitellyt riskien arviointia ohjaavat tekijät on otettu organisaatiossa huomioon ja ne koetaan tärkeiksi. Tietoturvapolitiikka toimii taustalla ja strategiaa tehtäessä se otetaan huomioon, mutta se ei kuitenkaan ole strategiaan sellaisenaan kirjattu.

> *"Kyllä se on tavallaan siellä meidän liiketoiminnan ytimessä ja lain kautta tulee suoraan se tietoturva. Se on pikemminkin tämmönen strateginen jatkuva asia, minkä on pakko olla kunnossa, että liiketoiminta voi jatkua ja olla olemassa."* (*haastateltava* C)

Finanssiyritys Oy:ssä ollaan sitä mieltä että tieto- ja kyberturvallisuus ovat alalla oletusarvoisen tärkeitä, koska finanssialalla ei tarvita isoja rikkomuksia, että organisaatio menettää maineensa. Tämä voi pahimmillaan johtaa liiketoiminnan loppumiseen. Haastattelussa tuotiin esille kolmen puolustuslinjan malli, joka on kirjattu koko konsernin riskienhallintapolitiikkaan.

> *"Riskienhallintapolitiikassa, joka on tehty sieltä konsernin huipulta, mainitaan kolmen puolustuslinjan malli, jossa me täällä yksikössä muodostetaan se ensimmäinen linja, konsernin riskienhallintayksikkö on se toinen ja riippumaton sisäinen sekä ulkoinen tarkastus se kolmas linja."* (*haastateltava* B)

Finanssiyritys Oy:n nykyinen riskienhallintataulukko keskittyy ylätason riskeihin eikä mene esimerkiksi tarjottujen palveluiden osalta sovellusten tiettyjen pienten palasten aiheuttamiin riskeihin. Riskien tunnistaminen on organisaation oman tietoturvapolitiikan mukaan myös työntekijöiden vastuulla siinä määrin, että riskin tunnistettuaan täytyy siitä ilmoittaa riskienhallinnalle. Tämä tukee myös olemassa olevien mallien näkemystä siitä, että koko organisaatio on omalla tahollaan vastuussa riskien tunnistamisesta. Politiikat asettavat ne askeleet ja työkalut, joita riskien arvioinnin ja riskien käsittelyn prosessissa käytetään. Strategia ja tietoturvapolitiikka johtavat siihen, että ulkoisia riskejä ylipäätään mietitään.

> *"Mä nään lähinnä sen, että meidän firma on sillä tasolla, että noi uhat joudutaan miettimään todellisina. En mä näe, että se vaikuttaa itse siihen prosessiin varsinaisesti mitenkään sillä tasolla, miten se tehdään. Strategia on niin ylätasolla, että sieltä tulee lähinnä se määräys ja mandaatti tehdä se asia ja käyttää siihen aikaa, mutta ei se sen tarkemmin ohjaa." (haastateltava C)*

Politiikat sanellaan ylhäältä emoyhtiön tarpeiden mukaan ja niitä tulee noudattaa omassa liiketoimintayksikössä. Liiketoimintayksikkö ottaa erikseen huomioon Finanssiyritys Oy:n omanlaatuisuuden osana emoyhtiötä omissa dokumenteissaan. Finanssiyritys Oy tekee omaa riskienhallintaa emoyhtiön ohjauksessa ja tälle raportoiden. Tällöin organisaatio itse voi vaikuttaa suoraan riskienhallinnalla omaan erityislaatuiseen tietoturvapolitiikkaansa paikallisesti. Emoyhtiön dokumenteissa vaikuttaminen hoidetaan pidemmän tien kautta, joka kulkee emoyhtiön riskienhallintayksikön läpi ehdotusten muodossa. Emoyhtiön lisäksi ulkoinen ohjaaja on Suomen viranomainen. Viranomainen valvoo, että Finanssiyritys Oy pitää huolen omista velvoitteistaan ja toimii lain mukaan.

> *"Jos tulee joku uus tuote tai palvelu, niin se pitää hyväksyttää viranomaisilla ja siihen viranomaishyväksyntään liittyen tehdään aina sen uuden tuotteen tai palvelun riskiarvio. Käydään hyvinkin tarkalla tasolla, että millasia tapauksia voi käydä ja miten sitä palvelua tai tuotetta voitais hyväksikäyttää rikollisessa mielessä. Kaikki nää pitää yrittää tietysti hahmottaa ja myös viranomainen odottaa meidän sen arvion suorittaneen" (haastateltava A)*

6.1 Ulkoisten kyberturvallisuuden riskien arviointimalli

Tässä tutkimuksessa ehdotetaan IRM:n (2002) mallin estimoinnin pilkkomista pienempiin palasiin. Estimoinnista tunnistettiin haastattelun pohjalta kaksi pienempää kokonaisuutta, jotka ovat riskien todennäköisyys ja riskien vaikuttavuus. Finanssiyritys Oy:ssä nykyinen riskien vaikuttavuuden arviointi pohjautuu luvun 3 taulukossa 2 esitellyn kaltaiseen matriisiin ja se koetaan sellaisenaan toimivaksi, mutta tästäkään ei ole olemassa varsinaista tietoa, että mille pohjalle matriisin merkinnät nojaavat ja mikä malli matriisia tarkalleen ottaen ohjaa taustalla. Riskien todennäköisyyksien arviointi Finanssiyritys Oy:ssä taas on hyvin subjektiivinen prosessi, jossa arvioinnissa näkyvät voimakkaasti arvioijan kokemukset sekä näkemykset.

> *"Täs tietenki täytyy muistaa, et niiden on pakko olla subjektiivisia arvioita, että kukaan ei voi sanoa, oliko se oikein vai väärin. Ja se on pakko hyväksyä se vajavaisuus, mutta kyllä siinä pystyy jonkinlaista todennäköisyysjärjestystä asettamaan riskeille, mutta se tarkka arvio on enimmäkseen sitä subjektiivista arviointia." (haastateltava A)*

Sen lisäksi, että riskien todennäköisyyksien arviointi irrotetaan uudessa mallissa selkeästi omaksi kokonaisuudekseen, malliin lisätään siitä puuttuva tai vajaaksi jäävä aktiivinen ote tiedonhankintaan ja arkistointiin. Ehdotus korostaa nimenomaan aktiivista otetta koko riskienhallintaprosessiin, jota voidaan hyödyntää estimointivaiheessa. Tämä tarkoittaa, että tiedon etsintään ja sen säilö-

miseen käytetään aikaa ja sitä tehdään systemaattisesti oma organisaatio mielessä jokaisessa riskienhallinnan prosessin vaiheessa. Tietoa voi etsiä mediasta, tutkimuksista, kirjallisuudesta, hakukoneista, riskilistoista, sidosryhmistä sekä erilaisin työkaluin, joita tiedonhankintaan erikoistuneet yritykset tarjoavat. Apuna voi ja kannattaakin käyttää myös ulkopuolisia yrityksiä. Tästä prosessista syntyy juuri organisaatiota itseään koskeva tietokokoelma, joka olemassaolollaan tukee kaikkien riskienhallintaan osallistuvien henkilöiden kykyä arvioida riskien todennäköisyyksiä.

> *”Meille ei tuu mitään sellasta informaatiota, minkä avulla me voitas siirtää sitä todennäkösyyspalikkaa mihinkään suuntaan sen alustavan arvion jälkeen. Johtuen siitä, että meillä ei oo sitä tiedustelutietoa siitä. Utopistisessa maailmassa meillä olis. Se olis vuosien ajalta ja siellä olis, että todennäköisyysarviota muutettu sillon ja sillon, tästä ja tästä syystä.” (haastateltava C)*

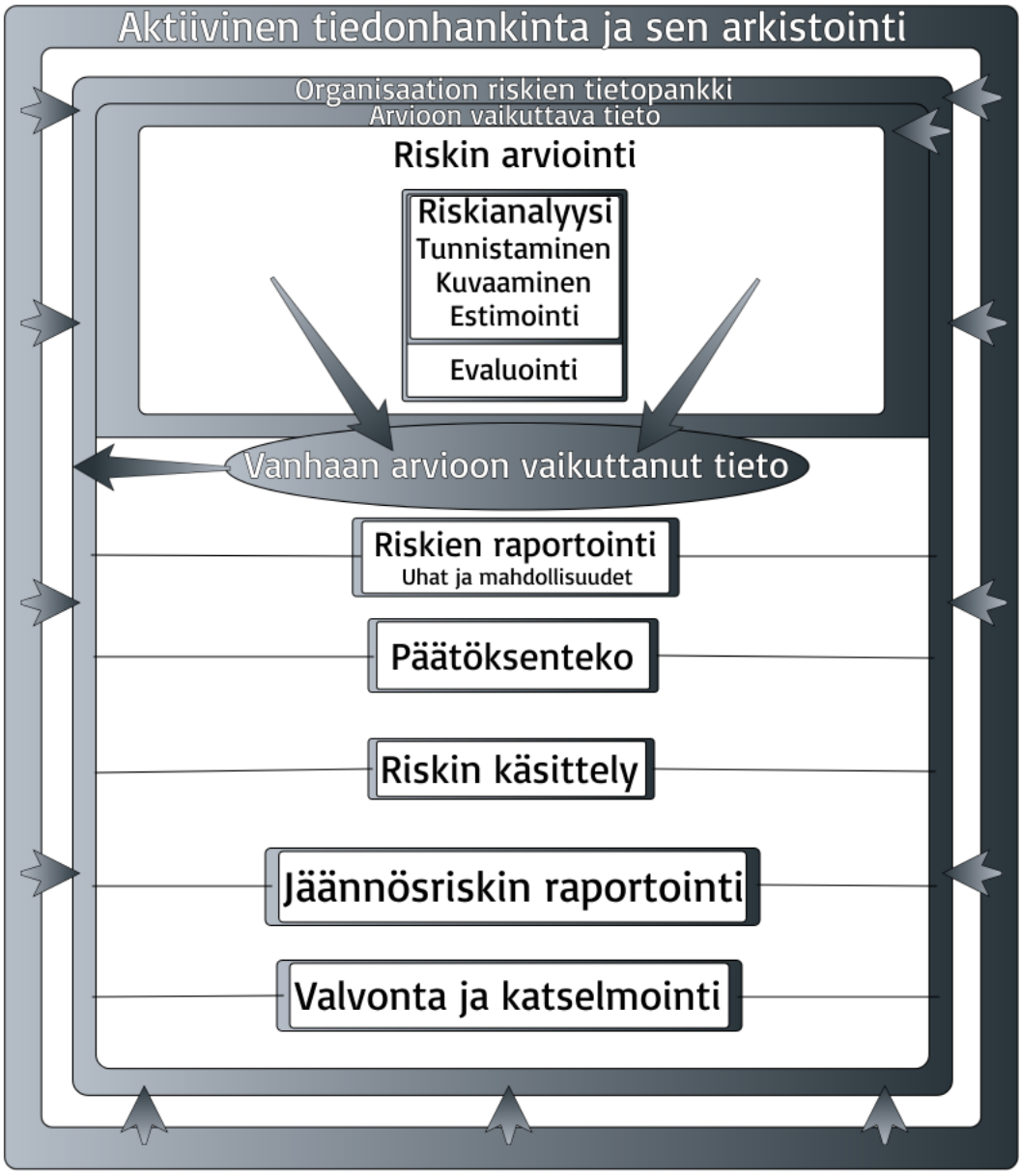
Tietokokoelma pitää sisällään aikaisempien riskien arvioiden pohjalla olevan tiedon ja dokumentit perusteluin, että miksi tiettyyn estimaatioon on päädytty juuri kyseisenä vuonna tai kyseisessä kvartaalissa. Tällöin voidaan aktiivisesti uutta tietoa hankkimalla rakentaa ajan kuluessa sellainen pohja riskien arvioinnille, joka tukee entistä varmempaa riskienhallinnan työskentelyä sekä antaa työkaluja oikeanlaisten politiikkojen kirjoittamiselle, jolloin organisaatio osaa kohdistaa omat resurssinsa oikein. Tärkeää on kuitenkin ymmärtää se, että riskien todennäköisyyksien arviointi tulee aina olemaan subjektiivinen näkemys ja tulevaisuutta ei voi ennustaa menneisyyden pohjalta, mutta lisäämällä tietoa subjektiivisen näkemyksen pohjalle siitä voidaan tehdä varmempi. Jäsennelty riskien estimointimalli on kuvattu kuviossa 8.

> *”- - se ongelma on se, että mikä niiden eri uhkakuvien tai uhkien oikee, realistinen todennäkösyys on. Millä konkreettisella, oikeella tiedolla sitä arviota vois tehdä uskottavammaks ja luotettavammaks. - - jos mennään ihan oikeesti simppeliin, niin mikä on tulipalon todennäkösyys tälläses toimistorakennukses. Se on vaan mun arvio siitä, että jos meillä on skaala yhestä viiteen tai yhestä kolmeen, niin se on vaan mun arvio, että se on yks. - - nää kaikki on sellasia subjektiivisia arvioita. Jos otettas, vaikka kolme ihmistä tekemään sama arvio, niin ne olis jossain määrin samanlaisia, mut siel olis varmaan paljon erojaki ja kukaan meistä ei voi sanoa, että hänen arvio on parempi kuin sen toisen, koska kellään se ei perustu varsinaiseen tietoon, vaan intuitioon siitä, mitä se vois olla. Tää on semmonen ihan musta aukko.” (haastateltava C)*

KUVIO 8 Rakennettu riskien estimoinnin malli

Ehdotus mallista muokattiin IRM:n (2002) käyttämästä riskienhallinnan prosessimallista siitä syystä, että se nojaa vahvasti ISO 31000 -standardiin ja organisaatio listaa nämä molemmat omaa työtään ohjaavina tekijöinä. Aivan kuten varsinaisessa IRM:n (2002) mallissa (luku 3.3), myös muokatussa mallissa korostuu dokumentoinnin tärkeys. Normaalin riskidokumentaation ja organisaation suuntaan viestimisen lisäksi dokumentointi pitää sisällään myös aktiivisen tiedonhankinnan sekä aktiivisen tiedon arkistoinnin. Tiedonhankinta sijoittuu mallissa formaalin auditoinnin tapaan käsitteeksi, joka ympäröi koko prosessia, ei pelkästään estimointivaihetta. Kun tiedonhankintaa ja arkistointia korostetaan jokapäiväisessä työssä, tietomäärä riskien arviointiin kasvaa ja tällöin vaikutus näkyy koko riskien arviointiprosessissa, ei ainoastaan estimointivaiheessa. Koska tiedonhankinnan tulee olla aktiivista ja sitä tulee aktiivisesti myös säilöä, tarkoittaa tämä sitä, että koko prosessin aikana tietoa riskeistä ja niiden todennäköisyyksien heilahteluista saadaan jatkuvalla syötöllä riskienhallinnan henkilöstölle erilaisista lähteistä riippumatta siitä, missä vaiheessa mallia ollaan menossa tietyn riskin kohdalla. Tiedon säilöminen sijoittuu riskienhallinnan prosessimallissa riskien arvioinnin kokonaisuuteen, koska siinä vaiheessa säilöttyä tietoa päästään hyödyntämään parhaiten ja tämä luo erinomaisen pohjan riskienhallinnan mallin muille askelille. Kuvio 9 esittää estimoinnin ympärillä pyörivän tiedon käytön koko mallissa. Kuviossa pyritään kuvaamaan estimoinnin mallin suhde koko riskienhallintamalliin. Siitä näkee, kuinka tietoa kerätään jokaisessa riskienhallinnan vaiheessa ja myös riskienhallinnan ulko-

puolella. Tätä prosessia toistetaan jokaisen riskin kohdalla, kun riski käydään läpi ja siitä saatu tieto siirretään organisaation riskien tietopankkiin, josta se taas vaikuttaa olemassaololollaan seuraavaan riskiarvioon.



KUVIO 9 Mallin suhteutuminen koko riskienhallinnan malliin

Iteratiivisena mallina jokainen riski tulee arvioida uudelleen säännöllisesti sen tiedon pohjalta, mitä riskistä on kertynyt edellisen arvion jälkeen ja mitkä tekijät ovat ohjanneet aikaisempia estimaatioita. Tietoa kerätään ajan kuluessa omaan, erilliseen taulukkoon, joka listaa organisaation tärkeimmät riskit riski-kehikon tapaan. Nykyaikaa kuvaavaan taulukkoon (taulukko 7) merkitään riskin nimi, nykyinen todennäköisyysarvio ja tekijät, kuten uutisointi, riskilistat, poliittinen tilanne maailmalla tai omakohtainen kokemus, jotka ovat vaikuttaneet todennäköisyysarvioon sillä hetkellä. Matriisi pitää sisällään myös riskin arvioinnin suorittaneen henkilön kommentit. Tämän jälkeen aina, kun riskiin

liittyvää tietoa löydetään, merkataan se lähteineen omaan dokumenttiinsa niin, että kaikki riskienhallinnassa mukana olevat henkilöt pääsevät siihen käsiksi. Taulukko toimii erillisenä tietokokoelmana varsinaisen riskienhallintakehikon rinnalla, jolloin alkuperäinen kehikko ei mene liian sekavaksi.

TAULUKKO 7 Esimerkki: miten nykyaikainen tieto riskin todennäköisyyteen vaikuttaneista asioista säilötään ehdotuksen mukaisesti

Riski	**Todennäköisyys 2019 (1-4)**	**Riskiarvioon vaikuttaneet tekijät**	**Arvioijan kommentit**
DDOS-hyökkäys	3	• Linkki uutiseen • Linkki tutkimusraporttiin, jossa käsitellään palvelunestohyökkäysten yleistymistä • Omakohtainen kokemus	• Palvelunestohyökkäysten yleistymisen ja helpottumisen johdosta riskin todennäköisyysarviota on nostettu aikaisemmasta kahdesta kolmeen. Nykyaikainen, yleistynyt CaaS-malli (Crime-as-a-Service) helpottaa erityisesti tavallisten ihmisten mahdollisuuksia ostaa palvelunestohyökkäys valitsemaansa kohteeseen. • Palvelunestohyökkäyksiä on yritetty kuluneen vuoden aikana normaalia enemmän. On vain ajan kysymys, koska joku onnistuu toteuttamaan massiivisen hyökkäyksen.

IRM:n (2002) mallin mukaisesti säännöllisin väliajoin järjestettävässä riskiarvioiden päivityksessä käydään tietoa sisältävän dokumentin uudet merkinnät läpi ja päivitetään riskien todennäköisyysarvioita siltä pohjalta, mitä tietoa riskeistä on kertynyt. Uuden tiedon lisäksi tehdään katsaus vanhaan tietoon, jota säilytetään omassa taulukossaan taulukon 8 mukaisesti. Tällä tavoin saadaan ajan kuluessa oikeaa tietoa siitä, laukeaako kyseinen riski useammin vai harvemmin kuin aikaisemmin ja tuleeko riskin todennäköisyyttä muuttaa isommaksi vai pienemmäksi.

Nykytilanteen lisäksi on siis tärkeää, että myös menneitä arvioita säilötään, jotta voidaan seurata, mitä on tapahtunut. Menneisyyden arviot säilötään samankaltaisessa taulukossa (taulukko 8), johon merkataan lisäksi vuosiluku. Tällöin saadaan oikeaa dataa siitä, millaiset asiat ovat vaikuttaneet riskien todennäköisyyksien arviointiin aikaisemmin ja millaisissa tilanteissa arviota on muutettu tai miksi se on pidetty samalla tasolla kuin aikaisemmin. Mennyttä kuvaavaan matriisiin siirretään joka vuosi vanhat tiedot todennäköisyydestä, vaikuttaneista tekijöistä sekä arvioijan vanhat perustelut arvion muutoksesta tai muuttumattomuudesta. Todennäköisyyksien taulukon lisäksi on hyvä ylläpitää samankaltaista taulukkoa myös vaikuttavuuden arvioista, vaikka Finanssiyritys

Oy:ssä tämä osa-alue koettiinkin nykyisellään toimivaksi, voi taulukko parantaa myös vaikuttavuuden arviointia.

> *"Mun mielestä se on se vaikutuksen arviointi helpompaa ja konkreettisempaa, että miten ehkä merkitsisi euroissa, jos tää tapahtuis, mut se todennäkösyys. Mä en välttämättä tykkää siitä perustelusta, et viimeseen viiteen vuoteen ei oo tällästä sattunu. Ei se oo niinku yhtään varma, että niin ei käy sitten huomenna, vaikka jotain osviittaa se antaa, mutta tälläsellä pohjalla täytyy kuitenki liikkua, että kun laitetaan sitä todennäkösyyttä, että miten tämä vois sitten olla. Ja just siinä puolessa auttais myös sellanen substanssitieto ja sen ilmiön tunteminen tarkemmin." (haastateltava B)*

Finanssiyritys Oy:ssä pitäisi siis pystyä paremmin arvioimaan todennäköisyyksiä, jotta dokumenteissa voitaisiin keskittyä olennaiseen. Tämä tarkoittaisi sitä, että riskienhallinnan ollessa vankemmalla tietopohjalla, voisi riskienhallinta tehokkaammin toimittaa palautetta politiikkojen luomista varten. Juuri tätä tiedon karttumista tämä ehdotuskin pyrkii tehostamaan. Kun palaute olisi laadukkaampaa, voitaisiin tehdä oikeanmallisia politiikkoja ja sitä kautta parannettaisiin myös riskienhallintaa ja riskien mitigointikeinojen tarkkuutta. Kaikki haastateltavat olivat sitä mieltä, että riskienhallinta ja tietoturvapolitiikka vaikuttavat toisiinsa. Dokumenttien tarkastelua tehdään Finanssiyritys Oy:ssä säännöllisesti yhdestä kolmeen kertaa vuodessa, riippuen tarkasteltavista riskeistä ja mikäli jotain tapahtuu maailmalla, luodaan katsaus omiin dokumentteihin ja varmistetaan, että asia on siellä käsitelty. Tämänkaltaisessa tiedon odottamisessa on se ongelma, että tiedon saapuminen organisaatiolle on tiedotusvälineiden varassa. Tietoa organisaatiolle valuu mediasta, viranomaiselta, emoyhtiöltä sekä silloin tällöin silmiin osuvista aihetta koskevista artikkeleista ja kirjallisuudesta. Aktiivisella, tiettyihin riskeihin ja omaan organisaatioon kohdistuvalla tiedonhankinnalla ja arkistoinnilla voitaisiin saada sellaista dataa, jonka pohjalta jokin vahingollinen tapahtuma olisi ennustettavissa ja organisaatio kykenisi suojautumaan siltä tai ainakin aloittamaan sen käsittelyn jo ennen kuin se aiheuttaa maailmalla isompia, organisaatioonkin vaikuttavia ongelmia.

Mallia tutkaillessa tulee muistaa, että muodostuva tietokokoelma on pitkäaikaisen tiedon keräämisen ja käsittelyn tulos ja sellaista ei voi olla olemassa, jos tietoa ei ole aikaisemmin säilötty ja etsitty aktiivisesti. Mallin heikkoutena voidaankin mainita se, että tiedon kartuttaminen vie aikaa ja malli ei helpota riskien arviointiprosessia heti, vaan vasta pidemmällä aikavälillä. Tutkimustulokset tarjoavat hyvän pohjan jatkotutkimukselle, sillä myös muiden organisaatioiden riskien arviointiprosessi voisi mahdollisesti hyötyä entistä järjestelmällisemmästä tiedonhankinnasta sekä omasta tietokokoelmasta liittyen juuri oman organisaation riskien todennäköisyyksiin vaikuttavaan tietoon. Kun on jotain, mihin nykytilaa saadaan verrattua, voidaan miettiä riskin todennäköisyyden tai vaikuttavuuden muutosta. Esimerkiksi voidaan ottaa taulukossa 8 mainittu 2016 DYN nimipalveluun kohdistunut palvelunestohyökkäys. Millainen oli poliittinen tilanne maailmalla, mistä isku tuli, miten tilanne eskaloitui ja miten

isku käytiin läpi mediassa? Tällainen tieto voisi teoriassa ennakoida uutta palvelunestohyökkäystä tai hyökkäysten aaltoa, joka omalta osaltaan saattaisi vaikuttaa myös organisaation toimintaan.

TAULUKKO 8 Esimerkki ajan kuluessa syntyneestä riskien arvioinnin tietokokoelmasta

Riski	**Aikaisemmat todennäköisyydet (1-4)**	**Riskiarvioon vaikuttaneet tekijät**	**Arvioijan kommentit**
DDOS-hyökkäys	2018 - 2 2017 - 2 2016 - 1 2015 - 1 2014 - 1	2018 • Vaikuttaneet tekijät 2017 • DYN DDOS tietoja: Mitä, miksi, milloin, mistä ym. 2016 • Vaikuttaneet tekijät 2015 • Vaikuttaneet tekijät 2014 • Vaikuttaneet tekijät	2018 • Kommentteja 2017 • Riskin todennäköisyyttä nostettu lokakuussa 2016 tapahtuneen DYN-nimipalveluun kohdistuneen palvelunestohyökkäyksen takia. Tämä hyökkäys toimii todisteena sille, että isotkin palvelut voidaan ajaa alas palvelunestohyökkäyksellä, jos niin oikeasti halutaan tehdä. 2016 • Kommentteja 2015 • Kommentteja • Perustelut arvion säilymiselle 2014 • Kommentteja • Perustelut arviolle • Maininta riskin kirjaamisesta ensimmäisen kerran kyseisenä vuonna
Esimerkkiriski	2018 - 1 2017 - 3	2018 • Vaikuttaneet tekijät 2017 • Vaikuttaneet tekijät	2018 • Kommentteja • Perustelut arvion radikaalille laskemiselle, esimerkiksi uusi tapa suojautua riskiltä. 2017 • Maininta riskin kirjaamisesta ensimmäisen kerran kyseisenä vuonna

Tästä päästään toiseen ongelmakohtaan, joka haastatteluissa nousi pintaan. Resurssien jakaminen oikein organisaatiossa, jossa riskienhallinta tapahtuu osana laajempaa toimenkuvaa. Ylempänä taulukoissa 7 ja 8 esitellyt matriisit ja niiden läpikäyminen vaativat vuodesta paljon aikaa, jota saattaa olla hankala järjestää, mikäli organisaatiolla itsellään ei ole panostaa resursseja riittävästi tai se kokee, että riskienhallintaan ei ole järkeä panostaa resursseja niin paljon, että arviointiprosessia varten olisi pyhitetty kokonaan oma tiimi.

Finanssiyritys Oy:ssä nähdään, että vaikka emoyhtiö osallistuukin jossain määrin riskienhallintaan tarjoamalla kehyksen ja tarvittaessa neuvoja, jää organisaatio silti turhan paljon erilleen emoyhtiöstä ja tämän riskienhallinnan resursseista.

> *"Eli ei meillä tosiasiassa oikeen vaan lihakset riitä hoitamaan sitä niin systemaattisesti. Sitte tietysti jälleen täydellisessä maailmassa meillä olis jotain työkaluja ja jälleen enemmän aikaa tehä sellasia taustaselvityksiä." (haastateltava B)*

Haastateltavat selkeästi toivoivat, että emoyhtiöstä jaettaisiin heidän riskienhallintayksikössään olevaa osaamista ja yhteistyö olisi entistä tiiviimpää. Koska riskienhallintaa tehdään Finanssiyritys Oy:ssä muun työn ohella, kokevat A ja B, että heillä ei ole aivan niin paljon aikaa käyttää tähän työhön kuin mitä se todellisuudessa oikeasti vaatisi. Riskiarvion tukena voidaan ja myös suositellaan käytettäväksi olemassa olevien mallien mukaan ulkoisiakin toimijoita, jotka ovat erikoistuneet organisaatiokohtaisten riskien tunnistamiseen ja tiedonhankintaan. Heidän hankkimansa tiedon pohjalta voidaan tarjota organisaatiolle lisää vankkaa pohjaa riskien arviointiprosessiin ja täydentää ehdotuksen mukaista tietokokoelmaa riskeihin liittyen.

> *"- - pitäs saada sellanen ymmärrys, että mikä on, ja mun toive on myös se, että me voitas saada sieltä emoyhtiön puolesta, koska heillä on resursseja ihan eri luokassa. - - me voitas kääntyy heidän puoleen, että mitä te voitte tarjota, että me voidaan tehä tää asia paremmin." (haastateltava C)*

Vaikka riskienhallintakehikko saikin kehuja, ei sekään ole nykyisellään täydellinen. Nykyprosessissa nähtiin ongelmakohtana se, että prosessikaavio tulee emoyhtiöltä ja riskimatriisia työstäessä taustalla on sellaisia logiikoita, mitä ei ole avattu organisaatiolle riittävästi sekä viittauksia dokumentteihin, mitkä eivät ole organisaatiolle suoraan saatavilla.

> *" - - ainahan nää luokitellaan sillä vakavuus-todennäkösyys asteikolla ja niiden tuloksena saamme hienon värikartan riskikehikkoon. Se on suoraan sanoen kyllä sellanen, että ei toimi ihan parhaiten meillä, koska se on konsernista sitten ylempää meille lasketettu ja sen verran monimutkaset logiikat siellä taustalla ja lisäksi viittauksia sellasiin taulukoihin, joita ei ole meillä talossa, mutta kyllähän sen logiikan näkee." (haastateltava B)*

Pitkäaikaisella, iteroivalla mallilla tuotettu tietokokoelma tukee tulevaisuuden arvioita ja organisaatiolla on parempi ymmärrys siitä, miten riskit elävät ja miten esimerkiksi maailmalla vallitseva poliittinen yleistila voi vaikuttaa, vaikka DDOS-hyökkäyksen todennäköisyyteen.

Finanssiyritys Oy:ssä ymmärretään se, että kaikki tämä perustuu pohdinnan ja tiedonkeruunkin jälkeen subjektiiviseen näkemykseen riskien todennäköisyyksistä. Kaikkien riskien perustaso voi olla liian matala tai liian korkea. Tärkeää on kuitenkin todennäköisyyden oikeellisen tason sijaan se, että riskienhallinta näkisi, miten riskitaso on muuttunut ja miksi. Vaikka riskitaso yleisesti olisikin dokumenteissa liian korkea oikeaan tasoon nähden, niin se ei aiheuta ongelmia, kun taustatieto on olemassa ja kaikelle on perustelut. Kun riskien todennäköisyyksien muuttunut tila on vuosien dokumentoinnin ohjaama, riskienhallinta keskittyy oikeisiin asioihin ja organisaation politiikat ovat tarkempia, jolloin organisaatio laittaa resursseja oikeasti sitä hyödyttäviin asioihin.

7 Tutkimuksen pohdinta ja yhteenveto

Tässä luvussa käydään läpi tutkimuksen pohdinta sekä yhteenveto. Tutkimuksen tarkoituksena oli muodostaa malli ulkoisten kyberturvallisuuden riskien arviointiin tutkittavan organisaation näkökulmasta. Tutkimus toteutettiin kvalitatiivisena tapaustutkimuksena, jossa tärkein tiedonlähde oli semi-strukturoitu haastattelu. Seuraavassa alaluvussa käydään läpi tutkimuksen tutkimuskysymykset ja miten niihin on tutkimuksen aikana vastattu. Toisessa alaluvussa käsitellään tutkimuksen validiutta, reliabiliteettia ja esitellään mahdollisuudet jatkotutkimukselle saman aiheen ympärillä.

7.1 Yhteenveto

Tutkimusmenetelmät valittiin sen pohjalta, että tutkimuksen kohde on pieni organisaatio finanssialalla ja heillä on pieni määrä riskienhallinnan ammattilaisia. Tästä syystä kvalitatiivinen, eli laadullinen tapaustutkimus oli oikeastaan ainut vaihtoehto. Valitut tutkimusmenetelmät tukivat hyvin tutkimusta ja tutkimuksen läpivienti oli sujuvaa.

Tutkimuksessa esiteltiin aluksi tutkimuskysymys sekä kaksi apukysymystä ohjaamaan tutkimuksen kulkua. Tutkimuskysymystä muutettiin tutkimuksen aikana useampaan kertaan tarkemmaksi sen mukaan, miten tutkimuksen aihetta lähdettiin missäkin osassa rajaamaan. Tutkimuksessa pyrittiin lopulta vastaamaan seuraavaan kysymykseen:

> **Millainen riskien arvioinnin malli tukee kyberturvallisuuden ulkoisten riskien arviointia?**

Tutkimusongelman selvittämiseksi laadittiin myös apukysymyksiä, joihin tämä tutkimus vastaa. Näiden avulla ohjattiin tutkimusta oikeaan suuntaan ja pyrittiin tuomaan lisäarvoa tutkimukselle. Apukysymykset muotoiltiin seuraavasti:

> **Millaisia nykymalleja riskien arviointiin on olemassa?**

Miten kyberturvallisuuden ulkoisia riskejä tulisi arvioida?

Tutkimusongelmaan tutkimus vastaa tutkimustulokset-luvussa, jossa esitellään malli, joka helpottaa ulkoisten kyberturvallisuuden riskien arviointiprosessia. Malli perustellaan luvussa 6 haastattelujen lainauksilla ja haastatteluissa ilmenneillä huomioilla. Yksinkertaisuudessaan malli, joka tukee ulkoisten kyberturvallisuuden riskien arviointia on perusrungoltaan jo olemassa oleva IRM:n (2002) malli, johon tuotiin lisäarvoa syventämällä sen riskien estimoinnin osiota.

Ensimmäiseen apukysymykseen vastataan tutkimuksen kirjallisuusosiossa, luvussa 3. Kolmannessa luvussa käydään läpi riskien arvioinnin olemassa olevia malleja, jotka tarjoavat rungon riskien arvioinnille. Toiseen apukysymykseen tutkimus vastaa luvussa 6. Luvussa kerrotaan esimerkein ja taulukoin, miten tätä muokattua riskien arvioinnin mallia voidaan hyödyntää ulkoisten kyberturvallisuuden riskien arvioinnissa. Haastattelujen tulokset tuovat hyvin toteen sen, miten nykyiset riskienhallinnan prosessit on tutkitussa organisaatiossa otettu haltuun. Kyberturvallisuuden ulkoisia riskejä tulee arvioida pitkäjänteisesti iteroivalla mallilla, joka palaa jo kertaalleen arvioituihin riskeihin tasaisin väliajoin ja käy riskin arvioinnin uudelleen läpi samalla tuottaen lisää dataa organisaation riskien tietoa sisältävään kokoelmaan. Organisaatio selvästi kokee, että strategia, tietoturvapolitiikka ja kulttuuri ohjaavat riskien arviointia aivan kuin luvussa 2 on esitelty. Organisaatio myös tukeutuu esiteltyihin standardeihin ja hyödyntää niitä omassa riskienhallinnan työssään.

Rakennetun riskien estimoinnin mallin heikkoutena huomataan, että mallin täydellinen hyödyntäminen vaatii useamman vuoden systemaattisen työn tietokokoelman rakentumiseksi, joten se ei nopealla aikataululla tuo parannusta ja saattaa jopa jossain määrin tukkia riskienhallinnan yksikköä, kun uudistusta aletaan toteuttaa. Mallin rakentaminen abstrakteille asioille ei myöskään helpotu sillä, että tarjolla ei ole olemassa tietoa, jota hyödyntämällä tulevaisuuden ennustaminen olisi mahdollista.

7.2 Pohdinta

Tutkimuksen tavoitteena oli selvittää toimeksiantajan kyberturvallisuuden ulkoisten riskien arviointiprosessin heikkouksia ja rakentaa prosessin kehittämistä tukeva malli. Tutkimustuloksista kuitenkin nähdään, että kyberturvallisuuden alakohtaisuus ei juurikaan näy haastatteluissa ja haastateltavat eivät ottaneet tähän kantaa. Tämä johtunee siitä, että kybertilassa olevat riskit näkyvät toimijoille samankaltaisina, joskin eri prioriteeteilla. Von Solms & Van Niekerk (2013) määrittelevät kyberturvallisuuden suojauskohteet, jotka ovat kattavat myös finanssialan organisaatiossa (luku 2.5). Kyberturvallisuuden alakohtaisuuden lisäksi tutkimustuloksista voidaan huomata myös ulkoisten riskien huomiointi, joka organisaatiossa ei eroa sisäisten riskien huomioinnista. Molemmista suunnista tulevat riskit käsitellään samalla kaavalla, mikä voi olla se-

kä hyvä että huono asia – hyvä asia siinä mielessä, että kaikki on yhtenäistä, ja huono asia siinä mielessä, että sisäiset ja ulkoiset riskit eroavat toisistaan jossain määrin, kuten luvussa 2.1 esitellään. Pitäisikö ulkoisten ja sisäisten riskien käsittelyprosessit eriyttää toisistaan vai ei? Tämän aiheen ympärillä olisi mahdollista tehdä lisätutkimusta.

Tutkimustulokset saatiin jäsenneltyä suoraan haastattelujen pohjalta ja haastattelut loivat hyvän asetelman muokatun mallin rakentamiselle. Muokattu malli rakennettiin olemassa olevaan IRM:n (2002) malliin muokkaamalla sen riskien arviointiosiota niin, että se tarjoaa pidemmällä aikajänteellä tukea organisaation ulkoisten kyberturvallisuuden riskien arviointiin. Samalla mallia vietiin enemmän Gerber ja Solmsin (2005) ehdottamaan riskienhallinnan ja riskien arvioinnin eriyttämisen suuntaan. Muokattu malli laajentaa myös alkuperäistä IRM:n (2002) mallia positiivisesti, sillä lisäykset parantavat sellaisenaan sitä käyttävien organisaatioiden hallussa olevaa tietoa omista riskeistään ja tarjoavat vankemman pohjan riskien arviointiprosessiin.

Mallin rakentaminen ei ollut itsessään helppo prosessi, sillä haastattelujen aikana selvisi, että tutkittavan organisaation kokemat ongelmat olivat niin abstraktilla tasolla, että niiden ratkaiseminen mallin rakentamisella vaikutti todella hankalalta. Haastateltavat näkivät kahdeksi suurimmaksi ongelmaksi ajanpuutteen ja todennäköisyyksien arvioinnin. Tutkimuksen tueksi löytyi paljon kirjallisuutta ja aikaisempaa tutkimusta liittyen riskienhallintaan. Mitä tarkemmin tutkimusta rajattiin ensin ulkoisiin riskeihin, sitten kyberturvallisuuteen ja lopulta haastattelun pohjalta riskien arvioinnin estimointiosioon, sitä vähemmän aikaisempaa tutkimusta löytyi ja lopulta todennäköisyysarvion tueksi tutkimus oli lähes olematonta. Tästä syystä on myös tärkeää, että tällaista ”tulevaisuuden ennustamista” tutkitaan lisää ja pohditaan sitä, mihin todennäköisyysarviot oikeasti pohjaavat kaikissa organisaatioissa.

Malli saa tukea myös Kokkomäen & Nortusen (2016) tutkimuksesta, jossa haastattelujen pohjalta he paikansivat samankaltaisia ongelmakohtia haastattelemalla useita tietoturvajohtajia. Kokkomäki & Nortunen (2016) lisäsivät omaan Heräte-malliinsa myös aktiivisen tiedonhankinnan yleisellä tasolla. Tämä tarkoittaa sitä, että oman riskeihin liittyvän tietopankin rakentaminen organisaatiokohtaisesti on asia, jota jokaisen organisaation tulisi harkita. Tämä tutkimus myös vahvistaa käsitystä, jonka Kokkomäki & Nortunen (2016) saivat omassa tutkimuksessaan ja samalla malli laajentaa heidän olemassa olevaa yleisen tason riskien arvioinnin mallia aivan, kuten malli laajentaa myös IRM:n (2002) olemassa olevaa mallia.

Tutkimuksen löydökset ovat yleistettävissä kaikille aloille ja niiden kautta voidaan pohtia minkä tahansa organisaation riskien arvioinnin prosessia ja sen ongelmakohtia. Kuten aikaisemmin luvussa 2 todetaan, riskienhallinta perustuu pitkästi intuitiolle ja useamman luvussa esitellyn lähteen mukaan epävarmuudelle tulevaisuudesta (Ahteensuu, 2014; Salmela, 2008; Straub & Welke, 1998; Fischhoff, 1992; Yates & Stone, 1992). Tämä tarkoittaa niin tutkimuksen kuin Baskervillenkin (1991) mukaan sitä, että riskien todennäköisyyden ennustaminen on arvioijasta kiinni ja prosessi ei ole tieteellinen. Fischhoffin (1992)

mukaan riski käsitteenäkin on subjektiivinen ja nojaa arvioijan käsityksiin. Tutkimus tukee ajatusta riskien arvioinnin subjektiivisuudesta, kuten Yates & Stone (1992) teoksessaan tuovat ilmi, ihmisten mielipiteisiin ja ajatuksiin vaikuttavat monet asiat ja tätä kautta ne vaikuttavat myös riskiarvioihin. Haastateltavat myös selkeästi kokivat subjektiivisuuden eräänlaisena ongelmana, joka vaikuttaa riskien arviointiin negatiivisesti.

Vaikka tietopankkiin siirtyvät arviot ovat jatkossakin subjektiivisia arvioita, antaa tämä kuitenkin tulevaisuudessa mahdollisuuden tarkastella menneisyyttä ja perusteita riskien arvioiden takana. Useamman arvioijan subjektiivisen näkemyksen perusteella rakentuu näkemys nykytilanteesta, joka mahdollisesti on lähempänä totuutta kuin vain yhden arvioijan näkemys. Samalla voidaan arvioida, kuinka hyvin aikaisempi arvio on pitänyt paikkaansa ja näin pienentää myös subjektiivisen näkemyksen vaikutusta. Historiatiedon säilöminen korostuu tutkimuksessa, koska luvussa 3 esitellyn mukaisesti Amaran (1981) mukaan ei ole muita tapoja tulevaisuuden ennustamiseen kuin menneisyys, josta voidaan nähdä merkittävien tapahtumien aiheuttamia trendejä ja ottaa oppia.

Ajanpuutteen sekä subjektiivisuuden vaikutusten vähentäminen on mahdollista. Spears & Barki (2010) mukaan osallistamalla henkilökuntaa enemmän riskienhallintaprosessiin, saadaan prosessille lisäarvoa. Spears & Barki (2010) tekevät tutkimuksessaan huomion, että vaikka henkilökuntaa pidetään usein heikoimpana lenkkinä riskienhallinnan kannalta, voi henkilökunta tarjota ääretömän tärkeää substanssitietoa riskienhallinnalle. Osallistamalla henkilökuntaa enemmän, voidaan työtaakkaa jakaa useammalle ja tällä tavoin lisätä riskienhallinnan ammattilaisten mahdollisuuksia keskittyä heille olennaisempiin asioihin (Spear & Barki, 2010). Tutkittu organisaatio tekeekin tätä jo, kuten tapauksen esittelyssä käy ilmi, mutta osallistamisen tulisi olla huomattavasti aktiivisempaa kuin 1-2 vuoden välein järjestettävä ajatushautomo.

Tutkimuksen tulosten päälle on riskienhallinnan ammattilaisten hyvä lähteä rakentamaan toimivampaa prosessia, joka ajan kuluessa nojaa enemmän ja enemmän tiedolle. Tällöin intuition vaikutusta saadaan pienennettyä ja kaikki pohjautuu johonkin. Tulosten merkitys riskienhallinnalle onkin positiivinen, jos mallia seurataan pitkäjänteisesti ja työtä tehdään systemaattisesti. Erityinen apu tuloksilla on riskien arviointiprosessille ja erityisesti arvioinnin analyysiosion estimointivaiheeseen, jossa riskin todennäköisyys- sekä vaikuttavuusarvio suoritetaan IRM:n (2002) mallissa (luku 3.3). Tutkimuksen tuloksia voivat hyödyntää riskienhallinnan ammattilaiset, tietosuojajohtajat sekä organisaatioiden johto. Tulokset soveltuvat erityisesti riskienhallinnan ammattilaisille. Tulosten hyödyntäminen voi olla esimerkkien mukaista mallin seuraamista, tai tuloksista voi ottaa käyttöön ne osa-alueet, joissa kokee parantamisen tarvetta omassa organisaatiossaan.

7.3 Tutkimuksen luotettavuus ja jatkotutkimus

Tutkimuksen luotettavuus arvioidaan kahden tekijän, validiteetti ja reliabiliteetti, summana. Hirsjärven, Remeksen & Sajavaaran (2009) mukaan validius tarkoittaa sitä, että tutkimuksella mitataan juuri sitä, mitä on tarkoitus mitata. Haastattelututkimuksella on useampia mahdollisuuksia epäonnistumiselle. Myers & Newman (2006) luettelevat kvalitatiivisen haastattelun kompastuskiviksi mm. tilaisuuden keinotekoisuuden, luottamuspulan, ajanpuutteen, haastattelijan saapumisen organisaatioon, väärin valitut haastateltavat, Hawthornen efektin, tiedon rakentamisen sivuuttamisen, kielen merkityserot ja yleisesti haastattelun epäonnistumisen. Reliabiliteetti Hirsjärven ym. (2009) mukaan on tutkimuksen toistettavuus, eli miten helposti joku toinen tutkija voi toistaa tutkimuksen jossain muualla. Reliabiliteetti voidaan varmistaa esimerkiksi niin, että kaksi eri tutkijaa päätyvät samankaltaisiin tutkimustuloksiin.

Tutkimuksen luotettavuus on pyritty varmistamaan tässä tutkimuksessa niin, että liite 1 pitää sisällään haastattelurungon ja tutkimus itsessään on kuvattu mahdollisimman tarkasti sillä ajatuksella, että sen voi mahdollisesti toistaa muuallakin. Haastattelututkimusten toistaminen toisaalta voi olla hankalaa, sillä jokainen haastattelu voi epäonnistua tai vaikuttaa haastateltavaan usealla eri tavalla, kuten Myers & Newman (2006) toteavat. Nämä tekijät itsessään voivat myös vähentää tutkimuksen luotettavuutta. Validiteetti tässä tutkimuksessa on riippuvainen tutkimusmenetelmien valinnasta ja toteutuksen onnistumisesta suhteessa näihin menetelmiin. Lisäksi taustalla vaikuttaa valittu kirjallisuus. Semi-strukturoitu haastattelu nähtiin parhaimpana vaihtoehtona pienen otannan haastatteluille ja toiveenakin oli, että keskustelu pääsisi rönsyilemään. Aikaa haastatteluille oli varattu tunti ja jokainen haastattelu venyi muutaman minuutin yli tavoiteajasta, joka ei sinällään vaikuttanut haastattelujen etenemiseen, koska haastateltavat olivat tietoisia suuntaa-antavasta aikatauluarviosta.

Tutkimus on hyvä pohja tulevaisuuden tutkimuksille, sillä tutkimusta aiheesta on erittäin vähän ja olisikin mielenkiintoista selvittää, miten prosessi toimii muissa organisaatioissa myös finanssialan ulkopuolella ja onko muilla organisaatioilla jo otettu huomioon mallissa esitellyt muutokset. Riskien arviointiprosessin tutkiminen myös nykymallien näkökulmasta voi paljastaa puutteita organisaatioiden toimissa ja sitä kautta auttaa organisaatioita kehittämään omaa riskien arvioinnin työtään. Lisäksi jatkotutkimuksen kannalta olisi varmasti hyvä tehdä tutkimusta mallin käyttöönoton seuraamuksista.

8 Lähteet

Ahteensuu, M. (2014). Riskianalyysi ja ennaltavarautumisen periaate. http://filosofia.fi/node/4062 Viitattu 2.12.2018.

Allen, J. (2005). Governing for enterprise security. Carnegie Mellon University/Software Engineering Institute Technical Note CMU/SEI-2005-TN-023.

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

Baccarini, D., Salm, G., & Love, P. E. (2004). Management of risks in information technology projects. Industrial Management & Data Systems, 104(4), 286-295.

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. Journal of Systems and Software, 81(12), 2118-2133.

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

Berg, H. P. (2010). Risk management: procedures, methods and experiences. Risk Management, 1(17), 79-95.

Boehm, B. W. (1991). Software risk management: principles and practices. IEEE software, 8(1), 32-41

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.

Colorado State University. (2019). Writing@CSU. https://writing.colostate.edu/guides/guide.cfm?guideid=60. Viitattu 5.1.2019.

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

Dhillon, G. (2004). Realizing Benefits of an Information Security Program, Business Process Management 10(3): 260–261

DiCicco-Bloom, B. & Crabtree B.F. (2006). The qualitative research interview. Medical Education 2006. 40: 314–321. doi:10.1111/j.1365-2929.2006.02418.x

Douglas, M. (1990). Risk as a Forensic Resource. Daedalus vol. 119. No. 4. pp. 1-16. https://www.jstor.org/stable/i20025331. Viitattu 20.12.2018.

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

Eskola, J. & Suoranta, J. (1998). Johdatus laadulliseen tutkimukseen. EISBN:9789517685047

Fairbank, J. F., Labianca, G. J., Steensma, H. K., & Metters, R. (2006). Information processing design choices, strategy, and risk management performance. Journal of Management Information Systems, 23(1), 293-319.

Fischhoff, B. (1992). Risk taking: A developmental perspective. In J. F. Yates (Ed.), Wiley series in human performance and cognition. Risk-taking behavior (pp. 133-162). Oxford, England: John Wiley & Sons.

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

Gillham, B. (2000). Case study research methods. London; New York: Continuum. ISBN 9781441159069

Gordon, L.A. and Loeb, M.P. (2002). Return on Information Security Investments, Myths vs Realities, Strategic Finance 84(5): 26–31

Hakala, M., Vainio, M. & Vuorinen, O. (2006). Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

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

Heikkilä, T. (2014) Tilastollinen tutkimus. Edita Publishing Oy 2014 9. painos. EISBN:9789513769420

Hirsjärvi, S. & Huttunen, J. (1995). Johdatus Kasvatustieteeseen. ISBN 951-0-20512-5.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). Tutki ja kirjoita. Helsinki: Tammi.

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

Ilmonen, Ilkka, Kallio, Jani, Koskinen, Jani, Rajamäki, Markku 2010. Johda riskejä – käytännön opas yrityksen riskienhallintaan. Helsinki: Kustannusosakeyhtiö Tammi.

Institute of Risk Management. IRM. (2002). A Risk Management Standard. https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf. Viitattu 9.12.2018.

IRM 12/2018a. (2018). Kotisivut: https://www.theirm.org/the-risk-profession/risk-management/irms-risk-management-standard.aspx. Viitattu 12.12.2018.

IRM 12/2018b. (2018). Kotisivut: https://www.theirm.org/about/.aspx. Viitattu 12.12.2018.

ISO 27001:2005. (2005). Information technology — Security techniques — Information security management systems — Requirements. ISO/EIC

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

ISO 27001:2018. (2018). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.

ISO 31000. (2018). 31000: 2018 Risk management - Guidelines. International Organization for Standardization.

ISO 12/2018. (2018) ISO Kotisivut. https://www.iso.org/about-us.html. Viitattu 12.12.2018.

ITU. (2018) Introduction to Security Cyberspace, Cybercrime and Cybersecurity https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf. Viitattu 24.4.2019

Kansallinen turvallisuusauditointikriteeristö, Katakri. (2015). Tietoturvallisuuden auditointityökalu viranomaisille. Suomen puolustusministeriö.

Kaplan, Robert S., and David P. Norton. (2004) Strategy Maps: Converting Intangible Assets into Tangible Outcomes. Boston: Harvard Business School Press, 2004.

Kaplan, R. S., & Norton, D. P. (2000). Having trouble with your strategy? Then map it. Focusing Your Organization on Strategy—with the Balanced Scorecard, 49.

Klimburg A, editor. (2012) National cyber security framework manual. NATO CCD COE Publications.

Kokkomäki, T. & Nortunen, M. (2016). Heräte: Validoitu riskien arvioinnin prosessimalli organisaation menestyksen tukemiseksi. JYU.

Kotler, P. & Keller, K.L. (2006). Marketing management 14. painos. Prentice-Hall. http://socioline.ru/files/5/283/kotler_keller_-_marketing_management_14th_edition.pdf. Viitattu 5.1.2019.

Krimsley, V. S. 1995. *Introductory Chemistry*, 2nd Ed. Brooks/Cole Publishing Co., Pacific Grove.

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

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

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

Lindström, G. (2012). Meeting the Cyber Security Challenge. Geneva Papers. Geneva Centre for Security Policy. https://www.files.ethz.ch/isn/147788/7-2012.pdf. Viitattu 4.1.2019.

Lämsä, A-M. & Hautala, T. (2005). Organisaatiokäyttäytymisen perusteet. 6. painos. Helsinki: Edita Prima Oy.

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

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

Maury, M. (2016). Ketterää strategiaa etsimässä: voiko strategia, jota ei tunneta olla ketterä? Työn tuuli 1/2016. S. 46.

https://www.henry.fi/media/ajankohtaista/tyon-tuuli/tt-1_2016.pdf#page=46 Viitattu 11.4.2019.

Metsämuuronen, J. (2008). Laadullisen tutkimuksen perusteet (3. uud. p.). Helsinki: International Methelp. ISBN 9789525372243.

Miettinen, J.E. (1999). Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari.

Myers, M. D. & Newman, M. (2006). The qualitative interview in IS research: Examining the craft. Information and Organization 17 (2007) 2–26. Viitattu 9.4.2019

Nieminen, S. (2016). Hyvä hankinta - parempi bisnes. Talentum Pro.

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

Oxford Dictionaries. (2018). Internet-lähde. Viitattu 9.12.2018

Popper, K. (1935). The Logic of Scientific Discovery.

Porter, M. E. (1980). Competitive Strategy: Techniques for Analyzing Industries and Competitors. New York: Free Press

Project Management Body of Knowledge. (2013) PMBOK. PMI.

Rakos, J., Dhanraj, K., Kennedy, S., Fleck, L. Jackson, S., & Harris, J. (2005). The practical guide to project management documentation. John Wiley & Sons.

Ropponen, J. (1999). Software risk management: Foundations, principles and empirical findings (Väitöskirja). Jyväskylän yliopisto.

Sanastokeskus TSK. (2004). "Tietoturvapolitiikka". Tiivis tietoturvasanasto. TSK31.
http://www.tsk.fi/tiedostot/pdf/TiivisTietoturvasanasto.pdf. Viitattu 23.12.2018.

Schein, Edgar H. (1985): Organizational Culture and Leadership. San Francisco: Jossey-Bass Publishers.

Schein, E. (1999). Sense and nonsense about culture and climate.

Suomen Pankki. (2018). Riskienhallinta ja -valvonta. https://www.suomenpankki.fi/fi/suomen-pankki/riskienhallinta-ja-valvonta/ Viitattu 2.12.2018.

Suomen riskienhallintayhdistys. SRHY. (2018) https://srhy.fi/toiminta/kansainvalinen-yhteistyo/ Viitattu 25.12.2018.

Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Management. MIS Quarterly Vol. 34 No. 3, pp. 503-522

Stake, R. E. (2010). Qualitative research: Studying how things work. New York: Guilford Press.

Stewart, A. (2004). On Risk: Perception and direction, Computers & Security 23(5): 362–370.

Straub, D.W. and Welke, R.J. (1998). Coping with Systems Risk: Security planning models for management decision making, MIS Quarterly 22(4): 441–469

Tsohou, A., Karyda M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. 79 Information Management & Computer Security, 14(3), 198 - 217.

Turvallisuus- ja puolustusasiain komitean sihteeristö. (2013). Suomen kyberturvallisuusstrategia.

Turvallisuuskomitea. (2015) Turvallinen Suomi 2015. https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/Turvallinen-Suomi-_-2015.pdf. Viitattu 5.1.2019

VAHTI. (4/2001). Sähköisen asioinnin tietoturvallisuuden yleisohje. Suomen valtiovarainministeriö. https://www.vahtiohje.fi/web/guest/home. Viitattu 24.12.2018

VAHTI. (4/2013). Henkilöstön tietoturvaohje. Suomen valtiovarainministeriö. https://www.vahtiohje.fi/web/guest/home. Viitattu 24.12.2018

VAHTI. (5/2013). Päätelaitteiden tietoturvaohje. Suomen valtiovarainministeriö. https://www.vahtiohje.fi/web/guest/home. Viitattu 24.12.2018

Valtioneuvosto. (2015). Suomen kansallinen riskinarvio 2015. http://urn.fi/URN:ISBN978-952-324-059-9

Valtiovarainministeriö, 1/2019 (2019) VATHI-ohjeen kotisivu: https://www.vahtiohje.fi/web/guest/home. Viitattu 2.1.2019

Vanhala, S., Laukkanen, M. & Koskinen, A. (2002). Liiketoiminta ja johtaminen (3. uud. p.). Helsinki: KY-palvelu

Von Solms, R. & Van Niekerk, J. (2013). From Information Security to Cyber Security. Computers & Security 38 97-102. School of ICT, Nelson Mandela Metropolitan University.

Whitman, M.E. (2003). Enemy at the Gate: Threats to information security, Communications of the ACM 46(8): 91–95.

Whitman, M.E. & Mattord, H.J. (2010). Management of Information Security. Course Technology

Whitman, M.E. & Mattord H.J. (2012) Information Security Governance for the Non-Security Business Executive. Kennesaw State University. Journal of Executive Education, 11(1) (2012). pp. 97–111.

Yates, J. F., & Stone, E. R. (1992). The risk construct. Teoksessa J. F. Yates, Wiley series in human performance and cognition. Risk-taking behavior, 1-25

Yhteiskuntatieteellinen tietoarkisto. (2019). Litterointi. https://www.fsd.uta.fi/aineistonhallinta/fi/kvalitatiivisen-datan-kasittely.html#litterointi. Viitattu 12.1.2019.

Yin, R. K. (2003). Case study research: Design and methods. Sage publications.

Young, C.S. (2009). Metrics and methods for security risk management. Burlington: Syngress.

9 Liite 1: Haastattelukysymykset

Haastattelukysymykset

Taustatietoa

1. Mikä on roolisi organisaation riskienhallinnassa?
2. Mikä on roolisi organisaation tietoturvallisuuden parissa?
3. Mikä on roolisi ulkoisten kyberturvallisuuden riskien arvioinnissa?

Tietoturva

4. Miten organisaation strategia ja tietoturvapolitiikka linkittyvät toisiinsa?
5. Miten strategia ja tietoturvapolitiikka huomioidaan ulkoisten kyberturvallisuuden riskienhallinnan sekä -arvioinnin prosessissa?
6. Vaikuttaako riskienhallinta tietoturvapolitiikkaan ja kuinka usein näitä verrataan, että ovat ajan tasalla toisiinsa nähden?

Riskikategoriat

7. Millaisia ulkoisia kyberturvallisuuden vahinko-, strategisia-, taloudellisia- ja operatiivisia riskejä organisaatio kohtaa?

Prosessi

8. Miten kuvaisit organisaation riskienhallinnan prosessia?
9. Miten kuvaisit organisaation ulkoisten kyberturvallisuuden riskien arviointia ja tunnistamista?
10. Mitä tietoa käytetään ulkoisten kyberturvallisuuden riskien arviointiin?
11. Mistä tieto tulee?
12. Miten organisaation kyberturvallisuuden riskianalyysin tulokset esitetään?
13. Päivitetäänkö riskien arvioita? Kuinka usein ja kuka päivittää?
14. Mitä standardeja, ohjeistuksia tai työkaluja organisaation ulkoisten kyberturvallisuuden riskien arviointi seuraa?
15. Mikä ulkoisten kyberturvallisuuden riskien arvioinnin prosessissa on toimivaa?
16. Mikä ulkoisten kyberturvallisuuden riskien arvioinnin prosessissa ei ole toimivaa?
17. Millainen on mielestäsi hyvä ulkoisten kyberturvallisuuden riskien arvioinnin prosessi?