LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Turvallisuusriskien hallintamalli, case Elisa Oyj

Harri Tiinus

Laurea-ammattikorkeakoulu

Turvallisuusriskien hallintamalli, case Elisa Oyj

Harri Tiinus
Turvallisuusjohtaminen (YAMK)
Opinnäytetyö
Heinäkuu, 2019

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusjohtaminen (YAMK)

Harri Tiinus

Turvallisuusriskien hallintamalli, case Elisa Oyj

Vuosi 2019 Sivumäärä 47

Tämän opinnäytetyön tavoitteena oli selvittää kohdeyrityksen turvallisuusriskien hallintamallin nykytila sekä tunnistaa hallintamallin mahdolliset puutteet suhteessa toiminnalle asetettuihin sisäisiin ja ulkoisiin vaatimuksiin. Tähän perustuen toteutettiin kohdeyritykselle päivitetty turvallisuusriskien hallintamalli. Päivitetyn hallintamallin piti vastata toiminnalle asetettuihin lakivaatimuksiin ja viranomaismääräyksiin sekä muuttuneen toimintaympäristön tuomiin haasteisiin.

Tutkimus toteutettiin laadullisena tapaustutkimuksena, jossa kohdeorganisaation nykytilaa tutkittiin tieteellisen havainnoinnin keinoin. Opinnäytetyössä käydään teoreettisessa osuudessa läpi riskienhallinnan käsitteitä sekä avataan riskienhallintaa, sen tavoitteita ja mahdollisia haasteita. Teoreettisessa osuudessa avataan hieman laajemmin ISO 31000 riskienhallinta standardia ja sen perusteella luotavan hallintajärjestelmän vaatimuksia.

Opinnäytetyön tuotoksena rakentui päivitetty turvallisuusriskien hallintamalli, joka noudattelee ISO 31000 riskienhallinta standardin vaatimuksia. Hallintamallin avulla kohdeorganisaatio kykenee hallitsemaan toimintaa uhkaavia turvallisuusriskejä kattavammin ja säännöllisemmin yhteismitallisten kriteereiden kautta.

Tutkimuksen tuloksia voidaan hyödyntää kohdeorganisaation muiden operatiivisten riskien hallinnassa sekä muidenkin riskilajien hallintamallin rakentamisessa. Koska riskienhallinta on johdettu pitkälti organisaation strategiasta ja tavoitteista ja riskien hallintamalli on räätälöity kohdeorganisaatioon sopivaksi, ei tutkimuksessa esitettyjä tuloksia pystytä suoraan hyödyntämään muissa organisaatioissa.

Asiasanat: riskienhallinta, turvallisuusriski, yritysturvallisuus

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

Harri Tiinus

Security Risk management model, case Elisa Corporation

Year 2019 Pages 47

The aim of this thesis was to identify the target company's security risk management model and to recognize any shortcomings of the current management model in relation to the internal and external requirements imposed on the company's risk management. The central part of this thesis was an updated security risk management model based on analysis of the current situation from the viewpoint of the selected theoretical framework. The aim was that the enhanced model would correspond to most relevant legal requirements and to resent changes in the target company's operational environment.

The selected research strategy was a qualitative case study, in which the current state of the target organization was investigated by the means of scientific observation. The theoretical part of the study presents the concept of risk management and explains the role and goals of risk management including some potential challenges regarding an organization's risk management. The study also reviews ISO 31000 risk management standard and the requirements the standard sets to risk management of the target organization.

The output of his thesis was an updated security risk management model, which corresponds to ISO 31000 risk management standard and its requirements. The enhanced risk management model enables the target company to manage its security risks regularly and more comprehensively through the aid of common risk management criteria.

The results of this study including the enhanced security risk management model can be utilized to manage also other operational risks for the target company. Elements of the principles and frameworks can also be utilized to manage other than operational risks. Because the risk management model is derived from the strategy and objectives of the host company and the risk management model is tailored to its needs, the results cannot be utilized in other organizations as such.

Keywords: risk management, security risk, corporate security

Sisällys

1 Johdanto

Viestintäviraston määräys teletoiminnan tietoturvasta edellyttää teleyrityksen huomioimaan turvallisuuden palvelujen elinkaaren eri vaiheissa sekä tunnistamaan teletoiminnan jatkuvuuden kannalta kriittinen omaisuus ja prosessit sekä käsiteltävä niihin kohdistuvia riskejä saannollisesti. Määräys edellyttää lisäksi, että teleyrityksen riskien hallinnan prosessit ja tulokset on dokumentoitava. (Viestintävirasto 2015)

Riskienhallinta on yrityksen turvallisuustoiminnan kannalta keskeinen prosessi, joka auttaa kohdistamaan organisaation turvallisuutta edistävät toimet oikein. Sekä turvallisuusjohtaminen että riskienhallinta ovat yritysturvallisuuden keskeisiä prosesseja ja ne ovat jatkuvia prosesseja, jotka pyrkivät ennaltaehkäisemään ja pienentämään yritykselle haitallisten tapahtumien vaikutusta. (Lanne 2007, 25-30)

Tämän opinnäytetyön tavoitteena oli selvittää kohdeorganisaation turvallisuusriskien hallintamallin nykytila sekä tunnistaa puutteet nykyisessä toiminnassa suhteessa organisaation turvallisuusriskien hallinnalle asetettuihin sisäisiin ja ulkoisiin vaatimuksiin. Tutkimuksessa tarkasteltiin kohdeorganisaation toimintaa ohjaavien laki- ja viranomaisasetusten vaatimuksia riskienhallinnan näkökulmasta sekä havainnoitiin kohdeorganisaation nykyistä toimintaa suhteessa vaatimuksiin. Havainnointiin sekä dokumentaation läpikäyntiin perustuvan analyysin jälkeen toteutettiin ehdotus päivitetystä turvallisuusriskien hallintamallista. Päivitetty malli pyrkii vastaamaan toiminnalle asetettuihin vaatimuksiin ja se pohjautuu ISO 31000 riskienhallinta -standardiin. Tutkimuksessa asetettiin kysymykseksi: ”Millä tavoin turvallisuusriskien hallinta on osana organisaation toimintaa?" ja "Millä tavoin toiminnalle asetetut vaatimukset ohjaavat turvallisuusriskien hallintaa?". Tutkimus toteutettiin laadullisena tapaustutkimuksena.

Tutkimus oli tarpeellinen, koska kohdeyrityksessä on tunnistettu tarve kehittää turvallisuusriskien hallintaa vastaamaan kokonaisvaltaisen riskienhallinnan periaatteita sekä muuttuneen toimintaympäristön asettamia vaatimuksia. Turvallisuusriskien hallinnan merkitys korostuu jatkuvasti, muun muassa toimintaan kohdistuvien uhkien lisääntymisen vuoksi. Lisäksi kohdeorganisaation toiminnan lisääntynyt kansainvälisyys asettaa riskienhallinnalle uusia haasteita, joihin uuden hallintamallin avulla pyritään vastaamaan. Hallintamalli oli tarpeen katselmoida ja päivittää myös lakivaatimusten ja viranomaismääräysten näkökulmasta, jotta organisaation toiminta on kaikkien sitä velvoittavien lakien ja asetusten mukaista. Lisäksi on oletettavaa, että esimerkiksi 5G:n laajempi käyttöönotto tulee lisäämään toimialaan kohdistuvaa kansallista ja kansainvälistä sääntelyä myös turvallisuuden ja riskienhallinnan osalta. Myös Sisäministeriön vuonna 2018 tekemän Kansallisen riskiarvio -julkaisun tulokset heijastelevat sitä trendiä, että kohdeorganisaatiossa on syytä tehdä vahvempaa ja systemaattisempaa turvallisuusriskien hallintaa.

Tämä tutkimus rajattiin käsittelemään vain kohdeyrityksen turvallisuusriskejä ja niiden hallintamallia. Tässä tutkimuksessa ei käsitellä muita riskilajeja, muuta kuin teoreettisella tasolla. Tutkimus rajattiin näin, jottei tutkittava kohde kasva liian suureksi, jolloin tulosten saaminen ja vertaileminen olisi ollut vaikeaa. Työn lopputuloksena syntyvää mallia pyritään tämän tutkimuksen valmistumisen jälkeen soveltamaan muihin kohdeorganisaation kohteisiin, ainakin operatiivisten riskien osalta.

1.1 Keskeiset käsitteet

Riski on termi, joka viittaa tappiolliseen tai vahingolliseen asiaan. Riski sanana pitää kuitenkin sisällään myös sen, että meillä on jo tieto siitä asiasta, joka uhkaa. Koska riskin aiheuttamaa vahinkoa voidaan mitata ja sen ilmenemisen todennäköisyyttä ennustaa, riskille voidaan laskea arvo. (Leppänen 2006, 29-30)

ISO 31000 standardi määrittelee riskin olevan epävarmuuden vaikutus, joka voi olla positiivinen, negatiivinen tai sekä että, tavoitteisiin.

Juvonen ym. (2014) määrittelevät riskin olevan ei toivottu tai epäedullinen tapahtuma henkilölle itselleen, toiselle henkilölle tai omaisuudelle. Suomenkielessä riskin synonyymit vaaraan tai uhkaan liittyviä, jolloin sana itsessään pitää sisällään olettamuksen epäedullisesta tapahtumasta.

Turvallisuusriski on sellainen tekijä, joka uhkaa yrityksen toimintaa, henkilökuntaa, yhteistyökumppaneita tai sen toimintaa sekä mainetta. Turvallisuusriskejä on laaja joukko ja uusia syntyy kaiken aikaa. (Allen & Loyear 2018, 4)

Riskienhallintaprosessi on kuvattujen periaatteiden ja menettelyjen soveltamista systemaattisesti ja säännöllisesti.

Riskien arviointi on käsite riskien tunnistamisen, riskianalyysin ja riskien merkityksen arvioinnin prosessille.

Riskien tunnistaminen on joukko erilaisia toimenpiteitä, kuten työpajoja, haastatteluita ja työvaiheiden havainnointia, joiden avulla havaitaan ja kuvataan tunnistettuja riskejä.

Riskianalyysi on prosessi, jossa pyritään ymmärtämään ja kuvaamaan riskin vaikutus kohteelle sekä tapahtuma taajuus eli todennäköisyys. Näiden avulla määritetään riskitaso.

Riskin merkityksen arvioinnissa riskianalyysin tuloksia verrataan määriteltyihin kriteereihin ja arvioidaan riskin suuruutta sekä tarvittavia toimenpiteitä sen hyväksymiseksi.

Riskinottohalukkuus on organisaation kyky tai taso, jonka se on valmis ottamaan päästäkseen tavoitteisiin.

Riskin sietokyvyllä tarkoitetaan riskin suuruutta, johon organisaatio on valmis sitoutumaan riskien määrittelyn jälkeen.

1.2 Kohdeorganisaatio

Elisa on tietoliikenne- ja digitaalisten palveluiden tuottaja, jolla on yli 6,2 miljoona kuluttaja, yritys ja julkihallinnon liittymää ja yli 2,8 miljoona asiakasta. Elisan päämarkkina-alueita ovat Suomi ja Viro, mutta se tarjoaa myös palveluitaan globaaleille markkinoille. Elisa on jaettu kahteen segmenttiin, henkilöasiakkaat ja yritysasiakkaat sekä kahteen niitä tukevaan yksikköön, tuotanto ja tukitoiminnot. (Elisa Vuosikatsaus 2018, 3)

Kuva 1: Elisan toimintamalli (Elisa 2018a)

Elisalla on pitkä, yli 135-vuotias historia ja Elisan historia heijastaa suomalaisen yhteiskunnan muutosta. Elisan tytäryhtiö Radiolinja kytki maailman ensimmäisen GSM-puhelun vuonna 1991. Tänä päivänä Elisan verkossa liikkuu eurooppalaisellakin tasolla huomattava määrä liikennettä ja matkapuhelinverkko peittää valtaosan Suomen väestöstä. (Elisa 2018b)

2 Tutkimuksen toteuttaminen ja menetelmät

Tämä opinnäytetyö on tutkimusstrategialtaan tapaustutkimus, jossa käytetään kvalitatiivista eli laadullista lähestymistapaa. Opinnäytetyö on tutkimuksellinen kehitystyö, jonka

tavoitteena on organisaation nykykäytänteiden tutkiminen ja analysointi sekä parannusehdotusten esittäminen.

Tapaustutkimuksen lähtökohtana on tuottaa syvällistä ja yksityiskohtaista tietoa tutkittavasta tapauksesta ja tapaustutkimus soveltuukin hyvin kehittämistyöhön, jonka tarkoituksena on tuottaa kehittämisehdotus tai -idea. Tapaustutkimus, kuten muutkin tutkimusmetodit, nojautuu teorioihin ja aiempiin aiheesta tehtyihin tutkimuksiin. Tutkijan on oleellista löytää kirjallisuudesta ne asiat, jotka ovat oleellisia omalle työlle ja joiden tapaus on ollut samankaltainen kuin omassa työssä. (Ojasalo, Moilanen & Ritalahti 2015, 52-54)

Tapaustutkimus soveltuu hyvin kyseiseen tutkimukseen koska sen avulla pyritään saamaan suppeasta aiheesta paljon tietoa ja siinä on otettava huomioon vallitseva toimintaympäristö ja sen ajalliset sekä sosiaaliset yhteydet. Tämän lisäksi tapaustutkimuksen luonteeseen kuuluu, että kattavan ja monipuolisen tiedon saamiseksi tutkittavasta tapauksesta käytetään monenlaisia menetelmiä, kuten tässä työssä tehdään. (Ojasalo ym. 2015, 55)

Tässä opinnäytetyö hyödynnetään konstruktiivista lähestymistapaa, jonka avulla pyritään tuomaan tutkimuksellista tietoa sekä uutta mallia tutkittavaan aiheeseen. Kappaleessa 3.1 kuvataan tarkemmin konstruktiivisen tutkimuksen menetelmät ja päämäärät.

Tieteellistä havainnointia hyödynnetään tässä tutkimuksessa kartoittamaan ja selvittämään nykyisen toimintamallin vahvuuksia ja heikkouksia. Havainnointia hyödynnettiin myös asiantuntijoiden aivoriihien ja työpajojen toimivuuden ja tulosten tarkastelussa. Tieteellisen havainnoinnin periaatteita on kuvattu tarkemmin kappaleessa 3.2. Tämän lisäksi nykytilan ja nykyisen toimintamallin arvioinnissa tutkitaan ja analysoidaan olemassa olevaa, kohdeorganisaation sisäistä, dokumentaatiota ja ohjeistusta. Olemassa oleva dokumentaatio piti sisällään muun muassa turvallisuusriskien hallinnanpolitiikan ja -periaatteet sekä tarkempia organisaatio kohtaisia menetelmiä ja ohjeita.

Heinonen, Keinänen ja Paasonen (2013, 34) toteavat kvantitatiivisen eli määrällisen ja kvalitatiivisen eli laadullisen tutkimustavan eroavan toisistaan ilmiön tai asian tarkastelukulman eroavuudesta. Määrällinen tutkimus voidaan toteuttaa, kun tutkittavaa ilmiötä on mahdollista tarkastella numeraalisten tilastojen avulla. Laadullisessa tutkimuksessa pyritään tulkitsemaan tutkittavaa ilmiötä sanallissilla tiedoilla.

2.1 Konstruktiivinen tutkimus

Konstruktiivisen tutkimuksen tavoitteena on ratkaista ongelma käytännönläheisesti luomalla uutta rakennetta. Konstruktiivinen tutkimus sopii kehittämistehtävän malliksi, kun tavoitteena luoda konkreettinen malli tai suunnitelma. Konstruktiivisen tutkimuksen tavoitteena on tutkimuksen kautta tuoda uutta tietoa liiketoiminnalle, sen haasteena on mallintaa

teoreettisen tiedon kautta ratkaisu liiketoiminnan käytännön ongelmaan. Ratkaisun pitäisi olla monistettavissa myös muualle kuin kohdeorganisaatioon. (Ojasalo, Moilanen & Ritalahti 2009, 65).

Konstruktiivisessa tutkimuksessa on kyse tavasta, joka pyrkii muuttamaan olemassa olevaa toimintamallia. Konstruktiivisessa tutkimuksessa korostuu teoreettisen tiedon merkitys osana tutkimusta ja uuden toimintamallin kehittämistä. (Ojasalo ym. 2009, 66).

Konstruktiivinen tutkimuksen prosessi pitää sisällään kuusi vaihetta. Kasanen, Lukka ja Siitonen (1993, 246) määrittelivät vaiheet seuraavasti:

1. Etsi käytännönläheinen ongelma, jossa on tutkimuksellista potentiaalia.
2. Hanki yleistä ja kattavaa tietoa aiheesta.
3. Innovoi uusi ratkaisu.
4. Demonstroi uuden mallin toimivuus.
5. Osoita teoreettinen yhteys ja mallin uutuusarvo.
6. Arvioi mallin sovellettavuus yleisesti.

Ojasalon ym. (2009, 66) mukaisesti konstruktiivisen tutkimus on lähestymistavaltaan pragmaattinen ja eroaa konsultaatiosta vahvemman teoriaan sidottavuuden kautta. Konstruktiivisessa tutkimuksen avulla toteutetun mallissa totta on se, mikä toimii.

Tässä opinnäytetyössä konstruktiivisen tutkimus prosessin avulla pyrittiin kuvaamaan prosessi sekä vaiheistamaan työn eri vaiheet. Konstruktiivinen tutkimus tapaa pystyttiin osittain soveltamaan tähän tutkimukseen, koska tavoitteena oli luoda uusi malli ja testata sen toimivuus käytännössä. Toki tässä tutkimuksessa ei innovoida kokonaan uutta ratkaisua, lähinnä pyritään löytämään olemassa olevalle toiminalle sopivampi hallintamalli.

2.2 Havainnointi

Tutkimuksellinen havainnointi eroaa jokapäiväisestä havainnoinnista systemaattisuudessa. Havainnointia voidaan käyttää muiden tiedonhankintatapojen, kuten haastatteluiden tukena tai itsenäisenä menetelmänä. Havainnoinnin käyttö tutkimusmenetelmänä mahdollistaa tutkimuksen toteuttamisen luonnollisessa ympäristössä. (Ojasalo ym. 2009, 103)

Tieteellinen havainnointi eli observointi on tieteellisen työskentelyn perusedellytys, joka merkitsee systemaattista tietojen kokoamista. Havainnointi on normaalia arkista havaitsemista tarkempaa ja sen tulee noudattaa systemaattista suunnitelmaa. (Heinonen ym. 2013, 35-36)

Ojasalon ym. (2009, 104) mukaan tutkimuksellisen havainnoinnin on oltava kaikissa tilanteissa mahdollisimman järjestelmällistä ja tulokset olisi tallennettava tai kirjattava muistiin. Kriittisin kysymys havainnoinnin suunnittelussa on havainnoijan rooli. Havainnoija voi olla täysin ulkopuolinen tai aktiivinen osallistuja, havainnoijan rooli pitääkin sovittaa tutkimuksen vaiheeseen sopivaksi.

Tutkimusmenetelmänä havainnointi on haasteellinen siitä näkökulmasta, että havainnoija vaikuttaa tutkittavaan joukkoon läsnäolollaan. Tätä voidaan lievittää esimerkiksi havaintoaikaa pidentämällä, mutta silloin haasteeksi voi muodostua havainnoijan sitoutuminen tutkittavaan joukkoon. (Ojasalo ym. 2009, 105)

Kuten Ojasalo ym. (2009, 106-107) kirjassaan toteavat, että havainnoinnilla kerätty materiaali ei ole ratkaisu tutkittavaan ongelmaan vaan dataa, jonka pohjalle tutkimus tehdään. Havainnoinnilla kerättyjen yksittäisten havaintojen yhdistäminen isommiksi kokonaisuuksiksi, josta voidaan tehdä johtopäätöksiä.

Tässä tutkimuksessa havainnointia käytetään sekä nykytilan arvioinnissa että uuden turvallisuus riskienhallintaprosessin toimivuuden arvioinnissa. Nykytilaa arvioitaessa havainnointi pyritään suorittamaan mahdollisimman laajan osaan toimintoja ja prosesseja, joissa tutkija näkee liityntäkohtia turvallisuuteen liittyvien riskien arvioinnille ja käsittelylle. Havainnointia suoritetaan tutkijan toimesta koko riskienarviointiprosessiin. Uuden prosessin osalta tutkija osallistuu tutkittavan joukon kanssa yhteisiin tilaisuuksiin, joissa uuden turvallisuus riskienhallinnan riskienarviointi mallia kokeillaan käytännössä.

2.3 Dokumenttianalyysi

Dokumenttianalyysissä kannattaa olla aina kriittinen ja tunnistaa dokumentin alkuperäinen käyttötarkoitus. On kuitenkin selvää, että työpaikalla tuotetut erilaiset dokumentit, kuten muun muassa muistiot, ohjeet, raportit ja www-sivut, sisältävät paljon hyödyllistä ja käyttökelpoista materiaalia. Dokumenttianalyysiä ei itsessään voida pitää kovinkaan kattavan tiedonhankintana, mutta sillä voidaan täydentää ja vahvistaa muualta hankitun tiedon oikeellisuutta. Dokumenttien käytön suhteen on myös aina muistettava huomioida niiden luottamuksellisuus. (Ojasalo ym. 2015, 43)

Tässä opinnäytetyössä dokumenttianalyysiä käytetään laajalti tutkittavan kohdeorganisaation vallitsevan nykytilanteen selvittämiseksi. Dokumenttianalyysi täydentää muita tiedonhankkimistapoja, kuten havainnointia. Tutkittavan dokumentit ovat pääosin sisäiseen käyttöön tehtyjä, luokiteltuja asiakirjoja, joissa ohjeistetaan ja kuvataan turvallisuusriskien toteuttamista kohdeyrityksessä.

2.4 Aivoriihi

Aivoriihi on luovan ongelmanratkaisun menetelmä, jossa joukko ihmisiä pyrkii ideoimaan uusia ratkaisuja tai lähestymistapoja johdettuna. Perinteisestä aivoriihestä on kehitetty suuri joukko erilaisia variaatioita ja sitä voidaan käyttää lukuisissa eri tilanteissa. Aivoriihen onnistumisen kannalta on tärkeää, että osallistujat tietävät riihen tavoitteet ja tuntevat rajat. Ensimmäisen vaiheen tärkein sääntö on, että ei saa arvioida tai tuomita ideoita, eikä esittäjän tarvitse niitä perustella. Valintavaiheessa ideoita tarkastellaan aivoriihen vetäjän ohjeiden mukaisesti, kriittisesti ja perustellen, sekä pyritään löytämään parhaat ideat. (Ojasalo ym. 2009, 145-146)

Tässä tutkimuksessa aivoriihi menetelmää sovelletaan työpajoissa, joissa asiantuntijat pyrkivät tunnistamaan ja analysoimaan nykyisiä sekä uusia turvallisuusriskejä.

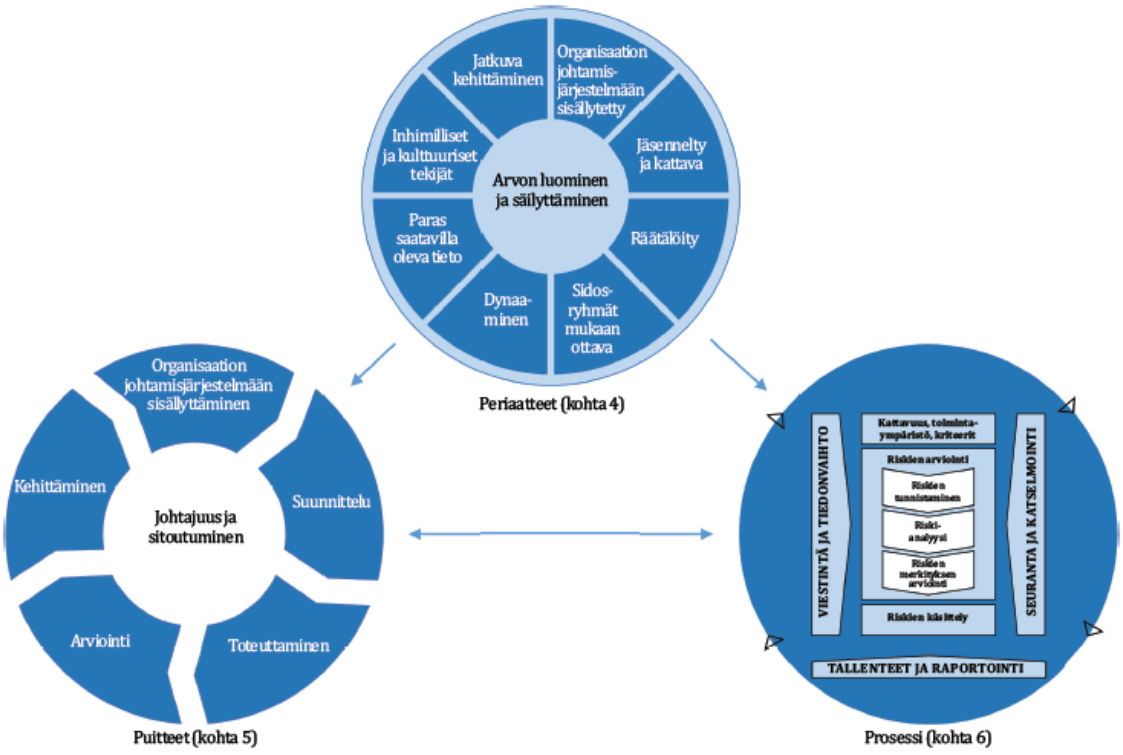
3 Riskienhallintajärjestelmä – ISO 31000

Tässä kappaleessa kuvataan ISO 31000 standardin vaatimukset pääpiirteittäin. Turvallisuusriskien hallintamallin sisäisen toimintaympäristön vaatimuksena on, että malli vastaa periaatteiltaan ja kattavuudeltaan ISO 31000 riskienhallinta standardin vaatimuksiin. ISO 31000 on kansainvälisesti yksi tunnetuimmista ja käytetyimmistä riskienhallinnan hallintajärjestelmistä.

Tämän kappaleen tarkoituksena kuvata kartoituksen jälkeen valitun riskienhallintajärjestelmän sisältö. Työn lopussa tehty hallintamalli pyrkii vastaamaan kaikilta osin tässä kappaleessa kuvattuihin ISO 31000 riskienhallinnan standardin vaatimuksiin. Työtä varten käytiin läpi myös Coso ERM, mutta ISO 31000 katsottiin vastaavan paremmin kohdeorganisaation tarpeisiin.

3.1 Yleistä

ISO 31000:2018 standardi määrittelee riskienhallinnan olevan organisaation kaikilla tasoilla tapahtuvaa iteratiivista toimintaa, jonka tarkoituksena on auttaa organisaatiota strategian määrittämisessä, tavoitteiden saavuttamisessa ja päätöksen teossa. Standardin mukaan riskienhallinta on keskeinen tekijä organisaation johtamisessa. Riskienhallinta sisältää organisaation koko toimintaympäristön, niin sisäisen kuin ulkoisenkin. ISO 31000 standardin mukainen riskienhallinta perustuu kuvassa 1 esitettyihin osatekijöihin, jotka voivat olla organisaation käytössä kokonaan tai osittain ja sellaisenaan tai muokattuna kuitenkin siten, että organisaation riskienhallinta on tehokasta ja johdettua. (ISO 31000:2018, 5)



Kuva 2: Periaatteet, puitteet ja prosessit (ISO 31000:2018, 5)

3.1.1 Periaatteet

Standardin mukaan riskienhallinnan päämääränä on organisaation arvon luominen ja säilyttäminen, riskienhallinnan tulisi tukea tavoitteiden saavuttamista ja parantaa suorituskykyä. Kuvassa 1 kuvatut periaatteet kuvaavat standardin mukaan vaikuttavan ja tehokkaan riskienhallinnan ominaisuuksia. Nämä periaatteet tulisivat olla perustana, kun halutaan toteuttaa riskienhallintaa ISO 31000 standardin mukaisesti. (ISO 31000:2018, 7)

Periaatteiden mukaan standardin mukaisen riskienhallinnan tulisi olla implementoitu ja tärkeä osa organisaation kaikkia toimintoja. Riskienhallinnan tulisi olla räätälöity organisaation toimintaan sopivaksi ja sen pitäisi olla jäsennelty toimintamalli, jotta arviointi olisi yhdenmukaista koko organisaatiossa. Sidosryhmien tulee olla osa riskienhallintaa, jotta koko organisaation ja ulkoisten vaikuttajien näkemykset ja havainnot saadaan osaksi sekä tietoisuutta riskienhallinasta kasvatettua. Riskienhallintaa on kehitettävä jatkuvasti kokemusten avulla ja riskienhallinta ottaa huomioon inhimilliset ja kulttuuriset tekijät. Standardin periaatteiden mukaisesti riskienhallinnan on otettava huomioon tietoon liittyvät epävarmuustekijät kuten tulevaisuuteen koskevan tiedon rajallisuus, riskienhallinnan onnistumisen osalta kriittistä onkin, että organisaatiolla on käytössään jatkuvasti paras saatavilla oleva tieto. (ISO 31000:2018, 8-9)

3.1.2 Puitteet

ISO 31000 standardin mukaan puitteiden tavoite on yhdistää riskienhallinta osaksi organisaation toimintaa. Se kuinka vaikuttaa riskienhallinta on riippuvainen siitä, kuinka hyvin organisaatio onnistuu sisällyttämään riskienhallinnan osaksi päätöksentekoa ja johtamista. Standardi korostaa tässä ylimmän johdon tukea kriittisenä onnistumisen tekijänä, jotta riskienhallinta saadaan osaksi johtamisjärjestelmää. Riskienhallinnan puitteissa olisi otettava huomioon nykyiset riskienhallinnan käytänteet ja arvioitava sen puutteet alettaessa soveltamaan sekä muokattava ne organisaatiolle sopiviksi. (ISO 31000:2018, 9)

Organisaation ylimmän johdon vastuulla on varmistaa organisaation toimintaa vastaavan riskienhallinnan organisoinnista ja varmistaa riskienhallinnan toiminnan vaikuttavuus. Riskienhallinnan toimintaperiaatteista tulisi viestiä koko organisaatiolle, esimerkiksi riskienhallintapolitiikan tai vastaavan dokumentin muodossa sekä varmistaa organisaation kaikille tasoille riittävä osaaminen ja resurssit riskienhallinnan toteuttamiseksi. (ISO 31000:2018, 10)

Puitteiden määrittelyssä ISO 31000 standardi painottaa riskienhallinnan sisällyttämistä organisaation johtamisjärjestelmään ja hallintotapaan. Sisällyttämällä riskienhallinta osaksi hallintotapaa, riskienhallinta saadaan osaksi organisaation strategista työtä, eikä se toimi toiminnasta irrallisena. (ISO 31000:2018, 10-11)

ISO 31000 standardin mukaisen riskienhallintajärjestelmän puitteiden suunnittelussa on tunnistettava organisaation ulkoiseen ja sisäiseen toimintaympäristöön vaikuttavat tekijät ja arvioitava niiden vaikutus toiminnalle. Ulkoisen toimintaympäristön tarkastelussa on otettava huomioon kansalliset ja kansainväliset velvoitteet sekä ympäristössä vaikuttavat muut yhteiskunnalliset tekijät. Myös toimittajasuhteet sekä verkostot ja riippuvuus niiden toiminnasta vaikuttaa suunniteltaessa riskienhallintajärjestelmän puitteita. Sisäisen toimintaympäristön tarkastelussa vaikuttavia tekijöitä ovat esimerkiksi organisaation arvot, strategiset tavoitteet sekä organisaatiorakenne. Myös yrityksen toimintaa liittyvät teknologiset ja resurssikyvykkyydet tulisi ottaa huomioon tarkastelussa. (ISO 31000:2018, 11)

Riskienhallinnan puitteiden toteuttamisen onnistuminen vaatii organisaatiolle ja sidosryhmille viestittyä toimintasuunnitelmaa, jonka avulla varmistetaan riskienhallinnan päätöksentekoprosessien toteutumien kaikilla organisaation tasoilla. Organisaation olisi myös säännöllisesti arvioitava puitteiden vaikuttavuutta, jotta riskienhallinta kykenee tukemaan tavoitteita muuttuvassa toimintaympäristössä. (ISO 31000:2018, 11)

3.1.3 Prosessi

Riskienhallintaprosessiin kuuluu riskien arvioinnin ja käsittelyn lisäksi viestintää sidostyhmien kanssa, jatkuvaa katselmointia sekä raportointia. Toimintaympäristön määrittelyn tulee olla osa toimintaa kaikilla tasoilla ja prosessi on kyettävä jalkauttamaan jatkuvaksi osaksi

organisaation toimintaa. Prosessin ja sen tulosten olisi ohjattava organisaation johtoa sekä päätöksentekoa ja sitä pitäisi pystyä hyödyntämään organisaation kaikilla tasoilla tehtävän päätöksenteon tukena. (ISO 31000:2018, 14)

Riskienhallintaprosessin toimivuuden ja vaikuttavuuden kannalta kriittisenä tekijänä toimii viestintä. Viestinnän avulla riskienhallintaprosessin päätöksiä ja riskitietoisuutta saadaan kasvatettua sekä sen avulla varmistetaan eri näkökulmien mukana olo työssä. (ISO 31000:2018, 14-15)

Riskienhallintaprosessin määrittelyn tavoitteena on luoda organisaation toimintaan suhteutettu käsittelymalli, joka ottaa huomioon kattavuuden eli millä tasoilla riskienhallintaprosessia toteutetaan milläkin tavalla. Sen lisäksi on määriteltävä se toimintaympäristö, jonka puitteissa prosessia toteutetaan. Riskienarviointiprosessin alussa on myös määritettävä riskikriteerit, joiden perusteella riskien merkittävyyttä ja vaikutusta tavoitteisiin arvioidaan. Riskikriteereiden tulisi olla johdonmukaiset ja kyseiseen kohteeseen räätälöidyt sekä niiden tulee olla yhteensopivat riskienhallinnan puitteiden kanssa. (ISO 31000:2018, 16)

ISO 31000 standardin mukaisesti riskien arviointi on prosessi, joka pitää sisällään kolme vaihetta: riskien tunnistamisen, riskianalyysin ja riskin merkityksen arvioinnin. Riskien tunnistamisen voi käyttää erilaisia menetelmiä, olennaista olisi tunnistaa ne riskit, jotka voivat vaikuttaa positiivisesti tai negatiivisesti organisaatiota saavuttamaan asettamiaan tavoitteita, huolimatta siitä ovatko riskin lähteet organisaation vaikutuksen piirissä. Riskianalyysin avulla organisaatio yrittää tunnistaa riskin ominaisuudet ja sen aiheuttamien epävarmuustekijöiden vaikutukset. Analyysi voidaan tehdä riskistä riippuen laadullisena tai määrällisenä, olennaista on tuottaa riittävä näkemys päätöksenteon tueksi. Päätöksenteko toteutetaan ISO 31000 standardin mukaan arviointi vaiheessa, jolloin analyysin pohjalta tehdään päätökset riskin vaatimille mahdollisille toimenpiteille. (ISO 31000:2018, 17-18)

Riskien käsittely on toistuva prosessi, jonka tarkoituksena on arvioida riskien käsittelyn vaikuttavuutta sekä päätettävä riskien hyväksynnästä. Riskien käsittelyn tavoite on löytää kutakin riskiä resursseiltaan vastaava tapa hallita riskiä. Riskejä voidaan käsitellä monella eri tapaa, kuten poistamalla riskiä aiheuttava työ, ottamalla riski tai jakamalla riskin vaikutusta esimerkiksi vakuutuksella. Koska riskienhallinta ei ole organisaation prosesseista erillinen komponentti, olisi riskienkäsittelysuunnitelmat yhdistettävä yleiseen johtamismalliin. (ISO 31000: 2018, 18-19)

ISO 31000 standardin mukaan jatkuva seuranta ja katselmointi, jonka on oltava osa kaikkia riskienhallintaprosessin osa-alueita, varmistaa ja parantaa prosessin laatua ja vaikuttavuutta. Tämän lisäksi prosessi ja sen tulokset dokumentoidaan, jonka avulla osoitetaan ylimmälle johdolle prosessin toimivuus sekä annetaan tietoa päätöksenteon tueksi. (ISO 31000:2018, 19-20)

3.2 Muut hallintajärjestelmät

Coso ERM on kansainvälisesti tunnetuin riskienhallintajärjestelmä ISO 31000 -standardin ohella. COSOn ensimmäinen versio on esitelty jo vuonna 2004 ja se on suunnattu erityisesti isoille organisaatioille. COSO ERM jakautuu kahteen selkeään osaan: ensimmäisessä kuvataan periaatteet, tavat ja viitekehys, toisessa osassa kuvataan menetelmät. (Ilmonen ym 2010, 31-32)

AS/NZS 4360:2004 on Australian ja Uuden-Seelannin viranomaisten julkaisema standardi riskienhallinnalle. Tätä voidaan pitää hieman käytännönläheisempänä kuin COSO ERM-mallia ja AS/NZS onkin toiminut mallina ISO 31000 -standardille, jota voidaan pitää sen päivitettynä versiona. (Ilmonen ym. 2010, 32)

4 Tutkimuksen empiirinen osio

Opinnäytetyössä asetettiin kaksi varsinaista tutkimuskysymystä: ”Millä tavoin turvallisuusriskien hallinta on osana organisaation toimintaa?" ja "Millä tavoin toiminnalle asetetut vaatimukset ohjaavat turvallisuusriskien hallintaa?". Nykytilaa arvioitiin havainnoimalla organisaation toimintaa sekä hallintamallia. Lisäksi pyrittiin vertailemaan käytettyjä malleja suhteessa toiminnalle asetettuihin vaatimuksiin. Konstruktiivisen tutkimuksen periaatteiden mukaan tavoitteena oli ratkaista ongelma käytännönläheisesti luomalla uutta rakennetta ja tuoda uutta teoreettista tietoa ratkaistavasta aiheesta liiketoiminnalle

4.1 Riskienhallinnan nykytila

Riskienhallinta on yksinkertaisuudessaan yrityksen toiminnan varmistamista sekä sidosryhmien odotusten ja vaatimusten täyttämistä. Riskienhallinnan keinoin suojataan omistajien sijoitusten arvoa ja täytetään esimerkiksi viranomaisten vaatimukset toiminnalle. Riskienhallinnan on oltava integroitu osa organisaation toimintaa ja sen tulee olla johdettu yrityksen arvoista sekä strategisista tavoitteista. (Ilmonen, Kallio, Koskinen & Rajamäki 2010, 33-34)

Nykypäivänä riskienhallinta pitää sisällään negatiivisilta tapahtumilta suojautumisen lisäksi myös riskien ja riskien ottamisen positiivisen puolen. Liiketoiminta edellyttää ja liiketoiminta itsessään on riskien ottamista, mutta riskienhallinnan kautta voidaan myös tunnistaa ja arvioida liiketoiminnan mahdollisuuksia. (Ilmonen ym. 2010. 17-18)

Elisan riskienhallinnan yhtenä keskeisenä tavoitteena on yhdessä sisäisen valvonnan kanssa varmistaa taloudellisten raporttien oikeellisuus ja lainmukaisuus. Riskit ovat jaettu yleisten riskienhallinnan periaatteiden mukaisesti strategisiin, operatiivisiin ja vakuutettavissa oleviin riskeihin sekä rahoitusriskeihin. Riskien tunnistaminen ja analysointi toteutetaan osana suunnitteluprosessia ja sen tarkoituksena on tunnistaa tavoitteiden saavuttamista vaarantavat tapahtumat. Riskienhallinnan riittävyyttä ja asianmukaisuutta valvoo hallituksen tarkastusvaliokunta. (Elisa 2018c)

Elisan Yritysvastuuraportin (2018) mukaan riskienhallinta on integroitu osaksi liiketoimintaa ja siihen vaikuttavat riskit tunnetaan ja niihin vaikutetaan. Yritysvastuun yhdeksi keskeiseksi riskiksi on nostettu henkilötietojen vuotaminen ja niihin kohdistuva tietojenkalastelu tai tietomurrot.

Tunnistamalla toimintaympäristön mahdollisuudet ja niiden esteet, organisaatiolla on mahdollisuus liiketoiminnan ja kannattavuuden kasvattamiseen. Kannattavuuden kasvattamisen edellytyksenä on, että organisaatio on tunnistanut sisäisiin prosesseihin ja toimintaympäristöön vaikuttavat riskit laatiessaan strategiaa. (Juvonen ym. 2014, 15)

Yrityksen riskienhallintaan vaikuttavat niin sisäiset kuin ulkoisetkin vaatimukset. Sisäisiä vaatimustekijöitä ovat yrityksen määrittelemät arvot, visio, missio ja strategia. Riskienhallinnan keinoin tuetaan strategisten tavoitteiden toteutumista varmistamalla, että otetut riskit ovat organisaation riskinkantokykyyn rajoissa. Ulkoiset vaatimukset riskienhallinnan tulevat käytännössä lainsäädännöstä ja asiakasvaatimuksista. Nämä vaatimukset voivat olla toimialaan liittyviä tai yleistä hallintotapaa koskevia, organisaation kannalta tärkeintä on tuntea omaan toimintaan kohdistuvat velvoitteet, joiden toteumista tuetaan riskienhallinnan keinoin. (Ilmonen ym. 2010, 21-23)

Kohdeorganisaatio toimii telepalvelujen tarjoajana sekä sähköisten tieto- ja viestintäpalveluiden tuottajana, toimintaan kohdistuu velvoittavia laki ja määräys velvoitteita. Valmiuslaki 1552/2011 ja laki sähköisen viestinnän palveluista 917/2014 edellyttävät organisaatiota tunnistamaan riskit ja suunnittelemaan toiminnan jatkuvuus normaaliolojen häiriötilanteissa sekä valmiuslain 9 luvun mukaisissa tilanteissa. (Finlex 2011; Finlex 2014)

Kansallinen riskiarvio 2018 -julkaisussa todettiin, että viestintäverkkoihin ja -palveluihin kohdistuvat uhat ovat kansallisesti kriittisiä monella eri sektorilla sekä yhteiskunnan että yritys-elämän näkökulmasta. Viestintäverkkoihin ja -palveluihin kohdistuu raportin mukaan monenlaisia tunnistettuja sekä uusia tunnistamattomia uhkia, jotka liittyvät esimerkiksi luonnonilmiöihin, työmarkkinatilanteeseen tai kybermaailman ilmiöihin. Raportissa arvioitiin todennäköisyyden trendin kasvavan. (Sisäministeriö 2019)

Epävarmuus on osa ihmisten ja organisaatioiden kaikkea toimintaa. Kaikkeen päätöksentekoon kuuluu epävarmuus ja epätietoisuus päätöksen seurauksista, ne voivat olla kielteisiä tai myönteisiä. Niin yksilön kuin yrityksenkin on otettava riskejä toiminnassaan, joiden hallitsemista pyritään parantamaan suunnittelulla. (Kuusela & Ollikainen 2005, 15-16)

Nykypäivänä riskienhallinnasta puhuttaessa, pitäisi aiempaa laajemmin ymmärtää sen olevan toiminnan ohjauksen prosessi, jonka tavoitteena on parantaa organisaation mahdollisuuksia saavuttaa sille asetetut tavoitteet. (Lanne & Heikkilä 2016, 4-5)

Kohdeorganisaation turvallisuusriskien hallinnasta julkisista lähteistä saatujen tietojen perusteella voidaan havaita kohdeorganisaatiossa puutteita kokonaisvaltaisen riskienhallinnan toteuttamisessa. Turvallisuusriskien osalta maininta Yritysvastuuraportissa ilmentää mielestäni sitä, että varsinkin turvallisuusriskien hallinnan tärkeyttä on jatkossa korostettava. Elisa toimii sellaisella liiketoiminta-alueella, johon kohdistuu merkittäviä turvallisuuteen liittyviä riskejä, kuten tietoturvan, tietosuojan ja toiminnan häiriöttömyyden osalta, joiden vaikutukset liiketoimintaan voivat olla kriittisiä.

Sisäisen dokumentaation läpikäynti ja kohdeorganisaatiossa tehty havainnointi tukevat julkisista lähteistä saatuja tuloksia ja johtopäätöksiä. Turvallisuusriskien hallintaa tehdään satunnaisesti erilaisten projektien yhteydessä. Esimerkiksi EU:n yleisen tietosuoja-asetuksen voimaantulon yhteydessä tehtiin organisaatiossa kattavasti tietosuojariskien tunnistamista ja arviointia, mutta tässä yhteydessä ei pyritty aktiivisesti tunnistamaan muita turvallisuusriskejä, ja jos niitä tunnistettiin niiden käsittely ei ollut määrämuotoista eikä kaikkia niistä käsitelty ollenkaan.

4.2 Riskienhallinnan tavoitteet

Ilmosen ym. (2010, 19) mukaan riskienhallinnan yksi tärkeimpiä päämääriä on löytää riskienhallinnan optimaalinen taso, jossa riskien tunnistamisen ja analysoinnin avulla löydetään ne asiat, joihin kannattaa panostaa. Optimoimalla resurssit, kustannukset ja pääoma, pyritään löytämään asiat, joiden avulla organisaatio saa maksimaalisen hyödyn suhteessa panostukseen.

Riskienhallinnan ja organisaation turvallisuustoiminnan tavoitteiden on oltava sidottu ja samansuuntaiset kuin organisaation muut tavoitteet sekä strategia. Tuotanto- ja palveluprosessin tavoitteena on tuottaa asiakkaille lopputuotoksia, joita he odottavat. Riskejä on arvioitava aina siitä näkökulmasta, että riskin toteutumisen seurauksena prosessi ei tuota asiakkaalle toivottua tuotosta ja tästä syntyy organisaatiolle vahinkoa. (Leppänen 2006, 175-176)

Havainnoin ja dokumentaatio analyysin perusteella voidaan todeta, että nykyiset turvallisuusriskien hallinnan tavoitteet eivät vastaa riskienhallinnan yleisiä periaatteita ja suositeltuja käytänteitä, kun verrataan toimintaa teoreettiseen viitekehykseen asiasta. Selkeänä puutteena voidaan lisäksi pitää turvallisuusriskien hallinnan tämän hetkisten tavoitteiden ja toiminnan löyhää tai olematonta yhteyttä organisaation yleisiin strategisiin tavoitteisiin ja päämääriin.

4.3 Riskienhallinnan sudenkuopat

Jos turvallisuustoiminnan ja riskienhallinnan tavoitteet eroavat muun organisaation tavoitteista ja asetusta suunnasta. on vaarana, että turvallisuustoiminnan merkityksestä organisaatiolle on ristiriitaisia näkemyksiä. (Leppänen 2006, 176)

Kokonaisvaltaisen riskienhallinta prosessin suunnittelun lähtökohtana on oltava yhtenäisen ja yhteismitallisten käytäntöjen toteuttaminen kaikissa organisaation osissa. Tehokas käyttöönotto vaatii ylemmän johdon edustajan sekä selkeät vastuut. (Leino, Steiner & Wahlroos 2005, 135)

Riskienhallinnan kehittämisen onnistuminen on kiinni muun muassa organisaation johtamisen kypsyydestä, riittävistä resursseista sekä selkeästä raportoinnista. Jos organisaation kypsyystaso ei ole korkea, on suositeltavaa aloittaa vain negatiivisten riskien hallinnasta ja jättää mahdollisuuksien hallinta pois. (Ilmonen ym. 2010, 48-59)

Douglas W. Hubbard (2009, 76-77) listaa kirjassa The Failure of Risk Management useita syitä riskienhallinnan epäonnistumiselle. Yhtenä keskeisenä ongelmana hän pitää riskin ja riskienhallinnan konseptia sekä terminologiaa. Jo sana riski voi tarkoittaa eri ihmisille hyvin erilaisia asioita. Lisäksi hän pitää ongelmallisena, että riskien arviointi perustuu edelleen pitkälti ihmisten arvioihin epävarmuudesta. Myös riskienhallinnan eräänlainen eristyneisyys on vaarana riskienhallinnan toimivuudelle, organisaation sisällä tai sidosryhmille ei jaeta riittävästi tietoa, vaan samoja riskejä käsitellään useassa paikassa.

Kohdeorganisaation turvallisuusriskien hallinnan nykytila ja kypsyys ovat sillä tasolla, että päivitetty hallintamalli ei tule vastaamaan mahdollisuuksien hallintaan, vaan toiminnan parantamisen ensimmäisessä vaiheessa on suositeltavaa keskittyä vain haitallisten tapahtumien tunnistamiseen ja analysointiin. Myöskin yhtenäisen terminologian luomiseen sekä riskien vaikutusten yhteismitallistamiseen on käytettävä resursseja. Lisäksi on kehitettävä metodeja, joiden avulla voidaan paremmin varmistaa arvioinnin yhtenäisyys.

4.4 Keskeisimmät löydökset

Nykytilan tutkiminen toteutettiin havainnoimalla kohdeorganisaation toimintaa sekä analysoimalla turvallisuusriskien hallinnan nykyistä dokumentaatiota. Lisäksi analysoitiin nykyistä riskirekisteriä sekä siihen liittyvää prosessia ja vuosikelloa. Dokumentteja analysoitaessa pyrittiin niistä tunnistamaan sekä positiivisia asioita sekä puutteita suhteessa ISO 31000 standardiin. Analysoidut dokumentit olivat muun muassa turvallisuusriskienhallinnan periaate, Yritysturvallisuuden riskirekisteri, riskikäsittelyiden ja johdon katselmuksien muistioita sekä työkalupohjia. Havainnointia toteutettiin useissa riskien tunnistamisen ja arvioinnin työpajassa, turvallisuusriskien johdon katselmus -tilaisuudessa sekä asiantuntijoiden kanssa pidetyissä workshopeissa. Taulukkoon 1 on koottu tutkimuksessa tehtyjen havaintojen ja dokumenttianalyysin perusteella tunnistetut puutteet tai ongelmat nykyisessä toimintamallissa.

Tutkimuksen keskeisimmät löydökset:

1. Turvallisuusriskienhallinnan periaate ei vastaa kattavuudeltaan toiminnalle asetettuja sisäisiä ja ulkoisia vaatimuksia eikä riskienhallinnan yleisiä parhaita käytänteitä.

2. Muutokset organisaation toimintaympäristössä asettavat uusia vaatimuksia organisaation turvallisuustoiminnalle sekä riskienhallinnalle.

3. Nykyinen toiminta ei täytä ISO 31000 riskienhallinta standardin ja/tai alan parhaiden käytäntöjen suosituksia riskienhallinnan periaatteiden eikä riskien arvioinnin määrämuotoisuuden ja säännöllisyyden osalta.

Turvallisuusriskien hallinta ja prosessin toteuttaminen on vastuutettu usealle taholle eikä sen toteuttaminen vastannut toiminnalle asetettuja tavoitteita. Turvallisuusriskien arviointia ja analysointia tehtiin satunnaisesti eri turvallisuuden osa-alueiden osalta, mutta systemaattinen ja yhtenäinen työ on puuttunut. Esimerkiksi tietosuoja-asetuksen voimaantulon aikoihin on tietosuojaan ja tietojen käsittelyyn liittyvä riskien tunnistamista ja arviointia tehty systemaattisesti koko organisaatiossa, mutta samalla on jäänyt tunnistamatta muut turvallisuuteen liittyvät riskit.

Tämän lisäksi turvallisuusriskien hallinnan prosessi on jättänyt huomiotta omaisuuden arvon toiminnalle. Riskit on arvioitu samalla tavalla riippumatta riskin kohteesta ja sen vaikutuksesta koko organisaation liiketoiminnalle. Näin ollen riskienhallinnan ei voida todeta olevan kovinkaan tehokasta, tuloksellista ja vaikuttavaa suhteessa organisaation toimintaan ja strategisiin tavoitteisiin.

Aihe	Havaittu ongelma	Ehdotettu toimenpide
Periaate / politiikka	Turvallisuusriskienhallinnan periaate ei täytä kattavuudeltaan ISO 31000 vaatimuksia eikä se ole enää vastuiden osalta ajantasainen	Päivitetään periaatedokumentti (Liite 1)
Säännöllisyys	Turvallisuusriskeihin ja niiden hallintaan liittyvät toimenpiteet eivät ole säännöllisiä eikä niiden toteutumista seurata	Luodaan vuosikello, joka liitetään osaksi hallintamallia
Johdon sitoutuminen	Ei ollut selkeästi havaittavissa, kenelle raportoidaan ja kenen vastuulla on	Päivitetty periaate hyväksytetään turvallisuuden johtoryhmällä ja

	turvallisuusriskien informoiminen organisaation johdolle.	hallintamalliin kirjataan johdon vastuut hallinnan osalta.
Sidottavuus strategiaan	Turvallisuusriskien hallinta ei ole sidoksissa organisaation strategiaan. Esimerkkinä 5G, joka näkyy kohdeorganisaation strategiassa, mutta ei turvallisuustoiminnassa tai riskienhallinnassa	Hallintamallin toimenpiteiden avulla pyritään turvallisuusriskien hallintaa työstämään aiempaa enemmän yhteistyössä liiketoiminnan kanssa, jonka avulla toimintaa saadaan sidottua organisaation tavoitteiden tueksi.
Vastuut	Turvallisuusriskien osalta määrittelemättä kenen vastuulla toimintaan liittyvien tehtävien suorittamien ja seuranta on.	Kuvataan periaate dokumentissa ylätason vastuut ja hallintamalliin päivitetään operatiivisen riskienhallinnan tehtävät esimerkiksi *RACI-mallin mukaisesti.
Terminologia	Puutteita yhtenäisessä terminologiassa, joka voi aiheuttaa väärinkäsityksiä.	Hallintamalli sekä työohjeet kirjoitetaan samalla terminologialla sekä riskien arviointiin liittyvien vaikuttavuuden ja todennäköisyyden kuvauksia selkeytetään.
Kattavuus	Turvallisuusriskien arviointi ei havaintojen mukaan kata kaikkia turvallisuuden osa-alueita.	Hallintamallin jalkautuksen osana tunnistettava kaikki liittyvät turvallisuuden osa-alueet ja niiden osalta raportointi vaatimus määritettävä.
Prosessi	Turvallisuusriskien prosessi ei ole yhteismitallinen eikä selkeästi kuvattu, nykyinen	Prosessi kuvattava kaikkien vaiheiden osalta ja dokumentoitava selkeästi.

	periaate kuvaa vain lyhyesti riskien tunnistamista ja käsittelyä.	Yhteisten työkalujen puute hidastanut toimintaa, joten niiden työstämistä suositeltava.
Jatkuva parantaminen	Turvallisuusriskien osalta työskentely ei ole suunniteltua eikä selkeää suunnitelmaa sen kehittämiselle ollut.	Hallintamallin vastattava ISO 31000 standardin mukaisesti jatkuvan parantamisen malliin.

Taulukko 1: Tutkimuksessa havaitut puutteet

(*RACI-malli on alun perin projektinhallintaan liittynyt malli, jota voidaan hyödyntää myös riskienhallinnan toteuttamisessa. R=responsible eli vastuullinen, A=accountable eli vastuussa oleva, C=consulted eli neuvoja ja I=informed eli tiedotettava.)

Tutkimuksessa tehtyihin havaintoihin sekä asetettuihin vaatimuksiin pohjautuen, tässä opinnäytetyössä päätettiin toteuttaa ehdotus uudesta turvallisuusriskien hallintamallista. Kappaleessa 5 on kuvattu päivitetty turvallisuusriskien hallintamalli, jonka avulla voidaan organisaation toiminta saattaa vastaamaan toiminnalle asetettuja vaatimuksia sekä pääosiltaan ISO 31000 -standardin riskienhallinta prosessille kuvaamia parhaita käytänteitä.

5 Turvallisuusriskien hallintamalli

Turvallisuusriskien hallintamalli toteutettiin vastaamaan aiemmin tässä tutkimuksessa todettuja puutteita organisaation nykyisessä toiminnassa. Päivitetyn mallin avulla organisaation turvallisuusriskien hallinnan on, riittävien resurssien ja johdon sitoutumisen avulla, mahdollista saavuttaa toiminnalle asetetut sisäiset ja ulkoiset vaatimukset.

5.1 Periaatteet

Turvallisuusriskien hallinta ja sen vaatimat toimenpiteet on yhdistettävä turvallisuustoiminnan vuosikelloon ja riskienhallinnan on oltava kiinteä osa kaikkea turvallisuustoimintaa. Riskienhallinnan ja riskien käsittelyn kautta turvallisuustoiminnalle saadaan vaikuttavat ja organisaation strategisia päämääriä tukevat tavoitteet.

Turvallisuusriskien hallinta on kaikissa tilanteissa suhteutettava toiminnan tasoon ja kriittisyyteen. Myöhemmin kuvatussa riskienhallinnan prosessissa kuvataan tarkemmin, millä tavoin suojattavan omaisuuden kriittisyys on huomioitava riskien hallinta työssä.

Turvallisuusriskien hallinnan on katettava kaikki organisaation turvallisuuden osa-alueet, siltä osin kuin ne ovat turvallisuusyksikön vastuulla. Turvallisuusriskien hallinnan kattavuutta ja toimivuutta valvoo sisäinen tarkastus.

Turvallisuusriskien hallintamallin toimintaa on mitattava, jotta varmistutaan hallintamallin suorituskyvystä suhteessa organisaation toimintaan. Lisäksi hallintamallin työkaluja ja metodeja on arvioitava vuosittain, jotta se pystyy vastaamaan muuttuviin ja kehittyviin riskifaktoreihin.

Hallintamallin ja toiminnan on huomioitava kaikissa vaiheissa sen toimintaan vaikuttavat ulkoiset ja sisäiset sidosryhmät sekä riskienhallintaan vaikuttavat organisaation kulttuurilliset tekijät.

Turvallisuusriskien hallinnassa on huolehdittava, että sen käytössä on jatkuvasti paras mahdollinen tieto organisaation sisäisistä asioista, joilla voi olla vaikutusta sekä tunnistettava nykyiset ja uudet uhkatekijät ulkoisesta ympäristöstä.

PESTLE-mallia voidaan käyttää riskienarvioinnin useassa vaiheessa kuten esimerkiksi riskien tunnistamisen apuna. Mallia voidaan hyödyntää myös toimintaympäristön hahmottamiseen sekä toimintaympäristössä tapahtuvien muutosten ja niiden vaikutusten arvioinnissa. (Valtiovarainministeriö 2017b).

Tässä hallintamallissa alla kuvattua PESTLE-mallia käytetään toimintaympäristön mahdollisimman laajan käsityksen saamiseksi sekä siitä aiheutuvien vaikutusten minimoimiseksi. Kohdeorganisaation toimialasta johtuen on esimerkiksi kriittistä tunnistaa kansainvälisen ja kansallisen regulaation vaikutukset toiminnalle riittävän hyvissä ajoin, jotta niiden mahdollisesti aiheuttamiin muutoksiin pystytään valmistautumaan.

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

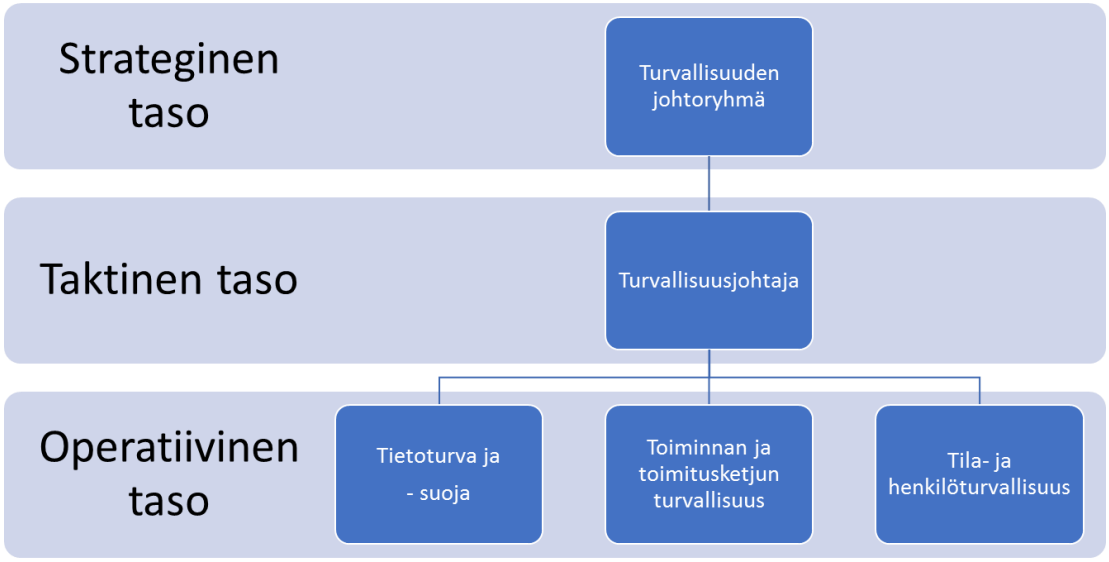
Kuva 3: PESTLE-malli (Valtiovarainministeriö 2017b)

5.2 Puitteet

Turvallisuusriskien hallintajärjestelmän puitteet määrittävät hallintajärjestelmän vastuut, toimintaympäristön sekä viestinnän. Tämän lisäksi puitteet osiossa kuvataan hallintajärjestelmän osalta keskeiset työkalut ja metodit yhdenmukaiselle toiminnalle.

5.2.1 Vastuut

Turvallisuusriskien hallinnan ja käsittelyn vastuut toteutetaan normaalin turvallisuuden johtamismallin mukaisesti. Turvallisuuden johtoryhmä toimii ylimpänä hallinnollisena toimijana, jonka tiedoksi ja päätettäväksi viedään strategisen tason turvallisuus riskit. Tai sellaiset turvallisuusriskit, joiden katsotaan voivan aiheuttaa merkittävää vahinkoa organisaation toimintakyvylle. Turvallisuusjohtaja omistaa turvallisuusriskien hallinnanprosessin ja vastaa sen toimivuudesta koko organisaation riskienhallinasta vastaavalle rahoitusjohtajalle. Turvallisuuden eri osa-alueiden vastuulliset vastaavat riskienhallinnan toteuttamisesta oman vastuualueensa osalta.



Kuva 4: Turvallisuusriskien hallinnan vastuut

Operatiivisella tasolla käsitellään yksittäisiä riskejä sekä tehdään päätöksiä operatiivisen tason riskien hallitsemiseksi, vähentämiseksi tai poistamiseksi. Operatiivisen tason toimijat tuottavat seuraavalle tasolle koostettuja, taktisen tason, riskejä, jotka voivat pitää sisällään useampia alemman tason yksittäisiä riskejä. Taktisella tasolla käsitellään turvallisuusjohtajan toimesta taktisen tason riskikokonaisuuksia, jotka ovat tietyn osa-alueen alta koostettuja. Taktisen tason tarkoituksena on suodattaa johdolle organisaation strategian ja liiketoiminnan kriittisyyden kannalta tärkeiden riskikokonaisuuksien nostamista strategiselle tasolle. Taktisella tasolla ei tunnisteta uusia riskejä tai arvioida olemassa olevien riskien vaikutuksia, vaan käsitellään niin sanottujen riskilausuntojen kautta isompia kokonaisuuksia. Riskilausunto voi pitää sisällään useita, jopa kymmeniä operatiivisen tason riskejä, joiden yhteenlaskettu

vaikutus muodostaa riskilausunnon luokituksen. Riskilausuntoa voidaan pienentää käsittelemällä siihen kuuluvia operatiivisen tason yksittäisiä riskejä. Strategiselle tasolle koostetaan riskilausuntojen pohjalta matriisiin perustuva esitys organisaation strategisiin tavoitteisiin vaikuttavista asioista. Tämän, eräänlaisen johdon katselmuksen, tarkoituksena on tuottaa ylimmälle johdolle tietoa organisaation toiminnan kannalta oleellisten turvallisuustilanteeseen vaikuttavien asioiden tilanteesta sekä auttaa ylintä johtoa kohdistamaan resursseja oikeisiin paikkoihin.

Riskienhallinnan yleisiin periaatteisiin kuuluu, että vaikka yrityksen toimitusjohtaja sekä viime kädessä hallitus ovat vastuussa riskienhallinnasta ja sen toteuttamisesta sekä tuloksista, niin riskejä hallitaan ja riskit omistetaan operatiivisella tasolla. Organisaatio, jossa on vahva riskienhallintakulttuuri, jokainen työntekijä vastaan omalta osaltaan riskienhallinnan toteuttamisesta. (Ilmonen ym. 2010, 56)

5.2.2 Sisäinen ja ulkoinen viestintä

Kokonaisvaltaisen turvallisuusriskien hallintamallin mahdollistaa riittävä viestintä ja tiedonvaihto. Viestinnän on oltava riittävän kattavaa ja konkreettista, jotta sidosryhmien on mahdollista osallistua ja tukea riskienhallinta työtä. Riittävällä viestinnällä myös varmistetaan riskienhallinnan tunnettavuus organisaatiossa sekä kehitetään myönteistä riskienhallintakulttuuria.

Turvallisuusriskejä käsiteltäessä ja arvioitaessa on viestittävä riittävän suuren joukon sidosryhmiä kanssa, jotta saadaan kattava kuva riskin toteutumisen mahdollisista vaikutuksista suojattavalle kohteelle sekä riskin toteutumismahdollisuuksista organisaation eri osa-alueilla.

5.2.3 Riskilajit

Riskejä voidaan luokitella monella eri tavalla. Tässä työssä riskit jaotellaan neljään luokkaan: strategisiin, taloudellisiin, operatiivisiin ja vahinkoriskeihin. Turvallisuusriskit sijoittuvat pääsääntöisesti operatiivisiin riskeihin, mutta osa turvallisuusriskeistä on myös luonteeltaan vahinkoriskejä.

Arto Suominen (2005, 149) kirjoittaa, että turvallisuusriskeistä puhuttaessa normaaliin riskitarkasteluun otetaan osaksi myös yhteiskunnan turvallisuustarpeet. Globalisoituvassa maailmassa on entistä tärkeämpää tunnistaa yritystä kohtaavat turvallisuutta vaarantavat uhkatekijät. Turvallisuusriskien tarkastelussa rikolliset tekijät, ulkoiset ja sisäiset, ovat usein keskeisessä roolissa turvallisuusriskejä käsiteltäessä.

Riskilaji	Kuvaus

Strategiset riskit	Strategiset eli liiketoimintariskit ovat strategisen tason riskejä, jotka voivat kohdistuvat organisaation strategisiin tavoitteisiin, toimintaympäristöön ja markkinoihin. Riskit voivat myös liittyä organisaation kykyyn kehittää tavoitteiden kannalta kriittisiä kyvykkyyksiä esimerkiksi uusiin teknologioihin liittyen.
Taloudelliset riskit	Taloudelliset riskit ovat yrityksen rahaprosesseihin liittyvät uhat. Taloudellisiin riskeihin luokitellaan ne riskit, jotka kohdistuvat maksuvalmiuteen, korkoihin ja luottoihin, lisäksi tähän luokkaan kuuluvat organisaation taloudelliseen raportointiin liittyvät tekijät.
Operatiiviset riskit	Organisaation päivittäiseen toimintaan liittyvät riskit ovat operatiivisia riskejä. Näihin kuuluvat sisäisten prosessien, henkilöstön ja järjestelmien mahdollisesti aiheuttamista vahingoista. Operatiivisille yhteistä on se, että niiden aiheuttaman riskin toteutuminen aiheuttaa organisaatiolle kriisitilanteen kuten esimerkiksi toiminnan keskeytyminen.
Vahinkoriskit	Ehkä parhaiten tunnettu tai helpoiten käsiteltävä riskiluokka on vahinkoriskit. Vahinkoriskejä ovat henkilöstön työkykyyn, matkustukseen, avainhenkilöihin ja ympäristöön liittyvät riskit.

Taulukko 2: Riskilajit

5.2.4 Turvallisuusriskien luokittelu

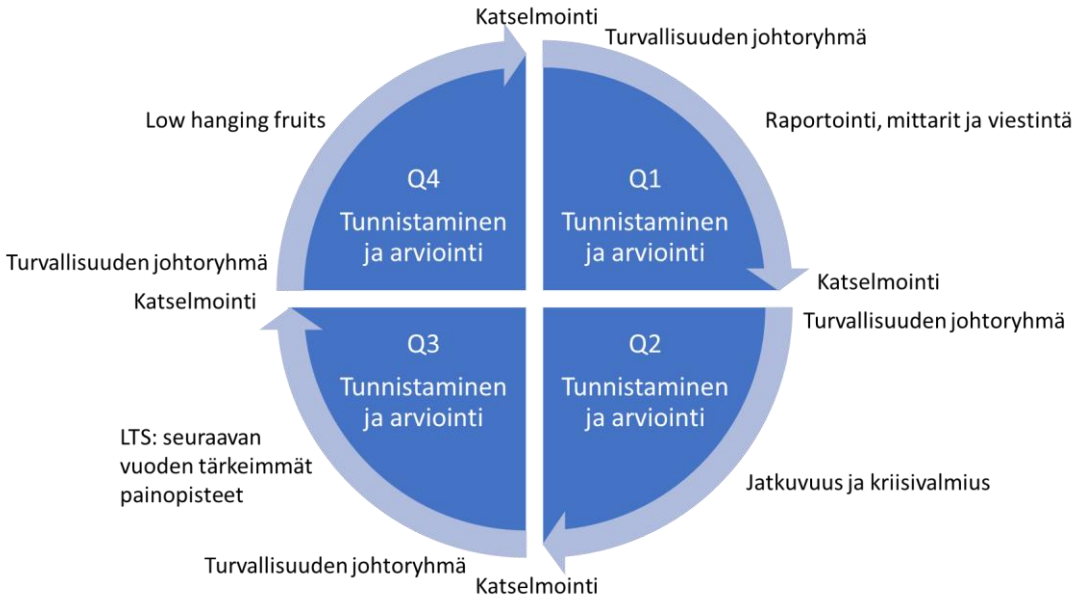
Turvallisuusriskit luokitellaan ilmenemismuodon tai sen mukaan mihin toiminteeseen riskin mahdollinen vaikutus kohdistuu. Turvallisuusriskit voivat olla mitä tahansa organisaation toimintaan vaikuttavia epävarmuustekijöitä. Turvallisuusriskit luokitellaan taulukossa 2 kuvatun mukaisesti.

Riskiluokka	Kuvaus
Tietoturvariski	Riski, joka vaikuttaa tietojärjestelmiin tai -verkkoihin ja voi aiheuttaa käytettävyyden, eheyden tai luotettavuuden heikentymisen tai menettämisen.
Tietosuojariski	Tietosuoja-asetuksen alaisen tiedon tai muun sensitiivisen tiedon joutuminen alttiiksi vuotamiselle.
Henkilöturvallisuusriski	Organisaation oman henkilöstön turvallisuuden vaarantuminen tai altistuminen rikoksille, onnettomuuksille tai muille vaaratilanteille töissä tai työmatkoilla.
Tilaturvallisuusriski	Organisaation tiloihin kohdistuvat riskit, jotka voivat johtua ihmisistä tai vallitsevista olosuhteista, kuten esimerkiksi luonnonkatastrofit ja tulipalot.
Vaatimustenmukaisuusriski	Riskit, jotka voivat toteutuessaan vaikuttaa organisaation kykyyn tuottaa palveluita vallitsevien lakien, määräysten ja/tai asiakasvaatimusten mukaisesti.
Jatkuvuusriski	Liiketoiminnan jatkuvuuteen ja organisaation kriisinsietoon liittyvät riskit, jotka voivat toteutuessaan vaikuttaa myös vaatimustenmukaisuuteen.
Rikosriski	Ulkoiset ja sisäiset rikosriskit, jotka toteutuessaan aiheuttavat vahinkoa organisaatiolle. Kyseessä voi olla esimerkiksi vahingonteko tai näpistys, mutta myös uudentyyppiset ns. toimitusjohtajahuijaukset luokitellaan rikosriskeihin.

Taulukko 3: Turvallisuusriskien luokittelu

5.2.5 Vuosikello

Turvallisuusriskien prosessi toimii myöhemmin kuvatun mukaisesti koko ajan. Turvallisuusriskejä käsitellään turvallisuuden osa-alueiden osalta turvallisuusjohtajan johdolla kerran kvartaalissa. Kerran kvartaalissa tapahtuvan käsittelyn jälkeen koostetaan Yritysturvallisuuden yhteinen riskisalkku, joka esitetään Turvallisuuden johtoryhmälle strategisten riskien osalta. Operatiivisen tason riskien hallintaa ja arviointia on syytä tehdä jatkuvasti.



Kuva 5: Turvallisuusriskien hallinnan vuosikello

Turvallisuusriskien hallinnan vuosikelloon on kuvattu riskienhallinnan jatkuvien toimenpiteiden lisäksi kvartaalikohtaiset painopistealueet. Painopisteiden tarkoituksena on varmistaa turvallisuusriskienhallinnan, turvallisuustoiminnan sekä siihen liittyvien toimintojen tehokkuus sekä säännöllisyys. Turvallisuusriskien hallinnan toimenpiteet täydentävät muuta turvallisuustoimintaa, mutta säännöllisyyden ja ohjaavuuden avulla pystytään varmistamaan riskienhallinnan tärkeys organisaation turvallisuustyölle. Ensimmäisen kvartaalin aikana tunnistetaan tavoiteasetannan kautta kyseiselle vuodelle tärkeimmät tavoitteet osa-alueen turvallisuustyölle, viestitään niistä sekä tunnistetaan toiminnan onnistumisen kannalta oleelliset mittarit. Toisen kvartaalin aikana varmistetaan, ja tarvittaessa päivitetään, osa-alueen jatkuvuussuunnitteluun ja kriisitilanteisiin liittyvien ohjeiden ja toimintamallien ajantasaisuus. Jatkuvuussuunnittelu ja liiketoiminnan jatkuvuuden varmistaminen ovat yksi keskeisiä turvallisuustoiminnan ja turvallisuusriskienhallinnan toiminnan päämääriä. Kolmannen kvartaalin aikana tunnistetaan olemassa olevien sekä nousevien riskien kautta seuraavan vuoden kannalta kriittisimmät kohteet ja/tai asiat sekä varmistetaan niiden toteutuminen resurssisuunnittelussa. Viimeisen kvartaalin keskeisimpänä turvallisuusriskien hallinnan painopisteenä on varmistaa ja toteuttaa niin sanottujen helppojen asioiden toteutumien ja riskien sulkeminen. Low hanging

fruits tarkoittaa sellaisten asioiden ja toimenpiteiden toteuttamista, jotka eivät vaadi juurikaan ajallista tai rahallista resurssia. Näitä ovat esimerkiksi tunnistetut asiat, joiden osalta ei ole tehty kirjallista toimintaohjetta, mutta toiminta on jo vakiintunut tietynlaiseksi.

5.2.6 Riskien tunnistaminen

Riskien tunnistaminen pitää sisällään useita vaiheita ja riskien tunnistamiseen voidaan käyttää erilaisia metodeja.

Valtiovarainministeriö (2017a, 21) kuvaa Ohje riskienhallintaan -julkaisussa, riskien tunnistamisen pitävän sisällään neljä vaihetta:

- on tunnistettava sellaiset asiat tai uhat, jotka voivat estää, haitata tai viivästyttää määritellyn tavoitteen saavuttamista
- pyrittävä tunnistamaan riskit, joiden hyödyntämättä jättäminen aiheuttaa organisaatiolla tilanteen olla hyödyntämättä tuloksellisempaa tai tehokkaampaa tapaa saavuttaa tavoitteet
- luodaan tunnistetuista riskeistä ja mahdollisuuksista luettelo
- kirjataan myös riskit, joiden aiheuttaja ei ole tiedossa tai organisaation hallittavissa

Riskien tunnistamiseen hyödynnetään asiantuntijoista koottua ryhmää, joka aivoriihi menetelmää hyödyntäen tunnistaa uusia toimintaan kohdistuvia uhkia ja mahdollisuuksia. Aivoriihi tyyppisen työpajan pitää olla suunniteltu ja sen fasilitoinnista vastaa varsinaisesta toiminnasta ulkopuolinen henkilö. Työpajassa on tärkeää sopia selkeät pelisäännöt toiminnalle, jotta kaikki toimintaan tai palveluun vaikuttavat asiat saadaan tunnistettua.

Riskien tunnistamiseen hyödynnetään lisäksi poikkeamien hallinta prosessista saatavaa aineistoa, työntekijöiden ilmoituksia havaituista poikkeamista tai mahdollisista riskitekijöistä sekä historia-aineistoa konkretisoituneista tapahtumista kohdeorganisaatiossa tai vastaavissa organisaatioissa. Skenaariotyön hyödyntämistä tulevaisuuden tapahtumien ennustamisessa pyritään hyödyntämään varsinkin silloin kun tarkastellaan uusia innovatiivisia palveluita, joita ollaan vasta tuomassa markkinoille. Riskejä voi nousta esiin myös erilaisten sisäisten ja ulkoisten auditointien seurauksena, prosessi läpikävelyissä sekä valvovien viranomaisten toimesta.

5.2.7 Riskien arvottaminen

Riskien todennäköisyyden ja vaikuttavuuden arvioinnissa käytetään anonyymin asiantuntijaryhmän eli niin sanotun delphin menetelmää. Tämän menetelmän avulla pyritään

muodostamaan mahdollisimman realistinen kuva riskin vaikutuksesta ja todennäköisyydestä ilman sosiaalisia riitatilanteita. Delphin menetelmän avulla jokaisen asiantuntijan arvio on samanarvoinen eikä esimerkiksi johtosuhteet vaikuta arviointiin, tämä tapa mahdollistaa myös kriittisten mielipiteiden paremman ja asiallisemman käsittelyn. Anonyymin asiantuntijaryhmän menetelmässä asiantuntijoilta kysytään riskin todennäköisyyttä ja vaikutusta ja tulokset koostetaan yhteen. Tämän jälkeen kysely toistetaan ja asiantuntijoita pyydetään arvioimaan kohde uudelleen muiden vastausten perusteella. Tämä toimintamalli voidaan toistaa useampiakin kertoja, kunnes riittävän yhtenäinen arvio on saatu aikaan. (Ilmonen ym. 2010, 114-115)

Todennäköisyys tarkoittaa riskin esiintymistaajuutta. Riskin todennäköisyyden ollessa korkea, riski toteutuu lähes varmasti seuraavan vuoden aikana. Taajuuden ollessa matala, riski todennäköisyys toteutua organisaatiossa on erittäin pieni. Tämä ei kuitenkaan tarkoita, ettei riski voisi toteutua.

Todennäköisyys	Esiintymistaajuus	Kuvaus
5 - erittäin todennäköinen	Useammin kuin 1 kerran vuodessa	Toteutuu nykyisessä tilanteessa; on toteutunut viimeisen vuoden aikana
4 - todennäköinen	Kerran vuodessa	Toteutuu oletettavasti nykyisessä tilanteessa; on toteutunut viimeisen kahden vuoden aikana
3 - mahdollinen	Kerran 2-4 vuoden aikana	Toteutuu oletettavasti nykyisessä tilanteessa; on toteutunut vastaavassa toimintaympäristössä viimeisen neljän vuoden aikana
2 - epätodennäköinen	Kerran 5-10 vuoden aikana	Toteutuu poikkeuksellisessa tilanteessa
1 - erittäin epätodennäköinen	Kerran 10 vuodessa tai harvemmin	Toteutuu erittäin poikkeuksellisessa tilanteessa

Taulukko 4: Riskin todennäköisyys

Riskin vaikutuksella tarkoitetaan riskin toteutumisesta aiheutuvaa tilannetta organisaatiolle. Vaikutus voi olla taloudellinen tai sillä voi olla vaikutusta esimerkiksi organisaation maineelle tai operatiiviselle toiminnalle.

Vaikutus	Toiminta	Vaatimustenmukaisuus	Taloudellinen menetys
5 - erittäin korkea	Organisaation toiminta keskeytyy; laaja ja näkyvä vaikutus asiakkaille	Toiminta lainvastaista; pitkäaikaisia vaikutuksia maineelle	yli 100 000 €
4 - korkea	Huomattavia vaikutuksia useille palveluille tai toiminnoille; merkittäviä asiakasvaikutuksia	Toiminta asiakasvaatimusten vastaista; merkittävä mainehaitta; ilmoitusvelvollisuus viranomaisille	50 000€ - 100 000€
3 - kohtuullinen	Vaikutus yksittäisille palveluille tai toiminnoille; kohtalaisia asiakasvaikutuksia	Aiheuttaa haittaa yksittäisten asiakkuuksien luottamukselle; mahdollinen raportointivelvollisuus viranomaisille	10 000€ - 50 000€
2 - matala	Vähäinen vaikutus; yksittäinen palvelu tai toiminto hidastunut	Ei vaikutusta tai vähäinen vaikutus	1000€ - 10 000€
1 - erittäin matala	Ei huomattavaa vaikutusta toimintaan	Ei vaikutusta	alle 1000 €

Taulukko 5: Riskin vaikutus

5.2.8 Riskien käsittely

Riskin käsittely pitää sisällään yhden tai useamman riskinhallintamenetelmän toteuttamisen tunnistetuille riskeille. Riskit käsitellään kriittisyys järjestyksessä, isoimmat tärkeään suojattavaan kohteeseen kohdistuvat riskit on käsiteltävä ensimmäisenä. Käsittelyssä suunnitellaan, vastuutetaan ja aikataulutetaan yksi tai useampi menetelmä, jolla riskin vaikutusta ja/tai todennäköisyyttä pienennetään. Soveltuvimman käsittelytavan valinta on aina suhteutettava aiheutuva kustannus suhteessa saavutettavaan hyötyyn sekä riskin mahdollisesta toteutumisesta aiheutuviin kustannuksiin.

Riskejä voidaan käsitellä neljällä tavalla:

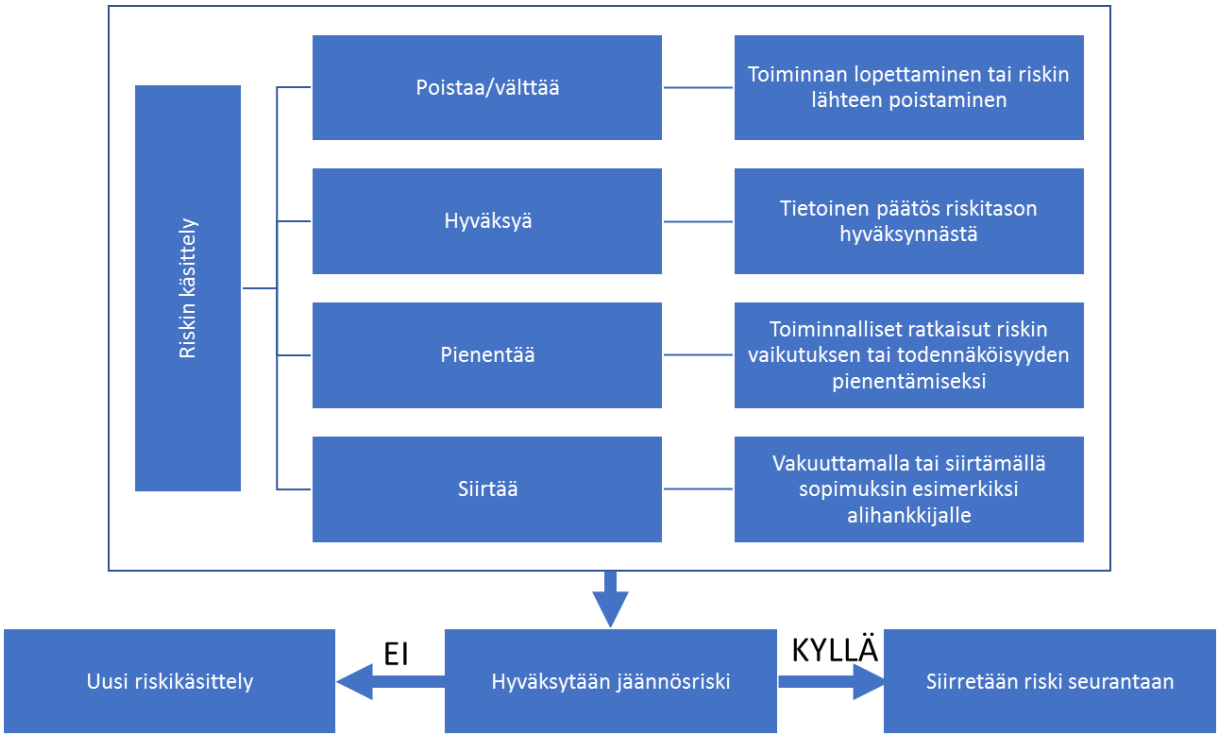
1. Hyväksyä - tietoisen päätöksen tekeminen siitä, että riskiluokitus on hyväksyttävällä tasolla tai, että riskin mitigoinnin kustannukset ovat suuremmat kuin siitä saatava hyöty. Riskin mitigoimiseksi ei toteuteta toimenpiteitä, mutta riskiä on suositeltavaa seurata, jotta mahdolliset muutokset havaitaan.

2. Poistaa/välttää - päätös, että riskiä tuottavaa toimintoa ei enää jatketa, vaan lopetetaan toiminta kokonaan tai etsitään vaihtoehtoinen tapa täyttää organisaation tarve saavuttaa asetetut tavoitteet. Toinen vaihtoehto on eliminoida riskin aiheuttaja kokonaan, jos se on mahdollista.

3. Pienentää - on sellaisten toimenpiteiden toteuttamista, jotka pienentävät riskin aiheuttamaan vaikutusta organisaatiolle tai vähentävät todennäköisyyttä. Riskin kokonaisvaikutusta on yleensä mahdollista pienentää. Kustannus-hyöty suhde on muistettava laskea, jotta pienentäminen on kannattavaa.

4. Siirtää - riskin aiheuttamaa vaikutusta voi siirtää sopimusten avulla alihankkijan kannettavaksi, siirtämällä omaisuutta tai toimintoja toiselle yritykselle. Riskejä on mahdollista myös siirtää vakuuttamalla osittain tai kokonaan.

Kaikki tunnistetut riskit kirjataan riskienhallintasuunnitelmaan, johon dokumentoidaan riski, riskin arvo sekä riskin käsittelyssä sovitut toimenpiteet. Käsittelyprosessissa päätetään riskikohtaisesti sille tehtävät toimenpiteet sekä vastuutetaan ja aikataulutetaan sovitut toimenpiteet. Suunnitelmaan kirjataan lisäksi tarvittavat resurssit riskin käsittely toimenpiteiden toteuttamiseksi. Kaikkien riskienhallintasuunnitelmaan kirjattujen riskien osalta laaditaan myös raportointi- ja seuranta vaatimukset.



Kuva 6: Riski käsittelyn vaiheet

5.2.9 Riskien seuranta ja arviointi

Riskienhallintasuunnitelmaan tai riskirekisteriin kirjattuja riskejä on tarkasteltava säännöllisesti, lisäksi kaikki toimenpiteet tai tapahtumat, jotka ovat vaikuttaneet riskin arvoon, on kirjattava. Riskien seuranta on oltava osa säännöllistä toimintaa ja sen toteuttamista on valvottava. Seuranta vaiheessa on otettava huomioon kaikki riskinhallintaprosessin, kuten että sovitut ja toteutetut kontrollit ovat vaikuttaneet ja että riskien hallinta on riittävän tehokasta. On myös analysoitava mahdollisia poikkeamia, jotka voivat vaikuttaa tunnistettuihin riskeihin tai luoda uusia. Lisäksi on arvioitava, että vaikuttavan riskien hallinnan toteuttamiseksi on riittävä ja ajantasainen tieto saatavilla.

5.3 Prosessi

Kuva 7 Riskienhallintaprosessi (Mukailtu Allen & Loyear 2018, 70)

Turvallisuusriskien hallintaprosessin halutaan vastaavan ISO 31000 standardin vaatimuksiin, mutta prosessi toteutetaan mukautettuna Allen & Loyear (2018) Enterprise Security Risk Management -kirjassa kuvatun mallin mukaisesti. Kyseisen mallin mukaisesti toteutettu prosessi kuitenkin vastaa ISO 31000 standardin vaatimuksia.

5.3.1 Tunnista ja priorisoi suojattavat kohteet

Turvallisuusriskien hallintaprosessin ensimmäisessä vaiheessa tunnistetaan toimintaan liittyvä omaisuus ja niiden omistajat sekä muut sidosryhmät. Tässä vaiheessa on tärkeää tunnistaa kaikki liiketoimintaan liittyvä aineellinen ja aineeton omaisuus, niiden omistajat sekä niille kriittiset sidosryhmät. Yhteistyössä sidosryhmien kanssa priorisoidaan omaisuuden kriittisyys liiketoiminnalle. Tämän luokittelun avulla voidaan myöhemmässä vaiheessa paremmin arvioida tunnistettujen riskien vaikutusta liiketoiminnalle. (Allen & Loyear 2018, 82).

Tutkimuksen aikana tehtyjen havaintojen perusteella turvallisuusriskien arvioinneissa suhteessa riskin vaikutukseen liiketoiminnalle koettiin paljon haasteita. Tästä syystä tässä mallissa tätä ongelmaa lähdettiin ratkaisemaan uudenlaisen lähestymisen kautta. Aivoriihien saadun palautteen perusteella voidaan todeta, että uuden mallin avulla riskienhallinnan toimenpiteitä pystyttiin paremmin kohdistamaan merkityksellisiin turvallisuusriskeihin. Tämän lisäksi

turvallisuusriskien arviointiin ja käsittelyyn saatiin vaikuttavuutta, koska omaisuuden omistajat liiketoiminnasta oltiin tunnistettu ja kommunikaatio oli tämän seurauksena parempaa.

Alla olevaa taulukkoa (Taulukko 5) voidaan hyödyntää priorisoitaessa suojattavia kohteita. Alla olevat luokitukset ovat suuntaa-antavia, kohteet voivat toiminnasta riippuen olla korkeampia tai matalampia kuin taulukossa. Suojattavan kohteen priorisointi on aina tehtävä Yritysturvallisuuden asiantuntijan sekä toiminnoista vastaavan henkilön/henkilöiden kanssa yhteistyössä, jotta priorisointi on riittävän kattava. Priorisoinnissa on huomioitava aina suojattavan kohteen sisältämä tietoaineisto, esimerkiksi henkilö- ja/tai välitystiedot.

Suojaustaso	Tilaturvallisuus (Viestintävirasto 54 B/2014 M)	Tietoturvallisuus (Elisan sisäinen luokitus)	Tietoaineiston luokittelu
5 - erittäin korkea	TL 1	High	Suojaustaso I (ST I)
4 - korkea	TL 2	Increased	Suojaustaso II (ST II)
3 - kohtuullinen	TL 3	Increased limited	Suojaustaso III (ST III)
2 - matala	TL 4	Base	Suojaustaso IV (ST IV)
1 - erittäin matala	TL 5	Base	Julkinen

Taulukko 6: Suojattavan kohteen priorisointi

5.3.2 Tunnista ja arvota riskit

Toisessa vaiheessa tunnistetaan omaisuuteen kohdistuvat uhat ja mahdollisuudet sekä priorisoidaan riskit. Riskien ja uhkien tunnistamisen lähtökohtana on tunnistaa kaikki omaisuuteen kohdistuvat uhat, sen alttius vaikutukselle sekä vaikutus eli mitkä ovat seuraukset. Riskin on pidettävä sisällään kaikki nämä kolme komponenttia, jotta sitä voidaan käsitellä. Käyttämällä aikaa liiketoiminnan kannalta tärkeän omaisuuden suojaamiseen, turvallisuustoiminnan vaikuttavuutta saadaan kasvatettua. Riskejä voidaan tunnistaa monella tapaa, aivoriihen lisäksi voidaan hyödyntää historia tietoa tapahtuneista poikkeamista sekä hyödyntää ulkoisia, esimerkiksi vakuutusyhtiöiden, riskirekistereitä. Riskien tunnistamisen jälkeen, tunnistetut riskit arvotetaan liiketoiminta kriittisyyden näkökulmasta. Eli mitkä riskit ja niiden vaikutukset ovat kriittisimpiä suojattavalle omaisuudelle ja ovatko joidenkin riskien vaikutukset määritellyn

sietokyvyn rajoissa. Tämän työn avulla saadaan kerättyä tieto liiketoiminnan näkökulmasta merkityksellisimmistä turvallisuusriskeistä. (Allen & Loyear 2018, 98-102).

Tutkimuksen perusteella asiantuntijoiden aivoriihen lisäksi on hyödyllistä käyttää aiempien tapahtumien dataa, kun tunnistetaan ja priorisoidaan riskejä. Aiemmin tapahtuneiden poikkeamien ja niiden vaikutusten analysoinnin avulla saatiin aiempaa paremmin tunnistettua ja varsinkin priorisoitua riskejä. Juurisyyanalyysien pohjalta asiantuntijat ja omaisuuden vastuullisten oli helpompaa löytää uhkien realisoitumisesta mahdollisesti aiheutuvia tapahtumia liiketoiminnan kannalta kriittisille kohteille.

5.3.3 Mitigoi priorisoituja riskejä

Turvallisuusriskien hallinnanprosessin kolmannessa vaiheessa mitigoidaan eli pienennetään tai poistetaan priorisoitujen riskien aiheuttamia vaikutuksia. Aiemmassa vaiheessa tunnistettujen uhkien aiheuttamia riskejä vähennetään sietokyvyn sallimalle tasolle tai mahdollisesti riskiä aiheuttava uhka poistetaan kokonaan. Riskien mitigointi on kriittinen osa turvallisuustoimintaa, mutta myös liiketoiminnalle. Riskejä voidaan mitigoida monella eri tavalla, ISO 31000 standardin mukaan mitigointi voi olla riskiä aiheuttavan työn lopettaminen, ottaminen mahdollisuuksien lisäämiseksi, vakuuttamalla tai muuttamalla riskin todennäköisyyttä tai seurausta sekä pitäminen ennallaan. Allen & Loyear (2018) mukaan turvallisuusriskejä voidaan käsitellä neljällä tavalla: hyväksymällä, lopettamalla riskiä aiheuttava työ, siirtämällä riski toiselle esimerkiksi vakuuttamalla tai vähentämällä uhan alttiutta tai vaikutusta. Riskien mitigoinnin on joka tapauksessa tapahduttava yhteisellä päätöksellä parhaan mahdollisen tiedon perusteella. (Allen & Loyear 2018, 116-121; ISO 31000:2018, 18-19)

Tutkimuksen aikana tehtyjen havaintojen perusteella voidaan todeta, että tekemällä turvallisuusriskeihin liittyvät päätökset tiiviissä yhteistyössä liiketoiminnan tai omaisuudesta vastaavan henkilön kanssa, turvallisuustoimintaa ja turvallisuuden kontrolleja saadaan paremmin näkyväksi organisaatiolle. Tämän lisäksi yhteistyöllä pystytään paremmin välttämään konflikteja liiketoiminnan ja turvallisuustoiminnan välillä, koska uhkia, niiden vaikutuksia ja priorisointia on tehty liiketoiminnan ehdoilla.

5.3.4 Jatkuva kehittäminen

Turvallisuusriskien hallintamallin jatkuvan kehittämisen kolme osa-aluetta ovat:

1. Poikkeaminen hallinta
2. Juurisyyanalyysit
3. Jatkuva riskien arviointi

Poikkeamien hallinta on organisoitava kaikkien turvallisuuden osa-alueiden osalta jatkuvaksi toiminnaksi. Poikkeamien hallinnalla tarkoitetaan pääasiassa reaktiivista toimintaa, jossa ilmenneisiin poikkeamiin puututaan välittömästi ja niiden vaikutus liiketoiminnalle pyritään minimoimaan. Kohdeorganisaatiossa turvallisuuspoikkeamien hallinnasta vastaa kaksi eri tahoa: tietoturva ja -suoja poikkeamien käsittelystä vastaa SOC-toiminne ja muiden turvallisuuspoikkeamien osalta Turvallisuusvalvomo. Molemmat toiminteet toimivat 24/7 periaatteella ja vastaavat ensimmäisen tason vasteesta poikkeamien sattuessa. Poikkeamien hallinta prosessi on yksi tapa luoda ja ylläpitää organisaation tietoisuutta uusien riskien ja jäännösriski päätöksen saaneiden riskien osalta. Uusien riskien osalta poikkeamien hallinta prosessilla on oltava selkeät toimintamallit vahinkojen minimoimiseksi. Riskien osalta, jotka ovat käsittelyssä ja ovat joko hyväksytty tai aktiivisesti hallittuja, on mahdollista, että haitallinen tapahtuma konkretisoituu. Tässäkin tapauksessa poikkeamien hallinta prosessi on ensimmäinen taho suojautumisen ja palautumisen osalta.

Juurisyyanalyysien tarkoituksena on selvittää tapahtuneiden poikkeamien todelliset tekijät ja poikkeaman aiheuttajat. Analyysin tavoitteena on läpikävellä koko prosessi ja tunnistaa prosessin heikot kohdat, joihin tunnistettu tai tunnistamaton tapahtuma on vaikuttanut. Juurisyyanalyysistä valmistuvan raportin pitäisi kertoa liiketoiminnalle ja turvallisuusyksikölle poikkeaman aiheuttaneen uuden tai tunnistetun riskin vaikutukset tavoitteille sekä mahdolliset korjaavat toimenpiteet, jotta sama tapahtuma ei pääse tapahtumaan uudestaan.

Poikkeamien hallintaprosessin ja juurisyyanalyysien kautta nousee tietoisuuteen uusia riskejä ja niiden osalta on tehtävä jatkuvaa riskien arviointia. Riskien arviointi toteutetaan saman prosessin mukaan. Jatkuvan riskien arvioinnin yhteydessä on tunnistettava toimintaympäristössä mahdollisesti tapahtuneet muutokset, arvioitava mitkä edellä mainittujen prosessien löydökset todella ovat riskejä, priorisoitava ne sekä käsiteltävä ne liiketoiminnan edustajien kanssa. Jatkuva riskien arviointi luo prosessille jatkuvan kehittämisen ja kehittymisen mallin.

6 Johtopäätökset

Opinnäytetyössä tehdyn tutkimuksen tavoitteena oli selvittää kohdeorganisaation turvallisuusriskien hallintaprosessin nykytila, tunnistaa kehityskohteet suhteessa omaan toimintaan sekä ulkoisen toimintaympäristön asettamiin vaatimuksiin. Tutkimuksessa päädyttiin toteuttamaan havaintojen perusteella tehdyn analyysin sekä johdon tahtotilan perusteella päivitetty turvallisuusriskien hallintamalli, joka vastaa edellä mainittuihin tavoitteisiin sekä täyttää ISO 31000 riskienhallinta standardin hengen.

Tutkimuksessa tehdyn havainnoinnin perusteella tunnistettiin kolme selkeää puutetta nykyisestä toimintamallista ja niiden pohjalta lähdettiin päivittämään uutta hallintamallia. Tehdyn tutkimuksen perusteella havaittiin turvallisuusriskien hallinnan kasvanut tärkeys sekä kohdeorganisaation muuttuneen liiketoiminnan ja toimintaympäristön osalta, mutta myös

kasvaneiden ja päivittyneiden lakivaatimusten ja viranomaismääräysten osalta. Toteutettu turvallisuusriskien hallintamalli pyrkii vastaamaan aiempaa paremmin asetettuihin vaatimuksiin ja ensimmäisten kokeilujen aikana saatiin paljon positiivisia kokemuksia uudesta hallintamallista. Hallintamallin jatkuvan kehittämisen kautta turvallisuusriskien arvoa toiminnalle pystytään oletettavasti nostamaan aiempaa paremmalle tasolle. Riskienhallinnan uudelleenorganisointi on huomattavasti pidempiaikaisempi projekti kuin tähän tutkimukseen käytössä oleva aika, joten päivitetyn hallintamallin todellisia tuloksia voidaan tarkastella vasta myöhemmin. Lisäksi hallintamallin käyttöönoton jälkeen panostettava yhteisten työkalujen tuottamiseen ja/tai käyttöönottoon, jotta riskienhallinnan kattavuus ja yhteismitallisuus saadaan kasvamaan.

Tämän tutkimuksen tuloksia sekä tässä tutkimuksessa luotua hallintamallia voidaan hyödyntää kohdeorganisaation muiden operatiivisten riskien hallinnassa. Kirjattujen hallintamallin periaatteiden ja puitteiden osia voidaan hyödyntää myös muiden riskilajien hallintamallin rakentamisessa. Koska riskienhallinta on johdettu pitkälti organisaation strategiasta ja tavoitteista sekä riskienhallinta on räätälöity kohdeorganisaatioon sopivaksi, on tässä tutkimuksessa saatuja tuloksia vaikeaa hyödyntää suoraan muiden organisaatioiden käyttöön. Jatkotutkimuksen näkökulmasta voisi tosin olla mielenkiintoista tutkia, voidaanko tämän tutkimuksen tuloksia hyödyntää suoraan esimerkiksi toisessa, saman toimialan organisaatiossa. Toinen mahdollinen jatkotutkimuksen aihe on myöhemmässä vaiheessa tutkia kuinka tässä työssä luodun hallintamallin tavoitteet ovat toteutuneet suhteessa odotuksiin.

Lähteet

Painetut

Allen, B. & Loyear, R. 2018. Enterprise Security Risk Management – concepts and applications. Conneticut: Rothstein Publishing.

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

Hopkin, P. 2017. Fundamentals of Risk Management 4th edition. Croydon: CPI Group

Hubbard, W. D. 2009. The Failure of Risk Management. John Wiley & Son: New Jersey

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2010. Johda riskejä – käytännön opas yrityksen riskienhallintaan. Pössneck: Kustannusosakeyhtiö Tammi.

ISO 31000:2018. Riskienhallinta. Ohjeet. Helsinki: Suomen Standardisoimisliitto

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala, T. 2014. Yrityksen riskienhallinta. Vantaa: Hansaprint.

Kuusela, H. & Ollikainen, R. 2005. Riskit ja riskienhallinta. Tampere: Tampereen Yliopistopaino-Juvenes Print.

Lanne, M. 2007. Yhteistyö yritysturvallisuuden hallinnassa. Helsinki: Edita Prima.

Lanne, M. & Heikkilä, J. 2016. Uutta riskien arviointiin! - Tietopohjan merkitys ja uudistamisen keinot. Espoo: Teknologian tutkimuskeskus VTT

Leino, M., Steiner, M-L. & Wahlroos, J. 2005. Corporate governance ja riskienhallinta. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) Riskit ja riskienhallinta. Tampere: Tampereen Yliopistopaino Oy – Juvenes Print,123-147.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Jyväskylä: Gummerrus Kirjapaino

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYPro.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Helsinki: SanomaPro.

Suominen, A. 2005. Kokonaisvaltainen riskienhallinta yrityksen suojajärjestelmänä. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) Riskit ja riskienhallinta. Tampere: Tampereen Yliopistopaino Oy – Juvenes Print,148-169.

Sähköiset

Elisa. 2018a. Toimintamalli ja tytäryhtiöt. Viitattu 8.7.2019. https://corporate.elisa.fi/tietoa-elisasta/toimintamalli-ja-tytaryhtiot/

Elisa. 2018b. Historia. Viitattu 8.7.2019. https://corporate.elisa.fi/tietoa-elisasta/historia/

Elisa. 2018c. Valvontajärjestelmät. Viitattu 25.4.2019. https://corporate.elisa.fi/sijoittajille/hallinnointi/valvontajarjestelmat/

Elisa Vuosikatsaus 2018. Viitattu 25.4.2019. https://corporate.elisa.fi/attachment/content/Elisa_vuosikatsaus_2018.pdf

Elisa Yritysvastuuraportti 2018. Viitattu 25.4.2019. https://corporate.elisa.fi/attachment/elisa-oyj/annual-report-2018/Elisa_vk18_responsibility_report.pdf

Finlex. 2014. Laki sähköisen viestinnän palveluista 917/2014. Viitattu 26.5.2019. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#O10L35

Finlex. 2011. Valmiuslaki 1552/2011. Viitattu 26.5.2019. https://www.finlex.fi/fi/laki/ajantasa/2011/20111552#O2L9P60

Valtiovarainministeriö. 2017a. Ohje riskienhallintaan. Viitattu 26.5.2019. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

Valtiovarainministeriö. 2017b. VM 22/2017 Ohje riskienhallintaan - LIITTEET. Viitattu 11.7.2019. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/Liitteet_VM22_2017.pdf?sequence=2&isAllowed=y

Viestintävirasto. 2015. Määräys teletoiminnan tietoturvasta 67 A/2015 M. https://www.finlex.fi/data/normit/44046/M67A_2015.pdf

Sisäministeriö. 2019. Kansallinen riskiarvio 2018. Viitattu 28.5.2019. https://intermin.fi/julkaisut/julkaisu?pubid=URN:ISBN:978-952-324-245-6

Taulukot

Kuvat

Kuva 1: Elisan toimintamalli (Elisa 2018a) 9

Kuva 2: Periaatteet, puitteet ja prosessit (ISO 31000:2018, 5)..... 14

Kuva 3: PESTLE-malli (Valtiovarainministeriö 2017b) 24

Kuva 4: Turvallisuusriskien hallinnan vastuut..... 25

Kuva 5: Turvallisuusriskien hallinnan vuosikello..... 29

Kuva 6: Riski käsittelyn vaiheet 34

Kuva 7 Riskienhallintaprosessi (Mukailtu Allen & Loyear 2018, 70) 35

Liitteet

Liite 1: Turvallisuusriskien hallinnan periaatteet

Turvallisuusriskien hallinnan periaatteet	
Document Information	
Document name:	Turvallisuusriskien hallinnan periaatteet
Document type:	Periaate
Document owner:	Elisa Corporate Security
Author(s): Org / name.	Elisa Corporate Security
Document applicability:	Elisa Oyj (incl. subsidiaries)
Document approval	Elisa Security Governance Board (Elisan turvallisuuden johtoryhmä (ETJR)
Review interval	Annually
Related documents	Elisa security policy
Document location:	

Reviews and approvals		
Date	**Participant(s)**	**Results**

Version history			
Version	**Date**	**Author(s)**	**Summary of changes**

Turvallisuusriskien hallinnan periaatteet

Perusteet

Elisa Oyj:n ja sen tytäryhtiöiden turvallisuusriskien hallinta perustuu toiminnalle asetetun lainsäädännön, viranomais- ja asiakasvaatimusten sekä ISO 31000 standardin vaatimusten mukaan.

Turvallisuusriskien hallinnan menettelyt ja toimintatavat ovat yhteneväiset ja turvallisuusriskeistä vastaavalla taholla on riittävät edellytykset päätösten tekemiseksi. Päämääränä on tukea organisaatiota tavoitteiden saavuttamiseksi sekä parantaa suorituskykyä. Turvallisuusriskien hallinnan on tuettava liiketoiminnan ja ylimmän johdon turvallisuustoiminnalle asetettuja tavoitteita.

Turvallisuusriskien hallinnan tavoitteena on ennakoivasti ja systemaattisesti havaita sellaiset turvallisuuteen liittyvät uhat, joilla voi olla vaikutusta käsiteltävän kokonaisuuden toimintaan tai toiminnallisuuteen. Riskienhallintatyön tuloksena tulee ennakoivasti toteuttaa sellaisia toimenpiteitä, joilla havaitun riskin todennäköisyyttä ja vaikutusta vähennetään hyväksyttävälle tasolle.

Määritelmät

Turvallisuusriskien hallinnalla tarkoitetaan operatiivisten turvallisuusriskien hallintaa, joiden mahdollinen toteutuminen voi vaarantaa suojattavia arvoja: tietoa, omaisuutta tai ihmisiä. Turvallisuusriski on sellainen tekijä, joka uhkaa yrityksen toimintaa, henkilökuntaa, yhteistyökumppaneita tai sen toimintaa sekä mainetta.

Periaatteet

Turvallisuusriskien hallinta on säännönmukaista toimintaa, jonka tarkoituksena on varmistaa liiketoiminnan jatkuvuus kaikissa tilanteissa sekä pyrkiä estämään ei-toivottujen tapahtumien aiheuttamaa vaikutusta toiminnalle ja suojattaville arvoille.

Turvallisuusriskien hallinnan periaatteet:

- Turvallisuusriskien hallinta on säännönmukaista ja dokumentoitua
- Turvallisuusriskien hallinnan vaikuttavuutta seurataan ja tuloksia mitataan
- Turvallisuuden toimenpiteet tähtäävät tunnistettujen ja nousevien riskien vaikutusten poistamiseksi tai pienentämiseksi.

- Turvallisuusriskien hallinnan avulla varmistetaan kriittisen omaisuuden riittävä suojaaminen sisäisiä ja ulkoisia uhkia vastaan.
- Turvallisuusriskien hallinnan on vastattava toimintaympäristön asettamiin kansallisen lainsäädännön sekä toimialan erityisvaatimuksiin.
- Turvallisuusriskien arviointi ja käsittely toteutetaan turvallisuusriskien hallinnan toimintaohjeen mukaisesti.

Vastuut

Turvallisuusriskien hallintaprosessin ylläpidosta ja kehittämisestä vastaa Elisan Yritysturvallisuus yksikkö. Yritysturvallisuus toteuttaa turvallisuusriskien arviointia turvallisuuden osa-alueiden osalta ja raportoi strategisen tason turvallisuusriskit säännöllisesti turvallisuuden johtoryhmälle. Elisan turvallisuuden johtoryhmä käsittelee kaikki strategisen tason turvallisuusriskit sekä vastaa turvallisuusriskien hallintaprosessin riittävyyden arvioinnista ja asettaa tavoitteet toiminnalle.

Jokainen Elisan prosesseissa työskentelevä on velvollinen raportoimaan havaitsemistaan turvallisuuteen liittyvistä riskeistä prosessin mukaisesti.