LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Miten Katakri on muuttunut?

Roivainen, Aki

2015 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Miten Katakri on muuttunut?

Aki Roivainen
Turvallisuuden tradenomi
Opinnäytetyö
Joulukuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuuden tradenomi koulutus

Aki Roivainen

Miten Katakri on muuttunut?

Vuosi 2015 Sivumäärä 108

Katakri 2015 keskittyy tarkastelemaan organisaation kykyä suojata viranomaisen salassa pidettävää tietoa ja siihen on koottu kansallisiin lakeihimme ja säädöksiimme, sekä kansainvälisiin velvoitteisiimme perustuvat kriteerit. Katakri 2015 – tietoturvallisuuden auditointityökalu viranomaiselle vaatii auditoijalta merkittävästi enemmän kuin aiemmat Katakrin versiot, koska aiemmista Katakreista poiketen se ei itsessään aseta ehdottomia vaatimuksia, vaan ne on mahdollista toteuttaa myös vaihtoehtoisilla tavoilla. Katakri 2015 – auditointityökalun täysi hyödyntäminen edellyttää, että organisaatiossa on toteutettu organisaatiolähtöinen riskienhallintaprojekti ja että organisaatio on sitoutunut sekä jatkuvaan turvallisuuden ylläpitämiseen että kehittämiseen. Näiden jälkeen Katakri 2015 – auditointityökalua voidaan käyttää tarkistuslistaluonteisesti, jonka avulla varmistetaan, että oleelliset asiat on tullut huomioitua.

Opinnäytetyössä tuodaan esiin Katakrin eri versioille yhteisiä asioita, niitä toisistaan erottavia asioita, sekä mitä kehityskohteita ja vahvuuksia niissä on ollut tai on tällä hetkellä. Opinnäytetyö keskittyy pääosin Katakri 2015 – auditointityökaluun tehtyihin olennaisimpiin muutoksiin, käyttötarkoitukseen, käyttötapaan, sekä tarpeeseen, johon se on tuotettu ja syihin niiden takana.

Opinnäytetyölle on perusteltu tarve. Katakri 2015 – auditointityökaluun vaatimuslähteistä kootut vaatimukset täyttämällä organisaatiolla on mahdollisuus osallistua kotimaisten ja kansainvälisten hankkeiden tarjouskilpailuihin, sekä myös hankkeisiin, joissa käsitellään viranomaisen turvallisuusluokiteltua tietoa. Tämän lisäksi usein edellytetään organisaatiolta osoitettua kykyä suojata viranomaisen turvallisuusluokiteltua tietoa, jotta organisaatio voi osallistua puolustusvoimien hankintojen tarjouskilpailuihin tai hankkeisiin, joissa käsitellään tälläistä tietoa. Näistä syistä opinnäytetyöllä on suora linkki elinkeinoelämään.

Katakri, riskienhallinta, riskienarviointi, turvallisuusjohtaminen, Katakri 2015

Laurea University of Applied Sciences **Abstract**
Leppävaara
Degree Programme in Security management

Aki Roivainen

How Has Katakri Changed?

Year 2015 Pages 108

Katakri 2015 – information security auditing tool focuses on inspecting an organization's ability to protect confidential information of the authority. Katakri 2015 – auditing tool demands significantly more from an auditor than the earlier versions of Katakri. The reuirements from our national laws, statutes and from our international agreements have been compiled into Katakri 2015 – auditing tool. To fully benefit from the use of Katakri 2015 – auditing tool, an organization needs to have completed an internal risk management project and the organization has to be committed continuous development and maintenance of security.

The thesis will firstly go through elements that are common to all Katakri versions, then what elements set the versions apart and what the strengths were and there was there to develop in the earlier versions of Katakri. However, this thesis is mainly about Katakri 2015 - auditing tool, what essential changes have been made in it, how it is meant to be used, what kind of strenghts and things to develop it has and the need behind compiling the Katakri 2015 –auditing tool.

There is a real need for this thesis as it will show the essential changes between the Katakri versions and how the Katakri 2015 – auditing tool should be used. By fulfilling the requirements compiled from requirement sources in Katakri 2015 – auditing tool an organization is able to verify its ability to protect confidential information of the authority. The organization has then an opportunity to take part in procurement and bid for procurement, in domestic and international arenas, where confidential information of the authority will be handled. Also possibility to take part in defence procurement and bidding for those may be available. For these reasons this thesis has a clear link to business and industry.

Katakri, Risk management, Riskassesment, Security management, Katakri 2015

Lyhenne luettelo

DSA	Designated Security Authority, Määrätty turvallisuusviranomainen
EK	Elinkeinoelämänkeskusliitto
EU	The European Union, Euroopan Unioni
FSC	Facility Security Clearance, Yhteisöturvallisuustodistus
GSA	General Security Agreement, Kansainvälinen turvallisuussopimus
ISO	International Organization for Standardization, Kansainvälinen standardisoimisliitto
Katakri	Kansallinen turvallisuusauditointikriteeristö
Katakri 2015	Tietoturvallisuuden auditointityökalu viranomaiselle
LVM	Liikenne- ja viestintäministeriö
NCSA	National Communication Security Authority, Kansallinen tietoturvallisuusviranomainen
NSA	National Security Authority, Kansallinen turvallisuusviranomainen
PSCC	Personnel Security Clearance Certificate
PLM	Puolustusministeriö
PSC	Personal Security Clearance, Henkilöturvallisuustodistus
PSI	Programme Security Instructions
RFV	Request for Visit, Vierailulupapyyntö
SAA	Security Accreditation Authority
SAL	Security Aspects Letter
SCG	Security Classification Guide
SM	Sisäministeriö
UM	Ulkoministeriö
VAHTI	Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
VM	Valtiovarainministeriö
VNK	Valtioneuvoston kanslia

Sisällys

1 Johdanto

Etsin mielenkiintoista opinnäytetyöaihetta ja Laurean Alumnien verkoistumistilaisuuksien avulla opinnäytetyöni keskeiseksi aiheeksi valikoitui Katakri 2015 ja sen merkittävimmät muutokset. Opinnäytetyö antoi myös mahdollisuuden päästä tutustumaan uuteen Katakri 2015 - auditointityökaluun ennen sen julkistamista. Etenkin Katakrin toiseen versioon olin koulussa jo ehtinyt tutustua jo jonkin verran, joten Katakrista yleensä oli jo jonkin verran pohjatietoa, vaikka pääosin vasta pintaraapaisun tasolta. Huomasin että Katakrista oli tehty runsaasti case study – tyyppisiä opinnäytetöitä, mutta Katakria itsessään ei ollut juurikaan tarkasteltu. Havainto herätti mielenkiintoni Katakria kohtaan. Katakri 2015 – auditointityökalun tuottamisen prosessi oli myös edennyt samalla pitkälle, se olisi myös jo hyvin lyhyessä ajassa kolmas versio Katakrista, joten katsaus siihen mitä oli versioiden välissä tapahtunut kiinnosti minua. Nyt olisi loistava tilaisuus tutustua Katakriin, sekä Katakri 2015 – auditointityökaluun opinnäytetyön muodossa. Kahdessa eri Laurean Aluminien verkostoitumistilaisuudessa aihetta palloteltiin Katakri 2015 – auditointityökalun työryhmään kuuluneen henkilön kanssa ja saimme aiheetta riittävästi rajattua, jotta sain opinnäytetyö prosessin käyntiin. Verkostoitumistilaisuuksien välissä myös Katakri 2015 – auditointityökalu työryhmän työ eteni kohti loppua. Hän lupautui auttamaan opinnäytetyöni ohjauksessa tarjoamalla tietoa, sekä auttamalla löytämään henkilöitä joilla olisi aikaa, sekä annettavaa opinnäytetyölleni.

Opinnäytetyöni aiheen rajauksen kautta päätutkimuskysymykseksi muotoilin:”Miksi Katakri on muttunut?” Ja lisäkysymyksiksi:”Miten Katakri on muuttunut?” ja ”Miksi Katakri uudistettiin? ”. Tavoitteena opinnäytetyössä on tuoda esiin Katakrin historiaa, sekä olennaisimmat muutokset Katakri 2015 – auditointityökalussa. Näitä tullaan opinnäytetyössä tarkastelemaan Katakrin versioissa annetuilla tiedoilla, asiantuntijoille suunnatulla esikartoitus kyselyllä, pyytämällä lausuntoja sekä haastatteluja Katakri 2015 – auditointityökalun työryhmän jäseniltä. Samoin määrätyiltä kansallisilta viranomaisilta ja kansalliselta turvallisuusviranomaiselta pyrin saamaan lausuntoja tai haastatteluja. Katakreihin tutustuminen ja esikartoituskyselytutkimus antavat pohjan tiedoille joita pyrin saamaan tai tarkentamaan lausuntojen ja haastattelujen avulla.

Opiskellessani Katakrin toisesta versiosta on tuotu asioita esiin, samoin auditointia kokonaisuutena on tarkasteltu. Henkilöstöturvallisuus, hallinnollinen turvallisuus, tietoturvallisuus, sekä fyysinen turvallisuus ovat merkittäviä osio opintojani, näitä tulen syventämään entisestään opinnäytetyötä tehdessä. Tietojen syventäminen, sekä kertaaminen ja Katakrin tuntemus edesauttavat minne tahansa tulen jatkossa työelämässä sijoittumaan turvallisuuden asiantuntijana.

Opinnäyteyössäni teoripohajana käytetään Katakrista löytyviä osa-alueita, sekä siihen oleellisesti liittyviä asioita. Näitä ovat fyysinen turvallisuus, turvallisuusjohtaminen, hallinnollinen turvallisuus, henkilöstöturvallisuus sekä tietoturvallisuutta. Riskienarvioinnin teoriaa käsittelen myös, koska sillä on vielä merkityksellisempi rooli Katakri 2015 – auditointityökalussa kuin aiemmissa Katakrin versioissa. Tärkeimpinä lähteinä teoriaan ovat Katakrien versiot, viranomaislähteet, sekä teorian termeihin oleellisesti liittyvästä kirjallisuudesta ja sähköisistä lähteistä.

1 Yleistä Katakrista

Kansallisena turvallisuusviranomaisena toimii ulkoasianministeriö ja tämä tehtävä perustuu kansainvälisistä tietoturvallisuusvelvoitteista annetuun lakiin (2004/588). Ulkoministeriö toimii kansallisen turvallisuusviranomaisen roolissa (National security authority, NSA). Sen tehtävänä on erityisesti ohjata ja valvoa, että kansainväliset turvallisuusluokitellut tietoaineistot suojataan ja niitä käsitellään asianmukaisesti sekä valtionhallinnossa että yrityksissä. Kansallinen turvallisuusviranomainen koordinoi määrättyjen turvallisuusviranomaisten toimintaa ja edustaa Suomea kansainvälisissä turvallisuuskomiteoissa ja –työryhmissä sekä osallistuu kansainvälisten turvallisuussääntöjen valmisteluun. Lisäksi Kansallinen turvallisuusviranomainen neuvottelee kahdenvälisiä, sekä monenvälisiä tietoturvallisuussopimuksia ja myöntää henkilö- sekä yhteisöturvallisuustodistuksia kansainvälistä yhteistyötä varten. Kansallinen turvallisuusviranomainen huolehtii myös tietoturvallisuusrikkomusten selvittämisestä, sekä ohjaa ja hallinnoi Katakriin liittyvää toimintaa. Toimeenpanevina, määrättyinä turvallisuusviranomaisina (Designated security authority, DSA) toimivat Puolustusministeriö, Pääesikunta ja Suojelupoliisi, joille on jaettu omat vastuualueet kansallisen turvallisuusviranomaisen kokonaisvastuukentästä. Viestintävirasto toimii määrättynä tietoliikenneturvallisuusviranomaisena (National Communications Security Authority, NCSA) niissä tapauksissa, joissa on kyse teknisestä tietoturvallisuudesta ja tietoliikenteen turvallisuudesta. (Turvallisuusviranomaisten käsikirja 2015, 6-7.)

Kansainvälisillä tietoturvallisuusvelvoitteilla tarkoitetaan Suomen tekemän tietoturvallisuussopimuksen (General Security Agreement, GSA) määräyksiä erityissuojattavan tietoaineiston suojaamisesta. Erityissuojattava tietoaineisto on määritelty koskemaan salassa pidettäviä asiakirjoja sekä materiaaleja, joissa on toisen valtion tai kansainvälisen järjestön tietoturvallisuussopimuksen mukaisesti tekemä turvallisuusmerkintä. Kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia (2004/588) sovelletaan myös yritykseen sekä yrityksen työntekijöihin silloin, kun yritys on sopimuspuolena tai alihankkijana turvallisuusluokitellussa hankkeessa tai osallistuu tällaista sopimusta edeltävään tarjouskilpailuun. Näin ollen erityissuojattavan tietoaineiston suojaamista koskevat velvoitteet sitovat myös yritystä. (Turvallisuusviranomaisten käsikirja yrityksille 2015, 4.)

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (2004/588) tarkoittamana määrättyinä turvallisuusviranomaisina toimivat Puolustusministeriö, Pääesikunta, Suojelupoliisi ja Viestintävirasto. Ne huolehtivat laissa säädetyistä kansallisista ja kansainvälisistä tietoturvallisuusvelvoitteista johtuvista tehtävistä. Suojelupoliisi on turvallisuusselvityslaissa (726/2014) tarkoitettu toimivaltainen viranomainen, jolla on yleinen toimivalta päättää turvallisuusselvitysten tekemisestä. Suojelupoliisi päättää henkilöturvallisuusselvityksen ja yritysturvallisuusselvityksen laatimisesta, ellei tehtävä kuulu Pääesikunnalle. Suojelupoliisi toimii myös määrättynä turvallisuusviranomaisena ja kansallisen turvallisuusviranomaisen asiantuntijana kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa, erityisesti henkilöstö-, yritys- sekä toimitilaturvallisuutta koskevissa asioissa. Puolustusministeriö ohjaa hallinnonalansa määrättynä turvallisuusviranomaisena toimintaa ja osallistuu kansainväliseen yhteistyöhön kansallisen turvallisuusviranomaisen asiantuntijana. Lisäksi puolustusministeriö hyväksyy kansainvälisten hankkeiden turvallisuusasiakirjat ja ohjeistaa niiden laatimisessa hallinnonalallaan. Pääesikunta tekee henkilöturvallisuusselvitykset puolustushallinnon henkilöstön osalta samoin yhteisöturvallisuusselvitykset, kun on kyse kotimaisista puolustushallinnon hankkeista. Tämän lisäksi Pääesikunta toimii Suojelupoliisin tapaisesti määrättynä turvallisuusviranomaisena kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa. Viestintävirasto toimii kansallisena tieto- sekä tietoliikenneturvallisuudesta vastaavana viranomaisena. Sen tehtäviin kuuluu kansainvälistä turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien hyväksyntä, Security Accreditation Authority (SAA). Tietojärjestelmien ja tietoliikennejärjestelyiden turvallisuutta tarkastelevien asioiden osalta viestintävirasto toimii kansallisen turvallisuusviranomaisen asiantuntijana. Viestintävirasto voi osana yritysturvallisuusselvityksen muodostaa tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa tarkastelevan selvityksen. (Turvallisuusviranomaisten käsikirja 2015, 6-7.)

Toimivaltaiset viranomaiset toteuttavat yritysten tai muiden kohteiden turvallisuustason tarkastamisen joko valtionhallinnon salassa pidettävää tietoa sisältäviin hankkeisiin liittyen tai kansainvälisen pyynnön seurauksena. Jälkimmäisessä tapauksessa tilanne on usein se, että suomalainen yritys voi osallistua kansainväliseen tarjouskilpailuun täyttäessään hankkeen turvallisuusvaatimukset. Vaatimukset täyttävälle yritykselle toimivaltainen viranomainen voi myöntää Facility Security Clearance (FSC)-todistuksen. (KATAKRI puolustusministeriö 2011.)

1.1 Yritysturvallisuusselvitys

Katakri on työväline, auditointyökalu, joka on tietyllä tapaa tiekartta. Siihen koottujen kriteereiden noudattamisella ja sen osoittamisella on mahdollista saada yritykselle, organisaatiolle tai henkilölle tarvittavat turvallisuusselvitystodistukset. Näin organisaatio tai henkilö voi

olla mukana tai osana turvallisuusluokiteltua tietoa käsittelevissä hankkeissa tai tarjouskilpailuissa. Niissa annetaan turvallisuusluokiteltua tietoa käyttöön jo tarjousvaiheessa tai viimeistään, kun tarjouskilpailu on voitettu.

Turvallisuusluokiteltua tietoa käsittelevä tai sisältävä hankinta lähtee käyntiin pääsääntöisesti niin, että hankintayksikkö ilmoittaa alustavat tiedot varsinaisesta hankinnasta. Pääsääntöisesti tämä vaihe ei edellytä turvallisuusluokitellun tiedon luovuttamista mahdollisille tarjoajille. Vasta seuraavassa osassa prosessia hankintayksikkö tekee tarjouspyynnön, josta hanketta koskevat turvallisuusvaatimukset tuodaan esiin. Turvallisuusluokitellun tiedon suojaaminen asettaa yritykselle erityisvaatimuksia ja saattaa lisätä hankinnan kustannuksia. Jos tarjouspyyntöasiakirjat sisältävät turvallisuusluokiteltua tietoa, niiden käsittely voi edellyttää käsittelyyn osallistuvan henkilön henkilöturvallisuusselvitystä tai selvityksen perusteella annettavaa henkilöturvallisuusselvitystodistusta, Personnel Security Clearance Certificate (PSCC). Mikäli yritys käsittelee turvallisuusluokiteltuja tietoja sisältäviä tarjouspyyntöasiakirjoja tiloissaan, voi hankintayksikkö jo tässä vaiheessa edellyttää myös yrityksestä laadittavaa yritysturvallisuusselvitystä, Facility Security Clearance (FSC). Yritysturvallisuusselvitys käynnistetään viimeistään siinä vaiheessa, kun yrityksen osallistuminen turvallisuusluokiteltua tietoa sisältävään hankintaan varmistuu, mikäli hankinta edellyttää yritysturvallisuusselvitystä. Ennen varsinaisen hankkeen käynnistymistä yritys ja hankintayksikkö tekevät turvallisuusluokiteltua tietoa sisältävää hankintaa koskevan sopimuksen (Classified Contract), mikä sisältää kaikki hankekohtaiset turvallisuusvaatimukset ja turvallisuusasiakirjat. Jos hankinta on kansainvälinen ja sen turvallisuusvaatimukset ovat monitahoiset, laaditaan pääsääntäisesti hankkeeseen hyvin tyhjentävä hanketurvallisuusohje, Programme security instructions (PSI). Joko hanketurvallisuusohjetta täydentävästi tai vaihtoehtoisesti voidaan turvallisuutta koskeva lisälauseke, (Security Aspects Letter, SAL) laatia. Turvallisuutta koskevaa lisälauseketta käytetään yleensä tarjouspyyntövaiheessa ja se on useimmiten hanketurvallisuusohjetta suppeampi dokumentti. Turvallisuusdokumentaatiossa on mukana pääsääntöisesti myös turvallisuusluokitteluohje, Security Classification Guide (SCG). (Turvallisuusviranomaisten käsikirja 2015, 16-19.)

Yritysturvallisuusselvitystä voidaan edellyttää, jos yritys käsittelee tiloissaan turvallisuusluokiteltuja asiakirjoja tasolla LUOTTAMUKSELLINEN (TL III) tai SALAINEN (TL II). Kansainvälisen turvallisuusluokitellun tiedon osalta vastaavat tasot ovat CONFIDENTIAL tai SECRET. Alimmalla KÄYTTÖ RAJOITETTU -tasolla ei useimmiten vaadita yritysturvallisuusselvitystä. Korkeimmalle luokiteltua tietoa (ERITTÄIN SALAINEN/TOP SECRET) ei yleensä luovuteta yrityksille. Yritysturvallisuusselvitys laaditaan turvallisuusselvityslain (726/2014) vaatimalla tavalla. Turvallisuusselvityslain tavoitteena on ennakolta kyetä ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita ja yleistä turvallisuutta erilaisilla tavoilla. Lain avulla osana yleisen edun suojaa turvataan turvallisuutta ja yhteiskunnan

toimivuuden kannalta kriittisen infrastruktuurin toimivuutta riippumatta siitä, onko kysymys julkishallinnossa vai yksityissektorilla hoidettavasta tehtävästä. Turvallisuusselvityslain tavoitteena on kansainvälisesti yleisesti noudatettavia sääntöjä ja käytäntöjä tuoda lähemmäksi alan lainsäädäntöä vastaamaan. Vain viranomainen voi hakea yritysturvallisuusselvitystä kansallisen turvallisuusluokitellun tiedon suojaamiseksi. Kun viranomainen tekee hankintasopimusta yrityksen kanssa silloin, kun sopimuksen teon yhteydessä yritykselle annetaan turvallisuusluokiteltuja dokumentteja, voidaan yritysturvallisuusselvitys laatia perustuen kansalliseen tarpeeseen. Yritysturvallisuusselvityksen laatimisesta sekä turvallisuusselvityksen tekemisestä päättää pääsääntöisesti Suojelupoliisi ja Pääesikunta tekee sen puolustusvoimien hankinnoissa. (Turvallisuusviranomaisten käsikirja 2015, 16.)

Kansainvälisten tietoturvallisuusvelvoitteiden edellyttämää yritysturvallisuusselvitystä voidaan pyytää Suomen viranomaisen toimesta, kun sopimukseen perustuen on yritykselle tarkoitus antaa pääsy toisen valtion tai kansainvälisen järjestön turvallisuusluokiteltuun tietoon, joka on määritelty vähintään tasolle CONFIDENTIAL. Tällöin viranomainen, joka selvitystä hakee, täydentää yritysturvallisuusselvityshakemuslomakkeen ja toimittaa sen kansalliselle turvallisuusviranomaiselle. Vaatimusten täyttyessä turvallisuusviranomainen välittää yritysturvallisuusselvityspyynnön edelleen Suojelupoliisille tai Pääesikunnalle, kun on kyse puolustusvoimien hankinnoista. (Turvallisuusviranomaisten käsikirja 2015, 16-17.)

Yritysturvallisuusselvitystä voi pyytää myös ulkomainen viranomainen, jonka tarkoituksena on tehdä turvallisuusluokiteltu sopimus (classified contract) suomalaisen yrityksen kanssa vähintään tasolle CONFIDENTIAL. Ulkomaan viranomainen lähettää oman maansa kansallisen turvallisuusviranomaisen kautta yritysturvallisuusselvitystä koskevan pyynnön Suomen kansalliselle turvallisuusviranomaiselle, joka välittää sen edellytysten täyttyessä Suojelupoliisiin tehtäväksi. Yritystä pyydetään tällöin täyttämään yritysturvallisuusselvityshakemus, sekä antamaan suostumuksensa yritysturvallisuusselvityksen tekemiseksi. Yritysturvallisuusselvitys voidaan pyytää myös, jos suomalainen yritys osallistuu kansainväliseen tarjouskilpailuun, joka edellyttää turvallisuusluokiteltuun tietoon pääsyä kansainvälisessä järjestössä tai toisessa valtiossa, vähintään CONFIDENTAL tasolla. Yritys tai organisaatio tekee tällöin yritysturvallisuusselvityshakemuksen ja toimittaa sen kansalliselle turvallisuusviranomaiselle, joka vaatimusten täyttyessä välittää Suojelupoliisille hakemuksen. (Turvallisuusviranomaisten käsikirja 2015, 16-17.)

Itse yritysturvallisuusselvityksenhakemus (Liite 5) on määrämuotoinen hakulomake, joka löytyy esimerkiksi Suojelupoliisin verkkosivuilta. Pääesikunnan laatiessa yritysturvallisuusselvitystä hakemukset tehdään erikseen ohjeistetulla puolustusvoimien lomakkeella, sekä niiden omalla sisäisellä menettelyllä. Yritysturvallisuusselvityksessä voidaan turvallisuusselvityslain (726/2014 38 §) mukaisesti selvittää yrityksen osalta sen kykyä suojata tietoa oikeudettomalta

ilmitulolta, muuttamiselta ja hävittämiseltä. Lisäksi voidaan selvittää sen kykyä estää asiattoman pääsy tiloihin, joissa tietoja käsitellään tai joissa harjoitetaan mahdollisesti muuta selvityksen perusteena olevaa toimintaa. Voidaan myös selvittää sen kykyä ohjata ja kouluttaa henkilöstöään asianmukaisesti Näiden turvallisuustoimenpiteiden toteutumista saadaan selvittää itse yritysturvallisuusselvityshakemuksessa esiin tuotujen tietojen, sekä turvallisuusselvityslain (726/2014 37 §) määriteltyjen tietolähteiden avulla sekä yritykseen sekä sen toimitiloihin ja tietojärjestelmiin kohdistuvien tarkastusten avulla. Yritysturvallisuusselvitys tehdään pääsääntöisesti tasolle TL II SALAINEN/SECRET tai TL III LUOTTAMUKSELLINEN/CONFIDENTIAL. KÄYTTÖ RAJOITETTU/RESTRICTED -tasolla yritysturvallisuusselvitystä ei yleensä tehdä. Auditointityökaluna voidaan käyttää KATAKRIa, kun selvitykseen kuuluvia tarkastuksia tehdään. KATAKRIa käytetään auditointityökaluna, kun tehdään Kansainvälisen tietoturvallisuusvelvoitteen perusteella tehtävää yritysturvallisuusselvitystä. Viranomainen tarkastaa pääsääntöisesti yrityksen tilaturvallisuuden ja hallinnollisen- sekä henkilöstö turvallisuuden, kun se arvioi yrityksen turvallisuustasoa. Yrityksen käsitellessä turvallisuusluokiteltua tietoa sen tietojärjestelmissä voidaan myös yrityksen tietojärjestelmien turvallisuus tarkastella, tarkastuksen niihin suorittaa Viestintävirasto. (Turvallisuusviranomaisten käsikirja 2015, 16-18.)

Yritysturvallisuusselvityksen osana voidaan laatia henkilöturvallisuusselvitykset yrityksen vastuuhenkilöistä ja niistä työntekijöistä yrityksessä, ketkä käsittelevät turvallisuusluokiteltua tietoa vähintään tasolla LUOTTAMUKSELLINEN/CONFIDENTIAL.Yritysturvallisuusselvitys voidaan tehdä myös osittaisena, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai se on perusteltua muulla tavalla yritysturvallisuusselvityksen tarkoituksen toteuttamiseksi. Jos yritykseltä ei edellytetä kykyä suojata turvallisuusluokiteltua tietoa toimitiloissaan (”FSC without safeguards”), arviointi voidaan kohdistaa myös ainoastaan yrityksen henkilöstö- ja hallinnolliseen turvallisuuteen. Jos yritykseltä edellytetään myös kykyä suojata turvallisuusluokiteltuja tietoja yrityksen toimitiloissa (”FSC with safeguards”), arviointi voidaan kohdistaa lisäksi yrityksen toimitiloihin, sekä tekniseen tietoturvallisuuteen soveltuvin osin. Mikäli turvallisuusluokiteltuja tietoja käsitellään myös tietojärjestelmässä (”including CIS”), voidaan arvioida yrityksen tekninen tietoturvallisuus. Suojelupoliisin tekemät yritysturvallisuusselvitykset ovat maksullisia poliisin maksuasetuksen (1023/2014) mukaisesti. Yritysturvallisuusselvityksen päättyy prosessina sitoumukseen, jossa yritys sitoutuu ylläpitämään vaaditun turvallisuustason, sen pohjalta yritykselle voidaan myöntää yritysturvallisuusselvitystodistus. (Turvallisuusviranomaisten käsikirja 2015, 16-18.)

”Yritysturvallisuusselvityksistä säädetään turvallisuusselvityslaissa (726/2014). Yritysturvallisuusselvityksessä toimivaltainen viranomainen voi selvittää laissa mainittujen tietolähteiden, yritysten vastuuhenkilöiden henkilöturvallisuusselvitysten sekä yritykseen ja sen toimitiloihin kohdistuvan tarkastusten avulla, miten yritys kykenee huolehtimaan tietoturvallisuutta koske-

vista turvallisuusvelvoitteistaan. Tarkasteltavia turvallisuusjärjestelyjä ovat muun muassa salassa pidettävien tietojen suojaaminen oikeudettomalta paljastumiselta, asiattoman pääsyn estäminen tiloihin, joissa salassa pidettäviä tietoja käsitellään, sekä henkilöstön ohjeistaminen ja kouluttaminen. Katakria voidaan käyttää työkaluna, kun arvioidaan yrityksen toimitiloihin ja tietojärjestelmiin kohdistuvan tarkastuksen avulla yrityksen kykyä huolehtia tietoturvallisuusjärjestelyistä." (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

1.2 Henkilöturvallisuusselvitys

Henkilöturvallisuusselvitys ja –todistus (Personnel Security Clearance, PSC) voidaan edellyttää turvallisuusvaatimuksissa hankinnassa. Se voidaan myös tehdä henkilöstä, joka hankinnan yhteydessä käsittelee tietoa, joka on turvallisuusluokiteltua. Pääsääntöisesti kansainvälisen tietoturvallisuusvelvoitteen mukaista henkilöturvallisuusselvitystodistusta edellytetään tilanteessa, jossa henkilö on oikeutettu pääsemään kansainväisen organisaation tai toisen valtion turvallisuusluokiteltuun tietoon, joka on tasolla CONFIDENTIAL tai korkeammaksi. Henkilöturvallisuusselvitykset tehdään useinmiten yritysturvallisuusselvityksen yhteydessä, mutta on tiettyjä tilanteitta joissa pelkkä henkilöturvallisuusselvitys riittää hankintaan osallistumiseen, selvimpänä esimerkkinä tilanne jossa tietoja päästään käsittelemään vain viranomaisen tiloissa. Osana yritysturvallisuusselvitystä voidaan tehdä yrityksen vastuuhenkilöistä henkilöturvallisuusselvitykset. (Turvallisuusviranomaisten käsikirja 2015, 19.)

Pääsääntöisesti se viranomainen, jonka kansallisesta turvallisuusluokitellusta tiedosta on kyse, hakee tiedon osalta turvallisuusselvitystä. Yrityksen on mahdollista myös tietyin perustein hakea henkilöturvallisuusselvityksen laatimista yrityksen oman tiedon suojaamiseksi esimerkiksi tietojen kansantaloudellisen vaikuttavuuteen perustuen. Turvallisuusselvitystä haetaan vakiomuotoisella lomakkeella. Kansainvälisen turvallisuusluokitellun tiedon osalta toimitetaan turvallisuusselvityksestä henkilöturvallisuustodistuksen saamiseksi pyyntö Suomen kansalliselle turvallisuusviranomaiselle, hankinnasta vastaavan Suomen viranomaisen tai ulkomaan viranomaisen toimesta. Henkilöturvallisuustodistusta varten täytetään henkilöturvallisuustodistus-hakemuslomake(Liite 8), joka löytyy täyttöohjeineen kansallisen turvallisuusviranomaisen sivuilta. Lomake on tarkoitettu vain Suomen viranomaisten ja yritysten käyttöön haettaessa Suomen kansallisen turvallisuusviranomaisen myöntämää henkilöturvallisuustodistusta. Lomakkeeseen liitetään turvallisuusselvityshakemus, perusteet hakemukselle, sekä muut pyydetyt liitteet ja hakemus toimitetaan kansalliselle turvallisuusviranomaiselle, joka arvioi onko turvallisuusselvitykselle kansainvälisen tietoturvallisuusvelvoitteen mukaisesti peruste ja toimittavat perusteiden täyttyessä sen Suojelupoliisille. Puolustusvoimien hankinnoista on oma Puolustusvoimien ohjeistus. (Turvallisuusviranomaisten käsikirja 2015, 19.)

Henkilöturvallisuusselvitykset tehdään siten kuin turvallisuusselvityslaissa (726/2014)

säädetään. Toimivaltainen viranomainen tarkastaa kohteena olevan henkilön taustatiedot henkilöturvallisuusselvityksessä, laissa säädetyllä menettelyllä, sen tekemiseen edellytetään henkilön kirjallista suostumusta, joka annetaan osana hakulomaketta, siinä ilmoitetaan samalla myös henkilön työnkuva ja rooli hankkeen yhteydessä. Huomioitavaa on, että turvallisuusselvitys voidaan tehdä ulkomaalaisesta, kuka on suomalaisen yrityksen palveluksessa, mutta suomalaisilla viranomaisilla voi olla rajalliset mahdollisuudet henkilön taustan selvittämiseen. Turvallisuusselvityslaissa osoitetaan tyhjentävästi turvallisuusselvityksessä käytettävät rekisterit. Toimivaltaisilla viranomaisilla on lain mukaan mahdollisuus tehdä kysely selvityksen kohteena olevan henkilön rekisteritiedoista myös ulkomaan viranomaisille. Kun turvallisuusselvityksen kohteena on ulkomaalainen tai ulkomailla asuva tai asunut suomalainen, ilmoitetaan turvallisuusselvityksen tuloksen yhteydessä se, miltä ajanjaksolta viranomaisilla on ollut tietoa käytössään. Tarvittaessa Suomen kansallinen turvallisuusviranomainen voi ulkomaan kansalaisen osalta pyytää valtioiden välisen tietoturvallisuussopimuksen perustella turvallisuusselvitystä vastaavaa henkilöturvallisuustodistusta henkilön kotimaan kansalliselta turvallisuusviranomaiselta. Henkilöturvallisuusselvityksessä Suojelupoliisi tai Pääesikunta ei ota kantaa selvityksen kohteen soveltuvuuteen tehtäväänsä, vaan arvioi rekistereistä ilmi tulevien tietojen perusteella, mitkä tiedot voivat selvityksen tarkoituksen kannalta olla merkityksellisiä. Tällaiset tiedot ilmoitetaan kirjallisesti hakijalle. (Turvallisuusviranomaisten käsikirja 2015, 20.)

Haettaessa henkilöturvallisuusselvityksen kohteesta henkilöturvallisuustodistusta, tiedot ilmoitetaan myös kansalliselle turvallisuusviranomaiselle, joka harkitsee selvityksessä ilmenneiden tietojen perusteella, voidaanko henkilöturvallisuustodistus myöntää. Kansallinen turvallisuusviranomainen välittää tiedon myönnetystä henkilöturvallisuustodistuksesta hakijalle. Henkilöturvallisuustodistus voidaan tietyillä edellytyksillä myös peruuttaa. Selvityksen kohteella on turvallisuusselvityksistä annetun lain mukaan oikeus saada tieto siitä, onko hänestä tehty turvallisuusselvitys tiettyä tehtävää varten sekä oikeus saada pyynnöstään turvallisuusselvityksen hänestä sisältämät tiedot. Tätä tiedonsaantioikeutta voi käyttää sopimalla henkilökohtaisen tapaamisajan Suojelupoliisissa tai Pääesikunnassa. On kuitenkin huomattava, että tiedonsaantioikeutta ei ole, jos tieto on peräisin sellaisesta rekisteristä, johon rekisteröidyllä ei ole tarkastusoikeutta, näistä esimerkkinä Suojelupoliisin toiminnallinen tietojärjestelmä, näissä tapauksissa selvityksen kohde voi pyytää tietosuojavaltuutettua tarkastamaan tietonsa. (Turvallisuusviranomaisten käsikirja 2015, 19.)

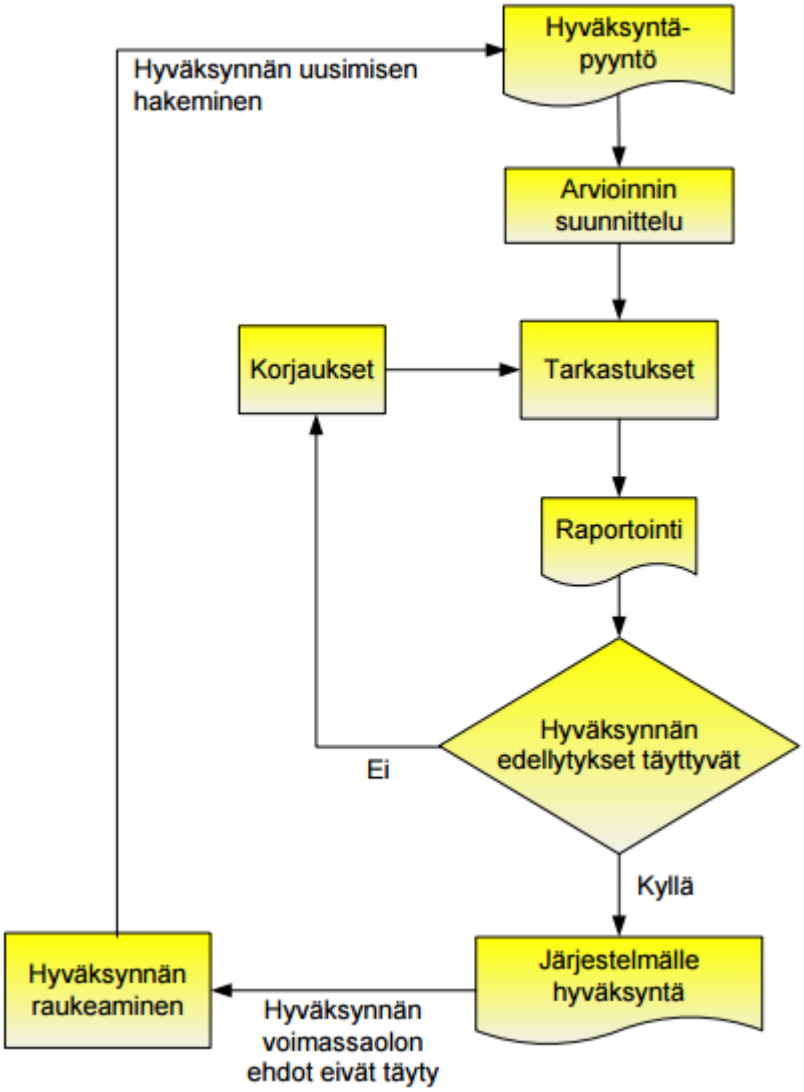
1.3 Tietojärjestelmien hyväksyntä

Tietojärjestelmien hyväksynnän, akkreditoinnin, myöntää Viestintävirasto osana yritysturvallisuusselvitystä. Hankintaan liittyviä turvallisuusluokiteltuja tietoja käsiteltäessä yrityksen tie-

tojärjestelmässä, on se hyväksytettävä hankinnan turvallisuusvaatimuksissa edellytetylle turvallisuustasolle. Hyväksyntä on prosessi, jonka aikana Viestintävirasto määrittää yhdessä tietojärjestelmän omistajan kanssa tietojärjestelmään kohdistuvan riskitason ja hyväksyy sen mukaiset turvallisuusjärjestelyt. Hyväksyntäprosessissa käytetään auditointityökaluna Katakria. Kansainvälistä luokiteltua hanketta koskevasta sopimuksesta tai muista kansainvälisistä velvoitteista saattaa aiheutua turvallisuusvaatimuksiin tarkentavia määräyksiä. Hyväksyntäprosessi alkaa, kun Viestintävirastolle toimitetaan hyväksyntäpyyntö. Hyväksyntäprosessin keskeisiä vaiheita ovat arvioinnin suunnittelu, tarkastukset, toisin sanoen auditoinnit, sekä raportointi. Mikäli tarkastuksessa havaitaan, että jokin hankkeen turvallisuusvaatimuksista ei täyty, merkitään tämä poikkeamaksi. Havaittujen poikkeamien tulee olla todennetusti korjattuja ennen kuin hyväksyntä voidaan myöntää. (Turvallisuusviranomaisten käsikirja 2015, 22.)

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) mukaisesti viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden arvioinnissa Viestintävirastoa tai Viestintäviraston hyväksymää tietoturvallisuuden arviointilaitosta. Katakria voidaan käyttää työkaluna selvitettäessä, miten viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tietoturvallisuudesta on huolehdittu suhteessa kansallisiin tai kansainvälisiin suojausvaatimuksiin. Katakrin käytön tulee perustua myöskin viranomaisten tietojärjestelmien turvallisuuden arvioinnissa järjestelmälliseen riskienarviointiin, sen pohjalta soveltuviksi valittaviin suojausvaatimuksiin ja niiden täyttymisen arviointiin toteutusesimerkkejä hyödyntäen. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen prosessi(kuvio 1).



Kuvio 1 Tietojärjestelmien hyväksyntäprosessi (Turvallisuusviranomaisten käsikirja 2015, 22)

Hyväksynnän myöntämisen yksi keskeinen edellytys on, että tarkastuksen kohde sitoutuu turvallisuustasonsa säilyttämiseen. Hyväksynnän voimassaolo raukeaa, mikäli tarkastetussa kohteessa tapahtuu olennainen sen turvallisuuteen vaikuttava muutos. Näitä voivat olla esimerkiksi merkittävät verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset. Tavanomaisesta ylläpitämisestä aiheutuvat muutokset, joista esimerkkinä ohjelmistojen turvapäivitysten asennukset, eivät aiheuta hyväksynnän raukeamista. Tapauskohtaiset ehdot hyväksynnän raukeamiselle määritellään hyväksynnän myöntämisen yhteydessä. Merkittävät turvallisuuteen vaikuttavat muutokset tulee ennen käyttöönottamista tai asentamista, hyväksyttää Viestintävirastolla. (Turvallisuusviranomaisten käsikirja 2015, 22.)

”Tietojärjestelmien turvallisuuden arviointiprosessi (L 1406/2011) alkaa, kun arvioinnin kohde toimittaa Viestintävirastolle arviointipyynnön. Arviointiprosessin keskeisiä muita vaiheita ovat arvioinnin suunnittelu, tarkastukset sekä raportointi. Arviointiprosessia on havainnollistettu

yksinkertaistetussa muodossaan yllä olevassa kuvassa. Arviointiprosessia voidaan hyödyntää esimerkiksi kohdeorganisaation sisäisen turvallisuustyön tukena, jättäen muun muassa jäännösriskien käsittelyn täysin kohdeorganisaation vastuulle. Arviointiprosessia kuvataan yksityiskohtaisemmin ohjeessa "Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma”.” (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

”Viestintäviraston hyväksyntään tai todistukseen tähtäävä hyväksyntäprosessi (L 588/2004, L 726/2014 tai 1406/2011) alkaa, kun arvioinnin kohde toimittaa Viestintävirastolle hyväksyntä- tai todistuspyynnön. Hyväksyntäprosessi mukailee arviointiprosessia eroten siitä siten, että tarkastuksissa mahdollisesti havaittujen poikkeamien tulee olla todennetusti korjattuja ennen kuin hyväksyntä tai todistus voidaan myöntää. Hyväksyntäprosessia on havainnollistettu yksinkertaistetussa muodossaan kuviossa 1 yllä. Hyväksyntäprosessia voidaan hyödyntää esimerkiksi silloin, kun arvioinnin kohde haluaa osoittaa tietojärjestelmänsä suojausten vaatimustenmukaisuuden Viestintäviraston hyväksynnällä tai todistuksella. Hyväksyntäprosessissa riskienarviointi toteutetaan hyödyntäen sekä kohdeorganisaation, että Viestintäviraston arvioita. Hyväksyntäprosessia kuvataan yksityiskohtaisemmin ohjeessa "Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma".”(KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

”Viestintävirasto voi myöntää vaatimukset täyttävälle kansainvälistä suojattavaa tietoa käsittelevälle järjestelmälle hyväksynnän (accreditation). Vaatimukset täyttävälle kansallista suojattavaa tietoa käsittelevälle järjestelmälle Viestintävirasto voi myöntää todistuksen vaatimustenmukaisuudesta. Sekä hyväksynnän että todistuksen myöntäminen edellyttää, että tarkastuksen kohde sitoutuu turvallisuuden tason säilyttämiseen. Sekä hyväksynnän että todistuksen voimassaolo raukeaa, mikäli tarkastetussa kohteessa tapahtuu merkittävä sen turvallisuuteen vaikuttava muutos. Tällaisia voivat olla esimerkiksi merkittävät verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset. Tavanomaisesta ylläpidosta aiheutuvat muutokset, kuten esimerkiksi ohjelmistojen turvapäivitysten asennukset, eivät aiheuta voimassaolevan hyväksynnän tai todistuksen raukeamista. Tapauskohtaiset ehdot hyväksynnän tai todistuksen raukeamiselle määritellään hyväksynnän tai todistuksen myöntämisen yhteydessä. Merkittävät muutokset tulee hyväksyttää etukäteen Viestintävirastolla. Viestintävirastolla on mahdollisuus myöntää järjestelmälle todistus tai hyväksyntä pohjautuen hyväksytyn arviointilaitoksen suorittamaan arviointiin (1405/2011). Myöntämisen keskeisinä ehtoina ovat tehtyjen tarkastusten rajausten yhteneväisyydet haettavan todistuksen tai hyväksynnän rajauksiin sekä toimitettujen arviointiraporttien sisältämien tietojen riittävyys. Todistusta tai hyväksyntää varten Viestintävirasto suorittaa tarvittaessa tarkentavia arviointeja tai pyytää tilaajaorganisaatiolta lisäselvitystä sen selvittämiseksi ja varmistamiseksi, että kohde täyttää

soveltuvat tietoturvallisuusvaatimukset.”(KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

2 Katakri – Kansallinen turvallisuusauditointikriteeristö

Tässä luvussa tuon esiin, mistä tarpeesta Katakri on lähtöisin sekä millainen organisaatio sen taustalla oli. Lisäksi kerron, ketkä saivat suorittaa Katakriin pohjautuvan auditoinnin sekä miten Katakria käytettiin. Käyn myös läpi aikaisempien Katakrien tavoitteita, sekä mihin niitä käytettiin.

2.1 Työväline viranomaisten ja organisaatioiden käyttöön

Katakri eli Kansallinen turvallisuusauditointikriteeristö oli työväline organisaatioiden, viranomaisten ja yritysten yhteiskäyttöön. Katakria lähdettiin luomaan elinkeinoelämän aloittesta, jotta suomalaisilla organisaatioilla olisi myös mahdollisuus osallistua kansainvälsiin hankkeisiin. Katakri luotiin osana Suomen sisäisen turvallisuuden ohjelman toista vaihetta, jonka Suomen hallitus vahvisti syyskuussa 2008. Puolustusministeriö toimi ensimmäisen version luonnissa johtovastuullisena. Työryhmän tarkoituksena oli luoda viranomaisille ja yrityksille yhteinen turvallisuuskriteeristö, joka yhtenäistää Suomen turvallisuustasojen määrittelyä sekä parantaa sen omavalvontaa sekä auditointia. Kriteeristön laadinnassa käytettiin laajalti maamme turvallisuusasiantuntijoita niin viranomais-, yhteisö kuin yritysmaailmastakin, mahdollisimman kattavan ja käyttökelpoisen tuloksen takaamiseksi. Katakrin ensimmäinen versio julkaistiin 20.11.2009 ja se otettiin käyttöön vuoden 2009 lopulla. (Kansallinen turvallisuusauditointikriteeristö 2009.)

”Tämän kansallisen turvallisuusauditointikriteeristön ensimmäisenä päätavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa yrityksessä tai muussa yhteisössä kohteen turvallisuustason todentavan tarkastuksen, auditoinnin. Viranomainen voi tarpeen mukaan täydentää auditointia turvallisuusarvioinnilla, joissakin tapauksissa myös konsultoinnilla. Nämä toimet eivät kuitenkaan kuulu itse auditoinnin piiriin. Tässä turvallisuusauditointikriteeristön ensimmäisessä versiossa keskitytään ainoastaan ns. security-turvallisuuteen.” (KATAKRI puolustusministeriö 2009.)

”Turvallisuusauditointikriteeristön toinen päätavoite on auttaa yrityksiä ja muita yhteisöjä sekä myös viranomaisia sidosryhmineen omassa sisäisessä turvallisuustyössään. Kriteeristö sisältää tästä syystä erilliset, viranomaisvaatimusten ulkopuoliset lähtötason suositukset, joista toivotaan voitavan poimia kulloinkin käyttökelpoisia turvallisuuskäytänteitä ja edetä tätä kautta tarvittaessa viranomaisvaatimusten tasolle.” (KATAKRI puolustusministeriö 2009.)

”Turvallisuusauditointikriteeristö jakautuu neljään pääosioon: 1) hallinnollinen turvallisuus (turvallisuusjohtaminen), 2) henkilöstöturvallisuus, 3) fyysinen turvallisuus ja 4) tietoturvallisuus. Auditointitapahtumassa tulee huomioida näiden kaikkien neljän osion vaatimukset, toisin sanoen niitä ei ole rakennettu itsenäisiksi kokonaisuuksikseen. Jokaiselle osiolle on laadittu kolmiportainen vaatimusluokittelu, joka vastaa paraikaa laajamittaisesti käyttöön otettavia turvallisuustasokäsitteitä – perustaso, korotettu taso ja korkea taso. Niitä täydentävät edellä mainitut lähtötason suositukset. Kriteeristö on rakennettu ehdottomien vaatimusten näkökulmasta, eikä se sisällä joissakin kriteeristöissä käytettävää pisteytysmenettelyä. Tällä on pyritty siihen, ettei auditoinnin lopputulokseen jäisi mahdollisesti tunnistamattomia, mutta kriittisiä riskejä. Valittu menettely asettaa erityisiä vaatimuksia turvallisuusauditointeja toteuttavalle henkilöstölle, mihin pyritään vastaamaan riittävillä koulutustasovaatimuksilla.” (KATAKRI puolustusministeriö 2009.)

”Valtionhallinnolla on käytössään ja valmisteilla useita yhteiskunnan elintärkeiden toimintojen turvaamisen alaan liittyviä vaatimusmäärittelyjä, jotka omalta osaltaan täydentävät nyt käyttöön otettavaa turvallisuusauditointikriteeristöä. Kyseiset näkemykset on pyritty huomioimaan kriteeristötyössä. Merkittävänä rinnakkaisaineistona voidaan pitää erityisesti valtiovarainministeriön johdolla valmisteltuja tietoturvallisuuden ja varautumisen kokonaisuuksia linjaavia ohjeistoja. Turvallisuusauditointikriteeristön nyt julkaistavassa ensimmäisessä versiossa on huomioitu mahdollisimman pitkälle myös samanaikaisesti valmistelussa olleiden valtionhallinnon tietoturvallisuusasetuksen ja Euroopan Unionin uuden turvallisuusregulaation linjaukset. Kriteeristö täydentää lisäksi omalta osaltaan sekä kansainvälisiä tietoturvallisuusvelvoitteita, että turvallisuusselvityksiä säätäviin lakeihin sisältyviä menettelyjä.” (KATAKRI puolustusministeriö 2009.)

2.2 Katakri II

Loppukesästä 2011 julkaisiitn Katakrin toinen versio. Kriteeristön toinen versio sisälsi viranomaisvaatimusten ulkopuoliset elinkeinoelämän suositukset, jotka koostuvat sellaisista turvallisuuskäytänteistä, joiden kautta voitiin edetä viranomaisvaatimusten tasolle silloin, kun tarve sitä vaati. Kansallisen turvallisuusauditointikriteeristön päätavoitteena oli yhtenäistää viranomaistoimintoja, kohteen turvallisuutta organisaatioissa viranomaisten suorittaessa turvallisuustasoa todentavan tarkastuksen. Katakrin toisessa versiossa esitettyjä vaatimuksia tuli kansallisen turvallisuusviranomaisen organisaation käyttää. Toisena päätavoitteena oli auttaa organisaatioita niiden omassa sisäisessä turvallisuustyössä.

Katakrin toinen versio. suositusosioineen oli suunnattu myös perustyökaluksi yritysten omaehtoiselle turvallisuustyölle. On huomattava, että elinkeinoelämän suositukset eivät olleet viranomaisvaatimuksia. Suositusten toteuttaminen oli askel oikeaan suuntaan jota edetä, jos

viranomaisvaatimukset joudutaan täyttämään lähitulevaisuudessa. Katakrin toisessa version näkökulma oli ainoastaan security-turvallisuuteen. Se jakautui neljään pääosioon joita olivat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, sekä tietoturvallisuus. Jokaiselle edellä mainituista osioista oli laadittu yksityiskohtiin menevä kolmiportainen vaatimusluokittelu, joka noudatti valtionhallinnon tietoturvallisuuden tasokäsitteitä – perustaso, korotettu taso ja korkea taso. Näitä vastaavat turvallisuusluokkamerkinnät olivat KÄYTTÖ RAJOITETTU, LUOTTAMUKSELLINEN ja SALAINEN. Kansallinen turvallisuusauditointikriteeristö oli rakennettu ehdottomien vaatimusten näkökulmasta. Tavoitteena oli, ettei auditoinnin lopputulokseen jäisi mahdollisesti tunnistamattomia, mutta kriittisiä riskejä. Valittu menettely asetti erityisiä vaatimuksia turvallisuusauditointeja toteuttaville henkilöstölle, koska vaatimusten toteuttamisvariaatiot vaihtelevat kohteittain.” (KATAKRI puolustusministeriö 2011.)

Kansallinen turvallisuusauditointikriteeristö, Katakri oli tarkoitettu työvälineeksi niille viranomaisille tai viranomaisten lukuun toimiville turvallisuustarkastajille, auditoijille, joille oli annettu valtuus todentaa auditoinnin kohteen turvallisuuden taso erityisesti Katakrin kriteereihin peilaten. Auditointi tehtävään hyväksyttiin valtionhallinnon taholta vain erillisen turvallisuusauditoijan koulutuksen saaneita henkilöitä. Laajamittainen turvallisuusauditoijan koulutus käynnistyi ammattikorkeakoulutasoisena syksyllä 2011. Tämän lisäksi täydennyskoulutuksena annettavaa turvallisuusauditointikoulutusta pystyvät hyödyntäämään ne henkilöt, joiden oman organisaation turvallisuustoimintaan liittyen tarvitsee tuntea kansallisen turvallisuusauditointikriteeristön vaatimukset.(Kansallinen turvallisuusauditointikriteeristö 2011.)

Hallinnollisen turvallisuuden osio piti sisällään laajan kontrollointi työkalun tiedon turvallisen hallinnan, sekä turvallisuusjohtamisen osalta ja auditointikysymykset, sekä niihin liittyvät vaatimukset. Osiossa tarkasteltiin periaatteet ja määrittelyt jotka ohjaavat turvallisuuspolitiikkaa sekä turvallisuustoimintaa, turvallisuuden vuotuista toimintaohjelmaa, turvallisuuden tavoitteiden määrittelyä, riskien tunnistamista, arviointia näiden lisäksi kontrollointia, turvallisuusorganisaatiolle, vastuille, onnettomuuksille, vaaratilanteille, turvallisuuspoikkeamille sekä ennalta ehkäiseville toimenpiteille, turvallisuusdokumentaatiolle sekä sen hallinnalle, turvallisuuskoulutukselle, turvallisuus tietoisuuden lisäämiselle sekä turvallisuusosaamiselle ja viimeisenä raportoinnille sekä johdon katselmuksille.” (Kansallinen turvallisuusauditointikriteeristö 2011.)

Katakrin toisessa versiossa tarkoitettiin henkilöstöturvallisuudella pääasiassa työyhteisölle, henkilön muodostamaa uhkaa tietoturvallisuudelle. Katakrin malli oli pitkälti yhtenevä VAHTI johtoryhmän julkaisemassa henkilöriskejä käsittelevään ohjeistukseen (VAHTI 2/2008). Henkilöstöturvallisuuden auditointikysymykset, sekä vaatimukset sisälsivät alakokonaisuuden. Alakokonaisuus koostui teknisestä kriteeristöstä eli henkilöstön hallinnoinnista, riittävästä osaamisesta varmistumisesta eli annettujen ja saatujen tietojen tarkastaminen, henkilön muusta

soveltuvuudesta tehtävään eli arvot ja luotettavuus, rekrytointipäätöksen jälkeiset toimet eli esimerkiksi salassapitosopimukset, toimenpiteet työsuhteen solmimisen yhteydessä eli tehtävät, vastuut, perehdytys, toimenpiteet työsuhteen aikana eli huolehtiminen, seuranta, sijaisuudet, puuttuminen.(Kansallinen turvallisuusauditointikriteeristö 2011.)

Fyysisen turvallisuuden käsite Katakrissa toisessa versiossa käsitti toimitilaturvallisuuden sekä sitä tukevat erilaiset järjestelyt. Fyysisen turvallisuuden osio oli Katakrin toisessa versiossa jaettu kolmeen osa-alueeseen ja niihin liittyviin auditointikysymyksiin, sekä vaatimuksiin. Ensimmäisenä oli alueen turvallisuus, toisena rakenteellinen turvallisuus ja viimeisenä turvallisuustekniset järjestelmät. (Kansallinen turvallisuusauditointikriteeristö 2011.)

Katakrin toisessa versiossa tietoturvallisuusosio oli jaettu neljään osaan ja niihin liittyviin auditointikysymyksiin sekä vaatimuksiin. Osat koostuivat tietoliikenneturvallisuudesta tietojärjestelmäturvallisuudesta, tietoaineistoturvallisuudesta, sekä käyttöturvallisuudesta. (Kansallinen turvallisuusauditointikriteeristö 2011.)

2.3 VAHTI ja Katakri II

Valtiovarainministeriö ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Sen asettama Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin. VAHTI käsittelee kaikki merkittävät valtionhallinnon tietoturvallisuuden linjaukset sekä tietoturvatoimenpiteiden ohjausasiat, sekä se tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa. VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista, sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. VAHTI edistää hallitusohjelman, valtionhallinnon tietoturvallisuusasetuksen (681/2010), Yhteiskunnan turvallisuusstrategian, valtion IT-strategian, valtioneuvoston huoltovarmuuspäätöksen, kansallisen tietoturvastrategian, valtioneuvoston periaatepäätöksen valtion tietoturvallisuuden kehittämisestä ja hallituksen muiden keskeisten linjausten toimeenpanoa kehittämällä valtion tietoturvallisuutta ja siihen liittyvää yhteistyötä. VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä. VAHTIn toiminnalla parannetaan valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös organisaatioissa, sekä kansainvälisesti. VAHTIn työn tuloksena on aikaansaatu yksi maailman kattavim-

mista yleisistä tietoturvaohjeistoista. Valtiovarainministeriön ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvallisuutta käsitteleviä yhteishankkeita sekä laaja valtion tietoturvallisuuden kehitysohjelma. (VAHTI julkaisu 2/2011.)

VAHTI käsittelee julkisen hallinnon tieto- ja kyberturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut niitä koskevat linjaukset. VAHTI ohjaa valtionhallinnon tietoturvatoimenpiteitä ja sen yhtenä tavoitteena on tieto- ja kyberturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa sekä varautumista, toisena tavoitteena on tieto- ja kyberturvallisuuden sekä ICT-varautumisen edistäminen jotta ne saataisiin kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta sekä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa ja käyttöä. VAHTI valmistelee sekä yhteen sovittaa valtioneuvoston ja valtiovarainministeriön linjauksia julkisen hallinnon tieto- ja kyberturvallisuudesta ja ICT-varautumisesta sekä seuraa ja edistää niiden toimeenpanoa. Se kehittää, yhteensovittaa ja ylläpitää julkisen hallinnon tieto- ja kyberturvallisuuden tavoitteita, toiminta-, organisointi-, arkkitehtuuri- ja resurssilinjauksia sekä normeja, ohjeita ja suosituksia. VAHTI myös edistää julkisen hallinnon tietoturvakulttuuria ja henkilöstön tietoturvatietoisuutta. Se käsittelee ja yhteensovittaa julkisen hallinnon kansainvälisen tietoturvayhteistyön linjauksia sekä vaikuttamista kansainvälisessä tietoturvatyössä se ohjaa ja käsittelee julkisen hallinnon ICT-strategiaa sekä sen valmistelua ja toimeenpanoa. VAHTI ohjaa, valmistelee ja yhteensovittaa tieto- ja kyberturvallisuuden ja ICT-varautumisen osalta julkisen hallinnon tieto- ja kyberturvallisuuteen liittyviä kehittämisohjelmia sekä niiden toimeenpanoa. (VAHTI toimintasuunnitelma 2014.)

3 Katakri 2015 – Tietoturvallisuuden auditointityökalu viranomaiselle

Tässä luvussa käsittelen sitä, miten Katakri 2015 – tietoturvallisuuden auditointityökalu viranomaisille on muuttunut Katakrin toisesta versiosta. Janhunen (2014) toi esiin, että Katakrin nimen muuttamista oli mietitty, mutta Katakri nimen tunnettuus oli tässä tapauksessa tärkeämpi tekijä. Katakri 2015 – auditointityökalun esipuhe tukee myös tätä käsitystä. Katakrin rakenne ja käyttötapa ovat muuttuneet uudistuksen yhteydessä, jonka vuoksi ei voida enää puhua Katakrin päivitysversiosta, vaan pikemminkin kokonaisuudistuksesta. Katakri - nimi on kuitenkin haluttu säilyttää, koska se on käytössä vakiintunut ja tunnettu. Katakrin nimi kokonaisuudessaan on Katakri - tietoturvallisuuden auditointityökalu viranomaisille. (Turvallisuus & Riskienhallinta 2/2015.)

2 Opinnäytetyön tarkoitus ja tavoite

Keskityn opinnäytetyössäni siihen, miten Katakri 2015 on muuttunut edeltävistä versioistaan. Fokukseni ovat Katakri 2015 – auditointityökalun olennaisimmat muutokset. Opinnäytetyössäni tuon esiin, mihin tarkoitukseen Katakri 2015 on tehty, mikä on sen nykyinen käyttötarkoitus ja miten sitä on tarkoitettu käytettävän. Lisäksi työssä tuodaan esiin kirjallisuuskatsauksessa ja asiantuntijalausuntojen sekä kyselyiden avulla, miten Katakri 2015 - auditointityökalun edeltävien versioiden vahvuudet ja kehityskohteet on huomioitu uudessa Katakrissa. Vain erityisestä tarpeesta tuon Katakri 2015 - auditointityökalusta esiin yksittäisiä vaatimuksia.

Opinnäytetyö toimii hyvänä pohjana lähtiessä tavoittelemaan Katakrin 2015 – auditointityökaluun vaatimuslähteistä koottuja vaatimuksia. Katakri 2015 – työkalussa vaatimuslähteistä esiintuodut vaatimukset täytettyä organisaatio kykenee osallistumaan kansallisiin, sekä kansainvälisiin hankkeisiin joihin vaatimuksena on kyky suojata viranomaisen salassapidettävää tietoa oikeudettomalta paljastumiselta sekä käyttämiseltä. Samoin se mahdollistaa osallistumaan puolustusvoimien hankkeisiin ja tarjouskilpailuihin, joissa käsitellään viranomaisen salassa pidettävää tietoa.

Tärkeimmät lähteeni opinnäytetyössäni ovat Katakrin kaikki versiot, Katakri 2015 - ohjausryhmältä saatavat materiaalit, sekä mahdolliset keskustelut, sekä kyselyt, haastattelut ja lausunnot ohjausryhmän jäseniltä ja mahdollisten muiden asiantuntijoiden kanssa.

Tutkimuskysymykseni ovat seuraavat:

Miten Katakri on muuttunut?
Miksi Katakri uudistettiin?

Mikä on turvallisuusjohtamisen merkitys Katakri 2015 – Tietoturvallisuuden auditointityökalussa viranomaiselle?

Toiminnallisen opinnäytetyön tuotoksena muodostan kuvan uudistetusta Katakri 2015 –auditointityökalusta. Aihe on hyvin merkityksellinen, koska Katakrin 2015 – auditointityökaluun vaatimuslähteistä kootut vaatimukset täyttämällä saadaan selkeää kilpailu etua niin kotimaisilla markkinoilla kuin kansainvälisilläkin areenoilla, sekä voidaan osallistua paitsi kotimaisiin niin myös kansainvälisiin hankkeisiin, joissa vaatimuksena on viranomaisen salassa pidettävän tiedon suojaamisen oikeudettomalta paljastumiselta todennettu hallinta. Tavoitteena on tuottaa ymmärrystä, miksi uusi Katakri 2015 on koettu tarpeelliseksi muodostaa. Opinnäytetyöllä on suora linkki elinkeinoelämään, koska se tuo esiin, mitä kaikkea Katakri 2015 – auditointityökalu sisältää ja mitä se vaatii kokonaisuutena ja siten antaa kuvan, kuinka vaativa projekti on saavuttaa Katakrin 2015 – auditointityökaluun vaatimuslähteistä kootut vaatimukset turvallisuuden eri osa-alueilla ja siten osoittaa, että organisaatio kykenee suojaamaan viranomaisen luottamuksellista tietoa paljastumiselta ja luvattomalta käytöltä.

3.1 Opinnäytetyön tutkimusmenetelmät ja aineisto

Opinnäytetyöni on toiminnallinen opinnäytetyö. Valitsin työhöni toiminnallisen lähestymistavan, koska tavoitteenani on tuottaa kuva Katakrista, etenkin Katakri 2015 –tietoturvallisuuden auditointityökaluun tehtyihin olennaisiin muutoksiin. Vilkka ja Airaksinen (2003, 9) kertovat toiminnallisen opinnäytetyön tavoitteena olevan antaa käytännön ohjeistusta, opastusta, toiminnan järjestämistä tai järkeistämistä. Toiminnallinen opinnäytetyö jakaantuu kahteen osuuteen; toiminnallisen osan tuotokseen esimerkiksi oppaaseen sekä raporttiin (Haaga-Helia ammattikorkeakoulu 2014, 13, 20). Toiminnallinen opinnäytetyöni sisältää teoreettisen viitekehyksen, integroivan kirjallisuuskatsauksen tutkimusosan, sekä toiminnallisen tuotoksen joka sisältää yleiskuvauksen Katakrin osa-alueista ja niiden sisällöstä, sekä Katakrin eri versioita vertailevan taulukon muodossa.

Käytin opinnäytetyössäni tiedonkeräysmenetelminä kuvailevaa kirjallisuuskatsausta, surveytutkimusta, sekä haastatteluja. Hirsijärvi, Remes ja Sajavaara (2013, 259) kertovat kirjallisuuskatsauksen olevan hyvä oppimismahdollisuus opinnäytetyön aiheesta. Kuvailevan kirjallisuuskatsauksen määrittelee Salminen (2011, 6) olevan yleiskatsaus ilman tiukkoja ja tarkkoja sääntöjä, siinä käytetyt aineistot voivat olla laajoja, eikä aineiston valintaa rajaa metodiset säännöt. Birmingham (2000) toteaa, että kuvailevasta kirjallisuuskatsauksesta erottuu kaksi hieman erilaista orientaatiota, joita ovat narratiivinen ja integroiva katsaus. Integroivan kirjallisuus katsauksen ero narratiiviseen kirjallisuuskatsaukseen on, että kriittisen tarkastelun voidaan oleellisesti katsoa kuuluvan siihen. Siinä on kyse myös metodisesta vaatimuksesta,

sillä kriittisen arvioinnin avulla tärkein tutkimusmateriaali on mahdollista tiivistää kirjallisuuskatsauksen perustaksi, integroidulla kirjallisuuskatsauksella on mahdollista kerätä merkittävästi suurempi otos tutkimuksen kohteena olevasta aiheesta, se sallii erilaisin metodisin lähtökohdin tehdyt tutkimukset käytettäväksi analyysin pohjaksi. Tutkittava aihe kyetään kuitenkin esittelemään laaja-alaisesti ja tutkittavan aiheen ominaisuudet pystytään tarpeen mukaan luokittelemaan. Metodisen vaatimuksen mukaan kriittisellä arvioinnilla tutkimusmateriaali kyetään tiivistämään kirjallisuuskatsauksen pohjaksi. (Salminen 2011, 8.)

Survey-tutkimus tarkoitetaan sellaisia kyselyn, haastattelun ja havainnoinnin muotoja, missä tietoa kerätään standardoidusti, sekä kohdehenkilöt muodostavat otoksen tai näytteen tietystä perusjoukosta. Standardoituudella tarkoitetaan tässä sitä, että kysymys on esitettävä, täsmälleen samalla tavalla, kaikille vastaajille. (Hirsjärvi ym. 2009, 193 – 194.) Tässä opinnäytetyössä esikartoituksena tehdyssä toimivassa kyselytutkimuksessa tutkitaan lukumääräisesti kohtuullisen kokoista, mutta rajoitettua joukkoa, joilla on joko vahva kokemus turvallisuusalasta tai joka on käyttänyt vähintään yhtä Katakrin versioista työssään.

Lomakkeen laatiminen sekä itse kysymysten asettelu ovat tärkeitä tekijöitä kysely tutkimuksen onnistumiselle. Heikohkot, umpimähkään laaditut lomakkeet ovat johtaneet negatiiviseen asennoitumiseen kyselyn käyttöä kohtaan osana tutkimusta. Niiden yleisyys on osaltaan vähentänyt ihmisten intoa kysely tutkimuksia kohtaan. (Hirsjärvi ym. 2009, 198.) Kyselylomaketta laadittaessa tulee huomioida tutkittavan motivaation kehitys kyselyä kohtaan, motivaatio jaetaan kolmeen vaiheeseen, nousuvaiheeseen, huipputasovaiheeseen, sekä laskuvaiheeseen. Kyselylomakkeessa taustakysymykset asetellaan usein kyselyn alkuun, jolloin ne toimivat lämmittelykysymyksinä niiden jälkeen kysytään pääsääntöisesti yleisluonteisia kysymyksiä. Näiden ensimmäisen vaiheen kysymyksillä tähdätään vastaajan luottamuksen voittamiseen kyselytutkimusta kohtaan ja tuoda esiin kyselyn merkityksen tärkeys sekä mielekkyys. Kyselyn huipputasonvaiheessa kysytään eniten ajatusta ja keskittymistä vaativat kysymykset ja loppuvaiheeseen jätetään jäähdyttelykysymykset. Kyselytutkimuksen ollessa pitkä taustakysymykset on mahdollista jättää kyselyn loppuun. Pitkän kyselyn edetessä motivaatio kärsii, sekä keskittyminen herpaantuu, taustakysymykset eivät vaadi näistä vastaajalta kumpaakaan. (Valli 2007, 103 – 104.)

Kyselylomakkeen pituus tulee olla oikeassa suhteessa tutkimuksen laajuuteen. Kun lomake on pitkä ja kysymyksiä on paljon, kynnys osallistua kyselyyn kasvaa. Kohderyhmä tulee huomioida kyselyä laadittaessa, toisin sanoen millaiset henkilökohtaiset kyvyt vastaajilla on sekä miten läheisenä ja henkilökohtaisena he kokevat kyselyn. Liian pitkässä kyselyssä motivaation hiipuminen loppua kohti heikentää tutkimuksen luotettavuutta. Liian tiiviisti ahdettu lomake aiheuttaa herkästi vastaajalle tunteen runsaasti aikaa vievästä ja vaivalloisesta työstä. (Valli 2007, 103 – 104.) Kyselyssä voidaan käyttää avoimia monivalintakysymyksiä tai asteikoihin,

toisin sanoen skaaloihin perustuvaa kysymystyyppiä. Avoimissa kysymyksissä esitetään kysymys ja jätetään tyhjä tila vastaukselle. Monivalintakysymyksissä tutkija laatii valmiit vastausvaihtoehdot, joista vastaaja valitsee vastauksensa ja merkitsee sen tai ne. Skaaloihin perustuvissa kysymyksissä esitetään väittämiä joihin vastaaja vastaa sen mukaan, miten voimakkaasti hän on samaa tai eri mieltä. Kyselytutkimuksessa käytetyssä avointen kysymysten mallissa annetaan vastaajalle mahdollisuus kertoa, mitä hänellä on aiheesta todella mielessään. Monivalintakysymykset pakottavat vastaajan valitsemaan valmiista vaihtoehdoista. (Hirsjärvi ym. 2009, 198 – 201.)

Haastattelu tiedonkeruumenetelmänä on joustava ja siinä ollaan vuorovaikutuksessa tutkittavan kanssa. Siinä on merkittävänä etuna, että aineiston keräämistä voidaan säädellä tilanteen edellyttämällä tavalla ja vastaajia myötäillen. Haastattelu on usein hyvä valinta, kun tutkittava kohde on vähän kartoitettu, jopa tuntematon alue tai se voi tuottaa moniin suuntiin meneviä vastauksia. Haastattelun avullaa on halutessa mahdollisuus selventää saatavia vastauksia sekä pyytää perusteluja haastattelun aikana esiintuoduille tiedoille. Haastattelun avulla päästään pintaa syvemmältä tutustumaan tutkittavaan kohteeseen. Normaalissa keskustelussa molemmat osapuolet ovat tasa-arvoisia kysymyksien tekemisessä sekä vastauksien antamisessa, mutta haastatteluissa haastattelijalla on ohjat käsissä. Tutkimustarkoituksessa tehdyt haastattelut ovat systemaattisia tiedonkeruun muotoja, jolla on tavoitteet ja niillä pyritään saamaan luotettavia ja päteviä tietoja tutkittavasta kohteesta. (Hirsijärvi ym. 2009, 204 – 209.)

Avoin haastattelu on kaikista haastattelun muodoista keskustelua lähimpänä. Se vie usein paljon aikaa, tunnista kahteen tuntiin, ja se voi edellyttää useampia haastattelukertoja. Avoimessa haastattelussa haastattelija tekee kysymyksiä aiheista, sitä mukaa kun ne tulevat esiin keskustelun kuluessa. Avoimessa haastattelussa ei ole selkeää rakennetta, jolloin haastattelutilanteen ohjailu jää haastattelijan tehtäväksi. Useimmiten käytetty avoimen haastattelun muoto on yksilöhaastattelu. Haastattelun käytännölliseen toteuttamiseen liittyy useita seikkoja, joista esimerkkeinä haastattelusta sopiminen, keskustelun avaukset, kysyminen ja dialogin ohjailu. Nykyään erilaisia haastatteluja on myös joustava tehdä käyttäen hyväksi tietoteknisiä apuvälineitä. (Hirsijärvi ym. 2009, 209 – 212.)

3.2 Opinnäytetyön aineiston analysointi

Opinnäytetyössäni käytin tiedon analysointitapana ymmärtämiseen pyrkivään lähestymistapaa käyttäen teemoittelua analyysimenetelmänä.

Tutkimuksen ydin on kerätyn aineiston analyysi, tulkinta ja johtopäätösten tekeminen. Analyysivaiheessa tutkijalle selviää, minkälaisia vastauksia ongelmiin hän on saanut. Päätelmiä

päästään tekemään vasta esitöiden jälkeen. Ensimmäisenä osana on aineiston järjestäminen, tietojen tarkistus, onko aineistossa virheellisyyksiä tai puuttuuko tietoja, täytyy tehdä päätöksiä sekä mitä tietoja ja millä perusteella niitä hylätään tai käytetään. Toisena osana tietojen järjestämisessä on tietojen täydentäminen. Sitä voidaan tehdä täydentävin haastatteluin ja kyselyin pohjautuen aiempaan tai uuteen tietoon. Viimeisenä osana tietojen järjestämisessä on aineistojen järjestäminen tiedon tallentamista sekä analyysejä varten. Aineiston järjestämisen toimenpiteet riippuvat tutkimusstrategiasta, esimerkiksi kvalitatiivisessa tutkimuksessa aineiston järjestelemisessä on suuri työ ja kvantitatiivisessa tutkimuksessa tutkimuksen aineistosta muodostetaan muuttujia. Lopuksi aineisto litteroidaan tarpeen mukaisesti, kuitenkin merkittävä tekijä on sitä tehtäessä, että käytetäänkö jotakin tietokoneelle suunniteltua analyysiohjelmaa. (Hirsijärvi ym. 2009, 221 – 222.)

Aineiston käsittely ja analysointi tulee aloittaa mahdollisimman pian keruuvaiheen tai kenttävaiheen jälkeen. Kvalitatiivisessa tutkimuksessa, jossa aineistoa kerätään useissa vaiheissa, sekä mahdollisesti rinnakkaisin menetelmin, ei analyysiä tehdä vain yhdessä tutkimusprosessin vaiheessa, vaan pitkin matkaa. (Hirsijärvi ym. 2009, 223.)

Analyysitavat jaetaan pääsääntöisesti kahteen tapaan. Ensimmäisenä on selittämiseen pyrkivä lähestymistapa, jota käytetään usein tilastollisten analyysien ja päätelmien yhteydessä. Toisessa, ymmärtämiseen pyrkivässä lähestymistavassa käytetään laadullisen analyysin keinoja. Tutkimusta varten valitaan sellainen analyysitapa joka parhaiten tuo vastauksen tutkimustehtävään tai tutkittavaan ongelmaan. Etenkin laadullisessa tutkimuksessa analyysi koetaan vaikeaksi toteuttaa. Aineistoon tutustuessaan tutkija tekee jo alustavia valintoja. Laadullista aineistoa on mahdollista käsitellä myös tilastollisin keinoin, mutta yleensä analyysimenetelminä käytetään teemoittelua, tyypittelyä, sisällönerittelyä, diskurssianalyysiä, sekä keskusteluanalyysiä. Laadullisessa tutkimuksessa aineiston runsaus tekee analyysivaiheen haastavaksi ja mielenkiintoiseksi. Yleensä tutkija ei pysty hyödyntämään kaikkea keräämäänsä aineistoa, eikä kaikkea olekaan tarpeen analysoida aina. (Hirsijärvi ym. 2009, 223 – 225.)

Keskeisiä aiheita, teemoja muodostetaan useimmiten aineistolähtöisesti etsimällä tekstimassasta sen eri haastatteluja, vastauksia tai kirjoitelmia yhdistäviä tai mahdollisesti erottavia seikkoja. Teemoittelu on luonteva etenemistapa muun muassa teemahaastatteluaineiston analysoimisessa. Teemat, joista haastateltavien kanssa on puhuttu, löytyvät yleensä kaikista haastatteluista, joskin vaihtelevassa määrin ja eri tavoilla. Aineisto voidaankin litteroinnin jälkeen järjestellä teemoittain, ihmisten puheesta litteroitua tekstiä tuleekin tarkastella ennakkoluulottomasti. Teemoittelua käytettäessä analyysimetodina voidaan teemojen muodostamisessa käyttää apuna koodausta, vaikkapa taulukointien avulla voidaan havainnoida sitä, mitkä seikat aineistossa ovat keskeisiä ja sen pohjalta voidaan miettiä yhdistäviä nimittäjiä, toisin sanoen teemoja. Aineistoa järjestellessä teemoittain kootaan esimerkiksi kunkin valitun

teeman alle haastattelusta ne kohdat, joissa puhutaan juuri siitä teemasta. Yleisin tapa on suorittaa teemoittelua tekstinkäsittelyn avulla leikaten ja liimaten tekstiä, tekstinkäsittelyn avulla on myös helpompi koota eri teemojen alle sellaisia tietoja jotka liittyvät useisiin teemoihin. Tutkimusraportissa esitetään yleensä teemojen käsittelyn yhteydessä näytepaloja, sitaatteja. Aineistosta lainattujen kohtien tarkoituksena on antaa havainnollistavia esimerkkejä ja tarjota lukijalle todiste siitä, että tutkijalla on ollut aineisto, johon hän analyysinsa pohjaa. Lisäksi lainatuilla kohdilla osoitetaan, että aineisto on antanut johtolankoja juuri näiden teemojen muodostamiseen. Huomioitavaa on, että tutkimusraportti ei ole vain kokoelma erilaisia, peräkkäisiä sitaatteja ilman tutkijan kommentointia, tulkintoja tai kytkentöjä teoriaan. Sitaattien tulee siksi olla hyvin harkittuja, lainauksia käytettäessä tulisi myös pohtia sitä, esitetäänkö niiden yhteydessä vastaajien taustatietoja. Teemojen nimeämisessä voi pysytellä hyvin kuvaavassa tyylissä tai vaihtoehtoisesti voi valita mielikuvituksellisempia otsakkeita, kunhan tyyli raportissa on yhtenevä. (Saaranen-Kauppinen. 2006.)

3.3 Katakri 2015

Katakrista on pyritty tekemään paremmin aikaa kestävä, jotta vältetään usein toistuvat kokonaisuudistukset. Katakri on viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Katakrin uudistamistyö lähti käyntiin kansallisen turvallisuusviranomaisen johtamassa ohjausryhmässä helmikuussa 2014. Osa-alueita valmisteltiin erikseen alatyöryhmissä, joissa oli mukana kunkin osa-alueen asiantuntijoita. Osa-alueiden yhteensovittaminen sekä lausuntojen pohjalta tehty viimeistely olivat hankkeen työläimpiä vaiheita. Viimeistelytyö tehtiin pienryhmässä, jossa mukana oli kunkin sektorin asiantuntemusta. Lausuntokierroksen pohjalta saatiin noin kaksikymmentä lausuntoa, jotka tarkasteltiin huolellisesti ja lopullista versiota hiottiin useamman päivän ajan. Katakriin kohdistuu runsaasti erilaisia odotuksia, joista osa on jopa keskenään vastakkaisia, joten lopullisessa versiossa päädyttiin kompromissiin. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015; Turvallisuus & Riskienhallinta 2/2015.) Katakri 2015 – auditointityökalu keskittyy pääosin security-näkökulmaan.

Ajantasainen Katakri on saatavilla sähköisenä, esimerkiksi kansallisen turvallisuusviranomaisen kotisivuilla osoitteessa www.formin.finland.fi. Palautetta erityisesti käyttökokemuksista sekä kehitysideoita otetaan kuitenkin mielellään vastaan ja niitä voi lähettää osoitteella NSA@formin.fi.

3.4 Organisaatio Katakri 2015 takana

Elokuussa 2012 sisäministeriö asetti neuvoa antavan työryhmän, jonka tehtävänä oli vuoden 2013 loppuun mennessä paitsi Katakrin päivittäminen, niin myös Katakria koskevien vastuiden

selvittäminen valtionhallinnossa. Työryhmä ei saanut tehtyä Katakrin päivittämistä valmiiksi sisäministeriössä asetetun määräajan puitteissa. Työryhmän esityksestä keskeiset ministeriöt, valtiovarainministeriö, ulkoministeriö, liikenne- ja viestintäministeriö, sisäministeriö ja valtioneuvoston kanslia, päättivät tammikuussa 2014, että päävastuu Katakrin hallinnoinnista sekä ylläpidosta siirtyy ulkoministeriössä toimivalle Kansalliselle turvallisuusviranomaiselle. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

Katakrin uudistamistyö ja hallinnointi ovat kansallisen turvallisuusviranomaisen yhteistyöryhmän alatyöryhmäksi perustetun ohjausryhmän vastuulla, tämän lisäksi Katakrin eri osa-alueita on valmisteltu erillisissä omissa alatyöryhmissä. Ohjausryhmissä ovat olleet edustettuina toimivaltaisten viranomaistahojen lisäksi myös elinkeinoelämän edustajat. Katakrin uudistamistyötä on koordinoinut ohjausryhmä, johon kuuluivat asiantuntijoita eri ministeriöistä ja pääesikunnasta sekä elinkeinoelämästä. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

3.5 Mitä on muuttunut Katakri 2015 - auditointityökalussa?

Lähtökohtana Katakrin uudistamisessa on ollut käytettävyyden lisääminen, skaalautuvuus, riskiperusteisuus, vaatimusten läpinäkyvyyden parantaminen sekä osittaisten auditointien mahdollistaminen. Koska uudistukset ovat mittavia ja ne ovat johtaneet Katakrin rakenteen muuttumiseen, ei enää voida puhua Katakrin päivitysversiosta. Katakri-nimi on kuitenkin käytössä jo niin vakiintunut ja tunnettu, että se on päätetty säilyttää jatkossakin tämän viranomaisten auditointityökalun nimenä. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.) Katakri 2015 on kokenut hyvin suuren muutoksen ja tavallaan palautettu alkupisteeseen. Se on nyt suunnattu selkeästi viranomaisen auditointityökaluksi.

Katakri-auditointityökalu on hyväksytty käyttöön kansallisen turvallisuusviranomaisen yhteistyöryhmässä 26.03.2015. Katakri 2015 –auditointityökalu on lähdetty rakentamaan täysin uudella tavalla. Pääsääntöisesti kaikki vaatimukset on perusteltu suorilla viittauksilla valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010), jäljempänä tietoturvallisuusasetus, jota noudatetaan Suomessa niin kansallisen kuin kansainvälisenkin salassa pidettävän tiedon suojaamisessa. Kansainvälisenä lähteenä on käytetty EU:n neuvoston turvallisuussääntöjä (2013/488/EU), jotka sisältävät EU:n turvallisuusluokitellun tiedon suojaamista koskevat vähimmäisvaatimukset ja perusperiaatteet. Katakrissa esitettyjen vaatimusten yhteyteen on merkitty lähdeviittaus läpinäkyvyyden varmistamiseksi. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

Katakri 2015 - auditointityökalu ei itse aseta ehdottomia vaatimuksia, vaan siihen on koottu minimivaatimukset, jotka perustuvat voimassa olevaan kansalliseen lainsäädäntöön, kansallisiin säädöksiin, Suomea sitoviin kansainvälisiin velvoitteisiin ja kansainvälisiin tietoturvallisuusvelvoitteisiin. Keskeisin kansalliseen lainsäädäntöön perustuva vaatimuslähde on tietoturvallisuusasetus (681/2010), jota noudatetaan Suomessa niin kansallisen kuin kansainvälisenkin salassa pidettävän tiedon suojaamisessa. Kansainvälisenä lähteenä on käytetty EU:n neuvoston turvallisuussääntöjä (2013/488/EU), jotka sisältävät EU:n turvallisuusluokitellun tiedon suojaamista koskevat vähimmäisvaatimukset ja perusperiaatteet. Katakrissa esitettyjen vaatimusten yhteyteen on merkitty lähdeviittaus läpinäkyvyyden varmistamiseksi. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

3.6 Katakri 2015 - auditointityökalun osa-alueet

Katakrin jaottelu on myös kokenut muutoksen. Katakri jakautuu kolmeen osa-alueeseen. Turvallisuusjohtamisen osa-alue (T) kattaa sekä hallinnollisen että henkilöstöturvallisuuden. Siinä on kuvattu perustaso, jonka vaatimukset organisaation tulee täyttää. Osa-alueen vaatimuksilla pyritään varmistumaan siitä, että organisaatiolla on riittävä kyvykkyys käsitellä viranomaisen salassa pidettävää tietoa turvallisesti. Fyysisen turvallisuuden osa-alue (F) perustuu salassa pidettävän tiedon käsittelytarpeen mukaisesti tehtyyn aluejakoon (hallinnollinen alue, turva-alue ja tekninen turva-alue). Jako mahdollistaa aikaisempaa joustavammin salassa pidettävien tietojen käsittelyn alueiden välillä. Teknisen tietoturvallisuuden osa-alueessa (I) puolestaan kuvataan käsittelyvaatimukset tietoaineiston suojaustaso-luokituksen mukaisesti tasoille ST IV, STIII ja STII. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015; Turvallisuus & Riskienhallinta 2/2015.)

Katakri 2015 - auditointityökalulle merkityksellisiä turvallisuuden osa-alueita ovat turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus. Turvallisuusjohtaminen sisältää hallinnollisen turvallisuuden sekä henkilöstöturvallisuuden. Fyysinen turvallisuus sisältää tiloja ja laitteita koskevia vaatimuksia, luvattoman pääsyn estämisen, suojaamisen salakatselulta ja salakuuntelulta sekä toiminnan jatkuvuuden hallinnan. Tekninen tietoturvallisuus sisältää tietoliikenneturvallisuuden, tietojärjestelmäturvallisuuden, tietoaineistoturvallisuuden sekä käyttöturvallisuuden. Näiden kaikkien yläpuolella on kuitenkin riskienhallinta, johon Katakri 2015 - auditointityökalun käyttäminen sen nykyisessä muodossa perustuu. (KATAKRI – Tietoturvallisuuden auditointityökalu viranomaiselle.)

Katakri 2015 - auditointityökaluun kirjatut vaatimukset on jaettu kolmeen osa-alueeseen. Turvallisuusjohtamista koskevassa (T) osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on riittävät turvallisuusjohtamisen valmiudet sekä kyvykkyys. Turvallisuusjohtamisen

osa-alueessa on kuvattu perustaso, jonka vaatimukset kohdeorganisaation tulee täyttää. Fyysistä turvallisuutta koskevassa (F) osa-alueessa kuvataan salassa pidettävien tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset. Organisaation tilat voidaan jakaa kolmeen alueeseen salassa pidettävien tietojen käsittely- ja säilyttämistarpeen perusteella: hallinnollinen alue, turva-alue ja tekninen turva-alue. Teknistä tietoturvallisuutta koskevassa (I) osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittely ympäristölle asetetut turvallisuusvaatimukset. Tämä osa-alue jakautuu kolmeen käsiteltävän tiedon mukaiseen suojaustasoon (ST IV, ST III, ST II). (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

Turvallisuusjohtamisen osa-alueessa käsitellään niitä menetelmiä, joilla turvallisuus ja sen hallinta jalkautetaan osaksi koko organisaation toimintaa. Turvallisuusjohtamisen osa-alue kattaa hallinnollisen turvallisuuden ja henkilöstöturvallisuuden. Turvallisuusjohtamisen vaatimuksilla pyritään siihen, että organisaatiolla on toimiva turvallisuuden hallintajärjestelmä sekä riittävät menettelyt sen varmistamiseksi, että viranomaisen salassa pidettäviä tietoja käsittelevä henkilöstö toimii asianmukaisesti. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.).

Katakri 2015 - auditointityökalussa tarkastellaan fyysistä turvallisuutta viranomaisen salassa pidettävän tietoaineiston suojaamisen näkökulmasta. Lähtökohtana on varmistaa, että salassa pidettävät tiedot ovat suojassa oikeudettomalta paljastumiselta. Fyysisten turvatoimien tarkoituksena on estää tunkeutuminen salaa tai väkisin, ehkäistä, estää ja havaita luvattomat toimet sekä mahdollistaa henkilöstön luokitus ja pääsy salassa pidettäviin tietoihin sen perusteella, mikä heidän tiedonsaantitarpeensa on. Tällaiset turvatoimet on määriteltävä riskienhallintaprosessin perusteella. Osa-alueessa F tilat ja tilaryhmät jaetaan alueisiin: hallinnollinen alue, turva-alue ja tekninen turva-alue. Tarve kunkin alueen perustamiseksi riippuu siitä, minkä tasoista salassa pidettävää tietoa alueella säilytetään tai käsitellään. Aluejako perustuu EU:n neuvoston turvallisuussääntöihin, mutta vastaavanlainen turvallisuusvyöhykkeisiin perustuva jako on käytössä myös kansallisesti. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

Katakri 2015 - auditointityökalun teknisen tietoturvallisuuden osa-alueessa kuvataan vaatimukset, joita soveltamalla pyritään varmistamaan turvallisuusjärjestelyiden riittävyys viranomaisen salassa pidettävän tiedon sähköisissä käyttöympäristöissä. Osa-alueessa täydennetään myös Katakrin muiden osa-alueiden kuvauksia paperimuotoisen aineiston suojausvaatimuksista. Vaatimukset on jaettu tietoliikenne-, tietojärjestelmä-, tietoaineisto- ja käyttöturvallisuuden osioihin. Osa-alue koostuu vaatimuksista, niiden tulkinnan tueksi laadituista toteutusesimerkeistä sekä muista taustoittavista lisätiedoista. Tiettyihin asiakokonaisuuksiin joista esimerkkinä hallintayhteydet, langattomat verkot, etäkäyttö ja varmuuskopiointi on

ryhmitelty niihin liittyvät vaatimukset. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

3.7 Katakri 2015 - auditointityökalun käyttäminen

Katakri 2015 - auditointityökalua toteutetaan turvallisuusjohtamisen kautta, koska se tarjoaa kaikki ne välineet, joilla voidaan paitsi johtaa ja hallita turvallisuutta erilaisten työkalujen avulla, niin myös määritellään, dokumentoidaan, sekä todennetaan että vaatimukset täyttyvät eri vaatimusten yhteydessä. Turvallisuusjohtamisen osa-alue on uusi osa-aluekokonaisuus Katakri 2015 - auditointityökalussa ja siksi käsittelen hieman laajemmin turvallisuusjohtamista toiminnallisen opinnäytetyöni teoriaosuudessa.

Katakri 2015 - auditointityökalua voidaan käyttää auditointityökaluna arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Sitä voidaan käyttää myös apuna yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä. Katakri 2015 -auditointityökalun käyttämisellä pyritään varmistamaan, että kohdeorganisaatiolla on riittävät turvallisuusjärjestelyt viranomaisen salassa pidettävien tietojen oikeudettoman paljastumisen ehkäisemiseksi kaikissa niissä ympäristöissä, joissa tietoja käsitellään. Tavoitteena on lisäksi varmistaa turvallisuusvaatimusten huomioon ottaminen turvallisuuden hallinnassa. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

Turvallisuusjärjestelyjen suunnittelun ja toteutuksen avulla pyritään varmistamaan uhkiin nähden hyväksyttävä turvallisuustaso. Kohdeorganisaation tulee kyetä osoittamaan turvallisuusjärjestelyjen riittävyys, luotettavasti. Turvallisuusjärjestelyjen riittävyyden arvioinnin tulee pohjautua järjestelmälliseen riskienarviointiin. Turvallisuusriskien hallinnalla on pyrittävä toteuttamaan turvatoimien yhdistelmä, jolla saadaan aikaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä. Katakri 2015 - auditointityökalun avulla arvioidaan kohdeorganisaation yleistä kykyä suojata viranomainen salassa pidettävää tietoa. Näin ollen Katakrin avulla tehtyä yritysturvallisuusselvitystä voidaan käyttää niin kotimaisissa kuin kansainvälisissäkin hankkeissa. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.)

Vaikka Katakri 2015 - auditointityökalussa kuvatut EU:n neuvoston turvallisuussääntöjen vaatimukset koskevat vain EU:n turvallisuusluokiteltujen tietojen suojaamista, ne edustavat EU:n jäsenvaltioiden yhteisesti hyväksymiä ja käyttämiä salassa pidettävän tiedon suojaamista koskevia perusperiaatteita ja vähimmäisvaatimuksia Euroopassa ja luovat sen vuoksi hyvän perustan salassa pidettävien tietojen suojaamiseksi myös Suomessa. Jäsenvaltiot noudattavat EU:n

turvallisuussääntöjä kansallisen lainsäädäntönsä mukaisesti, joten Suomessa EU:n salassa pidettävien tietojen suojaamisessa noudatetaan EU:n vaatimusten lisäksi tietoturvallisuusasetusta. Tietoturvallisuusasetuksen ja EU:n neuvoston turvallisuussääntöjen vaatimukset eivät merkittäviltä osin poikkea toisistaan. Mikäli Katakri 2015 -auditointityökaluun kirjattu vaatimus koskee pelkästään EU:n salassa pidettävää tietoa, se ilmenee lähdeviitteistä. Katakri 2015 - auditointityökalun osa-alueet on laadittu erillisiksi kokonaisuuksiksi, joten osa-alueita voidaan käyttää myös erikseen. Esimerkkinä on osittainen yritysturvallisuusselvitys, joka voidaan tehdä yrityksen toiminnan muuttuessa tai silloin kun auditointi kohdistuu rajattuun osa-alueeseen. Organisaation tulee kuitenkin täyttää T-osion vaatimukset osittaisenkin yritysturvallisuusselvityksen yhteydessä. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015.) Tässäkin esiin tuodaan T osion eli turvallisuusjohtamisen osa-alueen merkityksellisyys Katakri 2015 – auditointityökalun yhteydessä.

Katakri 2015 - auditointityökalua ei ole tarkoitettu käytettäväksi sellaisenaan julkisen hankinnan turvallisuusvaatimuksena. Julkisessa hankinnassa tarkat turvallisuusvaatimukset tulisi määrittää erikseen ottaen huomioon hankintaa koskevat riskit ja erityistarpeet. Yksittäiseen hankkeeseen voi sisältyä muitakin kuin Katakri 2015 - auditointityökalun koottuja salassa pidettävän tiedon käsittelyä ja suojaamista koskevia vaatimuksia. Näiden vaatimuksien toteutumista ei arvioida Katakri 2015 avulla, vaan kohdeorganisaatio sitoutuu noudattamaan niitä sopimusperusteisesti. (KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille 2015).

4 Katakri 2015 - auditointityökalulle merkitykselliset turvallisuuden osa-alueet

Aiemmin julkaistuille kriteeristöille merkityksellisiä turvallisuuden osa-alueita ovat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus sekä tietoturvallisuus. Hallinnollisessa turvallisuudessa oli mukana turvallisuuspolitiikka, turvallisuuden vuotuinen toimintaohjelma, sekä tavoitteiden määrittely, riskien tunnistus, arviointi ja kontrollit. Mukana olivat myös turvallisuusorganisaatio ja vastuut, onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat sekä ennalta ehkäisevät toimenpiteet, turvallisuusdokumentaatio ja sen hallinta. Lisäksi hallinnolliseen turvallisuuteen kuuluivat turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen, raportointi ja johdon katselmukset. Henkilöstöturvallisuudessa olennaista ovat henkilöstön työsuhteen elinkaari suunnittelu rekrytoinnista, työsuhteen päättymiseen, sekä henkilöstön riittävän osaamisen varmistaminen, sekä tehvävään muun soveltuvuuden varmistaminen. Fyysisessä turvallisuudessa tärkeää on itse alueen turvallisuus, rakenteellinen turvallisuus, sekä turvallisuustekniset järjestelmät. Tietoturvallisuus osa-alueeseen liittyy olennaisesti tietoliikenneturvallisuus, tietojärjestelmäturvallisuus, sekä käyttöturvallisuus. Katakri ensimmäisessä versiossa tietoturvallisuuteen kuului myös hallinnollinen tietoturvallisuus, sekä henkilöstön tietoturvallisuus, mutta ne integroitiin osaksi niihin suoraan liittyviä osa-alueita

Katakrin toisessa versiossa. Katakrin kaikki versiot keskittyvät security-näkökulmaan, joka liitetään esimerkiksi vartiointiin, sekä toimitilaturvallisuuteen. (Mäkinen 2007, 56 ,125.)

Katakri 2015 - auditointityökalua toteutetaan turvallisuusjohtamisen kautta, koska se tarjoaa kaikki ne välineet joilla voidaan johtaa ja hallita turvallisuutta erilaisten työkalujen avulla. Lisäksi määritellään, dokumentoidaan sekä todennetaan, että vaatimukset täyttyvät eri kriteereiden ja vaatimusten yhteydessä. Turvallisuusjohtamisen osa-alue on myös olennaisin osa uutta Katakri 2015 - auditointityökalua ja siihen perustuu myös turvallisuusjohtamisen teorian laajempi käsitteleminen toiminnallisen opinnäytetyöni teoriaosuudessa.

4.1 Riskienhallinta

Riskienhallinnalla tarkoitetaan niiden toimenpiteiden ja menetelmien kokoelmaa, joilla organisaatiossa riskejä pyritään tunnistamaan, arvioimaan ja hallitsemaan (VTT 2010). Turvallisuusjohtamisen yksi merkityksellisimpiä työkaluja on riskien arviointi. Sen avulla arvioidaan työympäristötekijöiden vaikutukset ja työolojen kehittämistarpeet. Turvallisuusjohtaminen varmistaa myös työntekijöiden motivoinnin, osaamisen sekä osallistumisen. Riskien arviointi on järjestelmällistä, sekä laaja-alaista terveyshaittojen, sekä vaarojen tunnistamista ja niiden merkityksen arvioimista työntekijän terveydelle ja turvallisuudelle. Riskien arvioinnin tavoitteena on työn turvallisuuden parantaminen. Riskienhallinta on osa turvallisuusjohtamista. Riskienhallinta on järjestelmällistä työtä toiminnan jatkuvuuden ja henkilöstön turvallisuuden varmistamiseksi. Se tarkoittaa kaikkea organisaatiossa tehtävää toimintaa riskien pienentämiseksi tai poistamiseksi. Käytännön työelämässä riskienhallinta on turvallisuusjohtamisen työväline. Työsuojelupäällikkö ja työsuojeluvaltuutettu ovat lainsäädännön edellyttämiä asiantuntijoita ja yhteistoimintahenkilöitä työpaikalla. (Työsuojeluhallinto 2014).

Riskienhallinnalla muodostetaan myös yksi perusta turvallisuusjohtamiselle. Siinä on kyse riskien tunnistamisesta ja riskien todennäköisyyksien sekä toteutumisen arvioinnissa. Riskienhallinta noudattaa niin sanottua kehämallia, jossa riskejä arvioidaan jatkuvasti uudelleen toimintaympäristön muuttuessa. Riskejä hallitaan järjestelmällisillä toimilla, joilla pyritään varmistamaan organisaation häiriötön toiminta. Riskeihin varaudutaan niiden estämisellä, vähentämisellä, siirtämisellä sekä jatkuvuussuunnittelulla. Riskienhallinta on osa jokapäiväistä toimintaa, johon on olennaista määritellä tarkoitus, tavoitteet, roolit ja vastuut. (Paasonen ym. 2012, 80 - 82). Riskienhallinta alkaa riskien tunnistamisella, koska riskejä joita ei ole tunnistettu ei voi myöskään hallita. Riskien tunnistaminen tarkoittaa sitä, että erilaisia työkaluja ja menetelmiä hyödyntämällä havaitaan ennakolta riskejä sekä vaaroja. Tunnistusmenetelmien perusteella tulee pystyä arvioimaan riskin mahdollisuus ja sen toteutumisen todennäköiset seuraukset. Tunnistusmenetelmien monipuolisuudella, paitsi edesautetaan arviointiprosessin

onnistunutta läpiviemistä, niin myös voidaan saada esiin piileviä riskejä, joita ei muuten vältämättä olisi havaittu. Riskien analysoinnin tavoitteena on tunnistaa kohteen riskit sekä arvioida niiden todennäköisyydet ja odotetut vahingot. Riskianalyysia voidaan tarkastella teknisesti, jolloin tunnistetaan ja arvioidaan riskiä, jonka tuottaa jokin tekninen järjestelmä. Riskikohteet käydään järjestelmällisesti läpi, jonka avulla pyritään selvittämään vahingon todennäköisyydet ja seuraukset. Riskianalyysi voi olla myös laajempi käsite, jolloin sillä tarkoitetaan kokonaisuutta, johon kuuluu riskin määrittäminen, arviointi, kokeminen ja hallinta. Käytännön tasolla kyse on silloin jo riskienhallintaprosessista. Riskianalyysimenetelmiä on runsaasti ja jokaiseen riskiin on parasta käyttää juuri siihen suunniteltua menetelmää, menetelmää valittaessa on huomioitava organisaation laajuus, sekä sen eri toiminnot. Riskien analysointi on yhteistyötä, jossa alusta lähtien eri toimijat organisaatiossa tekevät yhdessä analysointityötä. Käytännössä jokaisesta eri henkilökuntaryhmästä tulisi olla osallistujia analyysiryhmässä, jotta riskitietoisuus eri aloilta leviäisi kaikkien keskuuteen, sekä riskit saadaan kartoitettua tarkemmin, kun kaikista henkilöstöryhmistä on osallistujia mukana. Riskianalyysin perimmäisenä tarkoituksena on saada riskit tärkeysjärjestykseen, mutta tärkein vaihe on sopia tunnistettujen ja tärkeysjärjestyksessä olevien riskien hallintatoimenpiteistä. (Flink, Reiman & Hiltunen 2007, 131, 136 -138).

Organisaation riskit kohdistuvat sen maineeseen, henkilöstöön, tietoon, ympäristöön ja omaisuuteen. Organisaatio voi ottaa käyttöönsä riskienhallintamallin, jolla pyritään varmistamaan toimintojen tarkoituksenmukaisuus, sekä tehokkuus, taloudellisen tiedon ja raportoinnin luotettavuus sekä sääntelyn noudattaminen. (Paasonen ym. 2012, 82 - 85). Riskienhallinta on järjestelmällistä työtä henkilöstön turvallisuuden, sekä toiminnan jatkuvuuden varmistamiseksi. Se tarkoittaa kaikkea organisaatiossa tehtävää toimintaa riskien minimoimiseksi tai poistamiseksi. Käytännön työelämässä riskienhallinta on turvallisuusjohtamisen työväline. (Työsuojeluhallinto 2010).

Riskienhallinnan organisoimisen hallinnoimiseksi on luotu useita riskienhallintastandardeja, julkaisuhetkestä lähtien ne ovat uusineet aiempien standardien tulkintoja riskienhallinnasta, usein laajentaen itse riskienhallinnan käsitettä. Standardeja kehittävät valtioiden laitokset sekä kansainväliset standardointiorganisaatiot. Riskienhallintastandardien hyödyntäminen organisaatiossa voidaan suunnitella niiden sisältöä soveltaen, koska ne ovat ohjeellisia menetelmiä. Riskienhallintastandardit kattavat laajasti riskienhallinnan osa-alueet ja luovat yhteisen sanaston ja metodit riskienhallinnalle. Useimmiten organisaatioiden käytössä tällä hetkellä olevat riskienhallintajärjestelmät pohjautuvat ISO 31 000-standardiin tai yleisesti hyväksyttyyn COSO ERM-malliin. (Ilmonen ym. 2010, 30 - 31; Hopkin 2012, 57.)

Standardi ISO 31000 julkaistiin vuonna 2009 ja se on ensimmäinen kansainvälinen riskienhallinta standardi. Se muutti merkittävästi tapaa ajatella riskejä tuoden esille ajatuksen, että

riskit ovat positiivisia tai negatiivisia vaikutukseltaan sekä asialla on merkitys niiden hallintaan. Standardi koostuu riskienhallinnan toimintavasta, viitekehyksestä sekä hyvin kattavasta riskienhallinta-sanastosta joihin sisältyy riskienhallinta prosessi, sen vaatimat puitteet, sekä periaatteet ja miten koko tämä kokonaisuus on toisiinsa yhteydessä ja toimii yhdessä. (Ilmonen 2010, 32 - 33; ISO 31 000 2009.)

COSO ERM-malli on Yhdysvalloissa kehitetty jo yli 20 vuotta käytössä ollut ja edelleen jatkuvasti kehitetty riskienhallinta malli Enterprise Risk Management – Intergrated Framework käsittelee sisäistä valvontaa entistä kattavammin ja keskittyy aikaisempaa selkeämmin ja perusteellisemmin organisaatioiden riskienhallintaan. Tarkoituksena ei ole syrjäyttää sisäisen valvonnan mallia vaan liittää se osaksi riskienhallintaa, mallia on suunniteltu oman sisäisen valvonnan ja kehittämisen parantamiseen riskienhallintaprosessissa nykyistä kokonaisvaltaisemmaksi. Tähän malliin on julkaistu viimeisin päivitys vuonna 2014. (COSO-ERM 2015; The Committee of Sponsoring Organizations of the Treadway Commission 2015).

Yrityksen turvallista toimintaa uhkaavien riskien hallinta toimii perustana turvallisuusjärjestelyjen oikealle mitoitukselle. Toimivaltainen viranomainen suhteuttaa vaatimuksensa lähtökohtaisesti siihen uhkaympäristöön ja niihin turvatoimiin (kontrolleihin), jotka yritys esittää. Viranomaisen käsitys uhkista saattaa kuitenkin poiketa siitä, mihin yritys on omista lähtökohdistaan päätynyt. Tiedon suojaamiseen tähtäävä turvallisuusriskien hallintaprosessi voidaan kuvata yksinkertaistetusti neljään vaiheeseen, joista ensimmäinen on riskien tunnistaminen, toinen riskien analysointi vaikutusten ja todennäköisyyksien määrittämiseksi, kolmas riskien arviointi tarkoituksenmukaisten turvatoimienvalitsemiseksi ja neljäntenä riskien toteutumiseen varautuminen riskienhallintaprosessin seurantamenettelyjen kautta. Yrityksen tulee pystyä riskienhallintaprosessinsa kautta osoittamaan toimivaltaiselle viranomaiselle perusteensa valituille turvatoimille ja niiden riittävyydelle. Yritystä suositellaan keskustelemaan riskiensä määrittelystä ja turvatoimisuunnitelmistaan toimivaltaisen viranomaisen kanssa jo varhaisessa vaiheessa, jotta sekä yrityksen että toimivaltaisen viranomaisen arviot kyseisen ympäristön riskeistä pystytään huomioimaan jo turvatoimia suunniteltaessa. (KATAKRI – Tietoturvallisuuden auditointityökalu viranomaiselle.)

”Viranomaisen arvioinnissa huomioidaan muun muassa tiedon suojaustaso, määrä, muoto ja luokitteluperuste suhteessa arvioituun vihamielisen tai rikollisen toiminnan uhkaan. Katakrin eri osioissa kuvattujen turvatoimien soveltamisessa tulee huomioida, että kuvatut toteutusesimerkit voivat olla korvattavissa myös muilla vastaavan tasoisilla suojauksilla. Esimerkiksi vahvan käyttäjätunnistuksen toteutus on mahdollista ratkaista tietoteknisen tai fyysisen turvallisuuden menetelmin. Toisaalta esimerkiksi tietoliikenteen salaukselle ei yleensä pystytä toteuttamaan riittäviä korvaavia turvatoimia tilanteissa, joissa liikenne kulkee fyysisesti suo-

jatun vyöhykkeen ulkopuolella. Tilanteissa, joissa kohteessa ei arvioida ilmenevän vaatimusten tai toteutusesimerkkien taustalla olevia uhkia, viranomainen voi arvioida kyseisen vaatimuksen täyttämättä jättämisen olevan perusteltua. Esimerkiksi työasemiin, joista on fyysisesti luotettavasti poistettu kaikki verkkoliikennöintiin kykenevät rajapinnat, ei yleensä ole perusteltua edellyttää palomuurin tai sen säännöstön ylläpitomenettelyä. Viranomainen arvioi riskienarvioinnissaan soveltuviksi valittujen suojausvaatimusten täyttymisen Katakrissa kuvattuja toteutusesimerkkejä hyödyntäen. Viranomaisen arviointi perustuu yleensä hallinnollisen ja teknisen todentamisen menetelmiin." (KATAKRI – Tietoturvallisuuden auditointityökalu viranomaiselle.)

Yrityksen turvallisuusjärjestelyjen vaatimustenmukaisuuden kuvauksen tavoitteena on esittää kootusti ne turvallisuusjärjestelyt, joilla yritys pyrkii täyttämään turvallisuusvaatimukset. Kuvausta hyödynnetään erityisesti viranomaisen auditoinnin suunnittelussa ja toteutuksessa. (KATAKRI – Tietoturvallisuuden auditointityökalu viranomaiselle.)

4.2 Turvallisuusjohtaminen

Turvallisuusjohtaminen on kokonaisvaltaista toimintaa organisaation turvallisuuden hallitsemiseksi. Se tarkoittaa on kaikkia niitä yritysjohdon ja työnjohdon toimenpiteitä, joilla pyritään yrityksen turvallisuustason kehittämiseen. Turvallisuusjohtamisessa yhdistyvät menetelmien, toimintatapojen ja ihmisten johtaminen, se käsittää sekä korjaavan että ennakoivan toiminnan työympäristön jatkuvaksi parantamiseksi. Turvallisuuden hallintaa käytetään usein turvallisuusjohtamisen synonyymina, toisinaan turvallisuusjohtaminen mielletään kapeampana linjaesimiesten käytännön turvallisuustoimintana. Englannin kielen "safety management" voidaan kääntää sekä turvallisuuden hallinnaksi, että turvallisuusjohtamiseksi. (Oedewalt & Reiman 2008, 435).

Turvallisuusjohtaminen on osa normaalia yrityksen johtamista, sen tavoitteena on toiminnan turvallisuus eikä, että se on erillinen turvallisuustoiminto. (Yritysturvallisuus EK). Lainsäädännölläkin on oma roolinsa turvallisuusjohtamiselle, työturvallisuuslaki (738/2002) määrittää turvallisuusjohtamisen vähimmäisvaatimukset. Turvallisuusjohtaminen tulee olla kokonaisvaltaista, niin lakisääteisen kuin omaehtoisen turvallisuuden hallintaa, jossa yhdistyvät toimintojen, sekä menetelmien ja toimintatapojen että ihmisten johtaminen. Se sisältää ajatuksen jatkuvasta terveellisyyden ja turvallisuuden edistämisestä ja se pitää sisällään jatkuvan suunnittelun, toiminnan ja seurannan. (Työsuojeluhallinto 2014). Turvallisuusjohtaminen käsittää sekä ennakoivan että korjaavan toiminnan työympäristön jatkuvaksi parantamiseksi. (Oedewald & Reiman 2006, 25).

Turvallisuusjohtamisella pyritään hallitsemaan kaikkia organisaation turvallisuusasioita. Organisaatioturvallisuus on paitsi organisaation henkilöstön, omaisuuden, tiedon sekä ympäristön suojaamista vahingoilta niin myös se on tae organisaation toimintaedellytyksille sekä tuotannon ja toiminnan häiriöttömyydelle. Turvallisuusjohtaminen on ennakoivaa toimintaa, jolla luodaan toimintavalmiuksia (Kerko 2001, 21). Turvallisuusjohtamista vaikeuttaa se, että turvallisuustoiminta koetaan eri tavoin, toisinaan vakuuttamisena tai riskienhallintana ja toisinaan jopa osana kiinteistötoimintaa. (Leppänen, J. 2006, 57-58). Turvallisuusjohtamisen pitäisi olla systeemiajatteluun, ei komponenttiajatteluun, pohjautuvaa. (Oedewalt, P. & Reiman, T. 2008, 67).

Työpaikka pystyy järjestelmällisesti varmistamaan omien käytäntöjensä jatkuvan parantamisen toimivalla palautejärjestelmällä, mikä on yksi olennainen tekijä turvallisuusjohtamisessa. Organisaatiolla tulisi aina olla olemassa turvallisuusperiaatteet tai turvallisuuspolitiikka, joilla määritellään yleiset turvallisuuden päämäärät. (Työsuojeluhallinto 2014).

4.2.1 Organisaation johto ja -strategia

Turvallisuusjohtamisen kokonaisuus rakentuu organisaation turvallisuusjohtamisen koko vastuu- ja toimintakentästä. Se toimii ylimmän johdon toteuttaman strategian johtamisen, sekä linjajohdon toteuttaman operatiivisen johtamisen välissä eräänlaisena turvallisuuteen ja riskienhallintaan erikoistuneena asiantuntija-adapterina. Turvallisuusjohtamisen rakentamisen ylin taso on organisaation missio, visio ja strategia. Toisen tason muodostavat operatiivisen toiminnan organisoiminen sekä organisaation prosessit tuotantovälineineen. Näiden väliin turvallisuus- ja riskienhallintajohto luo kartan nykyisistä toiminnoista, joka kuvaa näiden kahden tason toteuttamisen tilan. Ei ole yhtä turvallisuusjohtamisen-projekti mallia joka toimisi kaikkialla. Jokaisen organisaation tulisi laatia omat tarpeet ja tavoitteet turvallisuus-johtamiselle ja päivittää niitä säännöllisesti vuosittain johdon strategian muutosten perusteella. Huomioitavaa on kuitenkin, että operatiivisessa toiminnassa, toimintakentän- lainsäädännön-, asiakkaiden tarpeiden muutoksissa, sekä viranomaisten vaatimuksesta on syytä tarkastella kokonaisuutena turvallisuusjohtamista organisaatiossa, jotta muuttuneet asiat ovat varmasti huomioitu siellä. Turvallisuusjohtamisen projektista saatu dokumentaatio toimii karttana toimintaa johdettaessa, joten niitä pitää päivittää säännöllisesti ja koordinoidusti. Turvallisuusjohtamisen projekti on pitkäjänteinen prosessi, johon osallistuvat sekä organisaation henkilöstöä, että ulkopuolisia asiantuntijoita. yhdessä organisaatiossa harvoin on kaikkea sitä viisautta, jota laajojen kokonaisuuksien rakentamisessa ja johtamisessa tarvitaan. (Leppänen, J. 2006, 58-61).

Organisaation strategia on perusta, johon turvallisuusjohtaminen perustuu. Turvallisuusjohtamisen näkökulmasta liiketoiminnan johtaminen voidaan jakaa kolmeen osa-alueeseen: arvoketju, yrityksen johtaminen sekä raha- ja reaaliprosessit. Turvallisuusjohtaminen on liitettävä kiinteästi reaali- ja rahaprosesseihin, yrityksen johtamiseen sekä arvoketjun toteutumiseen. Turvallisuusjohtamisella sekä riskienhallinnalla varmistetaan prosessien panosten, toimintojen ja tuotosten toteutuminen suunnitellusti. Turvallisuusjohtaminen toimii laatujärjestelmän osana varmistaen prosessin osien ja kokonaisuuden häiriöttömyyden sekä vahingoittamattomuuden. (Leppänen, J. 2006, 21-25).

Hyvän turvallisuusjohtamisen lähtökohtia on useita. Koko johdon tulee olla sitoutunut tällaiseen ajatteluun, jotta henkilöstö saadaan sitoutumaan siihen. Vasta henkilöstön sitoutuminen varmistaa sen, että turvallisuusjohtamisajattelu ja sen kautta tulevat toiminnot kehittävät turvallisuuskulttuuria.(Työsuojeluhallinto 2014). Turvallisuusjohtaminen sisältää kaikki ne osa-alueet ja toiminnot, joiden avulla varmistetaan organisaation tavoitteiden saavuttaminen ja suojattavien kohteiden vahingoittamattomuus. Turvallisuusjohtamisen projektin tulisi sisältää siis myös perinteisten turvallisuuden osa-alueiden lisäksi liike- ja muiden riskien hallinnan, nämä tuovat lisävaatimuksia turvallisuusjohtamiselle sekä sen toteuttamiselle. Yritysten liiketoiminnan tavoitteisiin perustuvan turvallisuusjohtamisen on perustuttava ylimmän johdon, sekä omistajien asettamille tavoitteille ja strategioille. Tuloksia saavutetaan toteuttamalla turvallisuusjohtamista käytännön teoissa. Turvallisuusjohtaminen ei ole vain turvallisuushenkilöstön vastuulla, vaan osa jokaisen perustehtäviä. Johdon sitoutuminen näkyy työpaikalla esimerkiksi johdon kierroksina sekä turvallisuusasioiden mukanaolona kaikissa kokouksissa ja palavereissa. Turvallisuusjohtamisen perustyökalut, kuten riskien arviointi sekä toiminnan seuranta ja tarkkailu, ovat itsestäänselvät osat työpaikan toimintaa. (Työsuojeluhallinto 2014).

Yrityksen johdon rooli korostuu turvallisuusjohtamisessa turvallisuudesta vastaavana, sekä turvallisuutta ohjaavana tekijänä. Johdon tehtävänä on asettaa yrityksensä turvallisuustoiminnalle tavoitteet, tarjota resurssit niiden saavuttamiselle, sekä valvoa niiden toteutusta. (Oedewald & Reiman 2006, 25). Leppänen (2006, 58) näkee, että ainoa oikea lähestymistapa turvallisuusjohtamiseen on omistajanäkökulma. Omistajan näkökulmalla tarkoitetaan keskittymistä yritystoimintaan sijoitetun pääoman tuoton kasvattamiseen.

Turvallisuuskulttuuri heijastaa organisaation perusarvoja, normeja, olettamuksia ja odotuksia, jotka sisältyvät yrityksen toimintaperiaatteisiin. Turvallisuuskulttuuri, organisaation tapa toimia turvallisuuden suhteen, vaikuttaa turvallisuusjohtamiseen. Turvallisuustyön pitäisi olla osa jokaisen esimiehen ja työntekijän normaalia työnkuvaa, työsuojelun asiantuntijat tukevat linjaorganisaation turvallisuustyötä. (Työsuojeluhallinto 2014.)

Turvallisuuskulttuuri on osa organisaatiokulttuuria. Siinä on kyse merkityksistä ja käytännöistä, joilla varaudutaan riskeihin ja epätoivottuihin tilanteisiin, sekä turvallisuustasosta, jonka organisaation tai yrityksen johto hyväksyy. Turvallisuuskulttuurilla on vahva sidos turvallisuusjohtamiseen, koska se on organisaation tapa toimia turvallisuusasioissa. Turvallisuuskulttuuri on kyky ja tahto ymmärtää turvallisuutta, siinä korostetaan voimakkaasti henkilöjohtamisen merkityksellisyyttä, koska kulttuurin kehittämisessä olennaista on henkilöstön läsnäolo ja motivaatio sen kehittämiseen. Henkilöstö saadaan mukaan parhaiten, jos turvallisuutta lähestytään työviihtyvyyden ja inhimillisten tarpeiden näkökulmasta. Turvallisuusjohtamisen yksi olennainen osa on turvallisuuskulttuurin ymmärtäminen ja erityisesti sen johtamiseen olennaisesti kuuluvat selkeät ohjeet, toimintatavat, monipuolinen viestintä, sekä riittävän kattava kommunikointi turvallisuustasosta, hyväksyttävistä toimintatavoista, sekä riskeistä. Johdon näkyvä sitoutuminen edesauttaa henkilöstön sitoutumista hyvän turvallisuuskulttuurin luomiseen, jotta sen edellytykset kyetään saavuttamaan. (Paasonen ym., 2012, 96-99).

Turvallisuusjohtaminen on osa työpaikan turvallisuuden kehittämistä. Se vaikuttaa positiivisesti työilmapiiriin, henkilöstön sitoutumiseen, tuotannon laadun paranemiseen sekä tapaturmien ja onnettomuuksien ehkäisemiseen. (Työsuojeluhallinto 2014). Turvallisuuden hallinta on suunnitelmallista, sekä organisaation joka tason huomioivaa toimintaa turvallisuuden edistämiseksi. Se pitää sisällään kaikki ne menettelytavat sekä toiminnat, joilla hyvään varautumisen tasoon päästään vaihtelevissa tilanteissa. Toiminta perustuu kiinteään yhteistyöhön koko henkilöstön kanssa. (Työsuojeluhallinto 2010).

4.2.2 Turvallisuuspolitiikka

Turvallisuuspolitiikassa ilmenee johdon kannanotto turvallisuustyön merkityksestä, henkilöstön keskinäisen yhteistyön toimintaperiaatteet, sekä siinä on toimintatavat määriteltävä. Turvallisuusjohtamisen avain osa-alueet organisoinnin näkökulmasta ovat toimintavastuiden, toimintajärjestelmien, sekä toimintavelvollisuuksien määritteleminen ja niille tarvittavien resurssien varaaminen, jotta tavoitteiden toteuttaminen on käytännössä mahdollista, toiminta ja toteuttaminen käytännössä tulisi kuulua osaksi työn tekemistä. (Työsuojeluhallinto 2014).

Turvallisuuspolitiikassa tulisi ilmetä yrityksen turvallisuuskulttuuria ohjaavat arvot ja se tulisi tuoda esiin ymmärrettävästi, sekä tiivistetysti. (Kerko 2001, 44 - 46). Turvallisuusjohtamisen tulee perustua valittuihin ja päätettyihin toimintaperiaatteisiin ja politiikkoihin, joista muodostetaan organisaatiolle turvallisuuspolitiikka. Se on strateginen ohjelma, jolla halutaan turvallisuus tärkeäksi osaksi liiketoimintaa, turvallisuushallintajärjestelmän aikaansaaminen, riittävät resurssit, menettelytapoja, henkilöstön sitoutuminen, koulutuksen varmistaminen, riskiperiaatteen huomioiminen ja katselmusten suorittaminen sekä vastuiden, valtuuksien ja velvoitteiden määritys. Nykytilanteen hyvä kartoitus, joka kattaa toiminnan ja riskien arvioinnin,

antaa perustan turvallisuustyölle. Nykytilanteen selvitykseen ja riskienarviointiin on valittavissa runsaasti työkaluja. Tehtyjen toimenpiteiden toteutumista pitää seurata, sekä ne pitää vastuuttaa ja turvallisuuden arvioimiseksi pitää valita sopivia mittareita. Osaaminen, oikeat asenteet ja motivaatio tarvitaan myös turvallisuuden saavuttamiseksi sekä ylläpitämiseksi. Johtamisen tueksi tarvitaan monipuolista tiedottamista näistä asioista. (Työsuojeluhallinto 2014).

Organisaation turvallisuuspolitiikan tarkoituksena on määritellä, mitä kaikkea organisaation turvallisuustoiminta sisältää. (Leppänen, 2006, 177). Se ilmentää myös johdon sitoutumista turvallisuuteen ja organisaation erityisiä painopistealueita turvallisuuden suhteen. (Oedewald ja Reiman. 2008, 436).

Ennen kuin organisaation turvallisuuspolitiikka voidaan laatia, on määriteltävä suojattavien kohteiden arvo, henkilöstön rooli turvallisuuden ylläpitämisessä, turvallisuusvastuiden jakaantuminen organisaatiossa sekä se, miten turvallisuustoiminta vaikuttaa organisaation sidosryhmiin. Näiden asioiden määrittely luo perustan organisaation turvallisuuspolitiikalle. Turvallisuuspolitiikassa määritellään organisaation turvallisuustoiminnan strategia ja tavoitteet, jotka pääsääntöisesti tähtäävät ”toiminnan turvaamiseen kaikissa olosuhteissa”.(Leppänen 2006, 177-178).

Turvallisuuspolitiikalla on kaksi ulottuvuutta, sisäinen ja ulkoinen. Ulkoinen turvallisuuspolitiikka määrittelee organisaation ne turvallisuustoiminnan periaatteet ja linjaukset, joilla voi olla vaikutusta ulkoisiin toimijoihin, Sitä ovat myös suhtautuminen korruptioon ja lahjontaan, yhteiskunta vastuu sekä Corporate governance. Turvallisuuspolitiikan sisäisessä ulottuvuudessa organisaation omalla henkilöstöllä on tärkeä rooli. Turvallisuuspolitiikasta ei tule tehdä mitään pitkää julistusta, vaan lyhyt ja ytimekäs johdon laatima määritelmä siitä, mitkä painopisteet ovat tärkeitä organisaation toiminnan jatkuvuuden turvaamiseksi. Sisäisessä turvallisuusviestinnässä rakennetaan turvallisuuskulttuuria, jonka hyvin oleellisia osia ovat turvallisuuteen liittyvät arvot. Turvallisuuspolitiikka voi sisältää myös turvallisuuden merkityksen, turvallisuustoiminnan sisältöön, vastuisiin, toimintakohteisiin ja toteutusvälineisiin liittyviä määritelmiä ja rajauksia. Turvallisuuspolitiikan lisäksi organisaation on laadittava turvallisuustoiminnan strategia sekä toimintasuunnitelma. (Leppänen 2006, 179)

4.2.3 Turvallisuusjohtamisjärjestelmät

Oedewald ja Reiman (2008, 64 - 65) näkevät tiivistetysti, että turvallisuusjohtamisjärjestelmällä tarkoitetaan järjestelmällistä ja dokumentoitua lähestymistapaa organisaation turvallisuuden hallintaan, sen tarkoituksena on tunnistaa, arvioida ja kontrolloida yrityksen toimin-

taan sisältyviä vaaroja. Näiden lisäksi turvallisuusjärjestelmän tulisi sisältää yleisessä johtamisjärjestelmissä käsiteltäviä asioita kuten organisaatiorakenne, vastuualueet, toimintatavat, sekä resurssit.

Turvallisuustyön kehittäminen on synnyttänyt johtamisjärjestelmiksi kutsuttuja turvallisuuden parantamiseen tähtäävien toimintojen ohjaus- ja hallintajärjestelmiä, ne perustuvat yleisiin hyviin johtamistavan periaatteisiin. (Pohjola pankki 2014).

Turvallisuusjohtamisjärjestelmään tulee kuulua kaikki kymmenen organisaatioturvallisuuden osa-aluetta, joita ovat rikosturvallisuus, tuotannon ja toiminnan turvallisuus, työturvallisuus, ympäristöturvallisuus, pelastustoiminta, valmiussuunnittelu, tietoturvallisuus, henkilöturvallisuus, toimitilaturvallisuus, sekä ulkomaantoimintojen turvallisuus. Asiantuntemus eri turvallisuuden osa-alueilla monesti hajautuu organisaatiossa monesti useille eri toimijoille, tällöin yhdelläkään toimijalla ei ole mahdollisuutta tunnistaa ja ratkaista toisiinsa kytkeytyviä ongelmia. (Paasonen ym. 2012, 93 - 96).

Turvallisuusjohtamisjärjestelmä auttaa organisaatiota toimimaan paitsi kansallisen lainsäädännön mukaan ja niin myös kansainvälisten sopimusten mukaisesti, joista esimerkkinä EU-direktiivien mukaiset turvallisuusnormit. Sillä on vaikutuksensa myös yhteistyösopimusten, sekä yhteistyöverkostojen muodostumiseen. (Kerko 2001, 32). Turvallisuusjohtaminen perustuu laatujohtamisen malliin. Toistaiseksi turvallisuusjohtamisjärjestelmät eivät ole täysin vakiintuneet ja niiden sisällöt saattavat vaihdella useisiin turvallisuuden eri osa-alueisiin. Turvallisuusjohtamisjärjestelmien elementteihin kuuluvat organisaatiorakenne, resurssit ja vastuualueet. Yhden johtamisjärjestelmän tarkoitus on tuottaa suurempaa synergiaetua kuin useat erilliset järjestelmät, joita käytetään yhtäaikaisesti. (Paasonen ym. 2012, 93 - 96).

4.2.4 Hallinnollinen turvallisuus

Hallinnollisessa turvallisuudessa yrityksen johto luo edellytykset tietoturvallisuusasioiden ylläpitämiselle, sekä kehittämiselle. Se on tietojärjestelmän tietoturvan eri osa-alueiden johtamista, jossa tarkastellaan esimerkiksi tietoturvallisuuden johtamista, resursointia, toimintapolitiikkaa sekä tietoturvallisuuteen liittyvien asioiden hoitamisen vastuuttamista. (Miettinen 1999, 18; Ruohonen 2002, 4).

Hallinnollinen turvallisuus on osa tietoturvallisuuden kehittämistä sekä sen johtamista, se pitää sisällään myös yhteydenpidon toimielimiin sekä tarvittaessa viranomaisiin, jotka vastaavat tietoturvallisuudesta organisaation sisällä sekä organisaation ulkopuolella, siitä vastaa pääsääntöisesti tietohallinto organisaatiossa. Organisaation tietohallinto vastaa pääsääntöisesti

hallinnollisesta turvallisuudesta. Avaintoimintoina ovat lainsäädännön0 ja erilaisten lisenssisopimusten, sekä palvelusopimusten vaikutusten arvioiminen tietoturvallisuudessa käytettäviin menetelmiin. (Hakala, Vainio ja Vuorinen 2006, 10–11; SFS 27001 2006, 32–33.)

Hallinnollinen turvallisuus muodostuu organisaation hyväksymistä periaatteista. Se on keskeinen osa tietoturvallisuuden johtamistoimintoa ja se muodostaa lähtökohdan organisaation koko tietoturvallisuustoiminnalle. Hallinnollisessa turvallisuudessa on kysymys paitsi vastuunjaosta, riskien arvioinnista, niin myös resurssien varaamisesta, sekä sen kautta luodaan organisaatiolle tietoturvalliset toimintatavat ja -mallit. Toimintamallien pohjalta luodaan henkilöstön koulutusjärjestelmät, liittyen paitsi tietoturvallisuuteen niin myös välttämättömiin ohjeistuksiin ja valvonta- sekä tarkastusmenettelyohjeistuksiin, jotka ovat oleellisia tietoturvallisuuden ylläpitämiseen sekä kehittämiseen. (SFS 27001 2006, 14–20.)

Hallinnollisessa turvallisuudessa oleellista on käyttäjien organisaation tietoturvallisuus periaatteiden tietäminen, sekä ymmärtäminen. Tätä varten organisaation johdon tulee julkaista organisaation tietoturvapolitiikka. Politiikka jaetaan koko henkilökunnalle. Tietoturvallisuuspolitiikan tueksi on suunniteltava ohjekokonaisuus organisaatiolle sekä määritellä tarpeellisten tietoturvallisuuskuvausten taso. Näiden lisäksi muodostetaan tietoturvallisuussuunnitelmat, mistä näkyvät organisaatiolle elintärkeät tietojärjestelmät, sekä niiden vaatimat toipumistoimet sekä vaatimukset poikkeustilanteissa. (SFS 27001 2006, 14 – 20.)

Merkittävä osuus hallinnollisessa turvallisuudessa on tietoturvallisuuden hallintajärjestelmän sisäisissä sekä ulkoisissa auditoinneissa. Tietoturvallisuuspolitiikasta vastaavien tulee katselmoida tietoturvallisuuden hallintajärjestelmä, ennalta suunnitellun ohjelman aikataulun mukaisesti, vähintään kerran vuodessa. Katselmoinnin avulla varmistetaan hallintajärjestelmän jatkuvuus, soveltuvuus, asianmukaisuus ja vaikuttavuus, tulokset dokumentoidaan katselmuksesta selkeästi, tuloksiin pohjaten toteutetaan tarpeelliset parannukset ja muutokset tietoturvallisuuden hallintajärjestelmään. Organisaation tulisi suunnitella sekä suorittaa sovituin aikavälein tietoturvallisuuden auditointeja, jotta kyetään selvittämään ja osoittamaan ovatko tietoturvallisuuden hallintajärjestelmän velvoitteet, eri turvamekanismit, prosessit ja menettelytavat suunnitelmien, sekä vaatimusten, että lainsäädännön mukaisia. Tarkoitus on osoittaa, että toiminta on tunnustettujen tietoturvallisuusvaatimusten mukaista, sekä uskottavasti toteutettua, sekä ylläpidettyä. (SFS 27001 2006, 26.)

4.2.5 Henkilöstöturvallisuus

Hakala, Vainio ja Vuorinen (2006) määrittelevät henkilöturvallisuuteen kuuluvaksi toimenpiteet, joilla huolehditaan tietojärjestelmän käyttäjien kyvystä toimia, sekä toimista joilla heidän käyttöoikeuksia rajataan organisaation tietojärjestelmissä käyttötarpeen mukaiseksi ja

rajataan tietoja, joihin heillä on oikeudet saada käytettävikseen. Tällaisia erilaisia varmistustoimenpiteitä ovat esimerkiksi varahenkilöjärjestelyt, tietoturvallisuuteen sekä tietojärjestelmiin liittyvät koulutukset, vastuiden ja oikeuksien määrittely tarveperäisesti ja tarvittaessa työntekijöiden taustatietojen selvittäminen. Henkilöturvallisuudesta vastaa organisaation henkilöstöhallinto yhteistyössä tietohallinnon ja muiden turvallisuuselinten kanssa. (Hakala, Vainio ja Vuorinen 2006, 11.)

Laaksosen, Nevasalo ja Tomula (2006) mukaan henkilöturvallisuus on myös henkilöstöön kohdistuvia tietoturvallisuus uhkien hallintaa sekä henkilöstön toimista aiheutuvien tietoturvallisuus uhkien hallitsemista. Vaaralliset työyhdistelmät aiheuttavat tietoturvallisuus ongelmia, välttääkseen niitä henkilöstön toimenkuvien tulee olla selkeitä ja vastuiden, sekä oikeuksien rajattuja. Henkilöstöhallinnon erilaiset prosessit palkkauksesta, työtehtävien muutoksista aina työsuhteen päättymiseen ovat osa henkilöturvallisuuteen liittyviä riskitekijöitä, jotka tulee huomioida ja niihin tulee etukäteen varautua. (Laaksosen, Nevasalo ja Tomula 2006, 138 – 144.)

Henkilöstöturvallisuudella tarkoitetaan toimenpiteitä, joissa tarkastellaan organisaation tietojärjestelmän ja tilojen suojausta ihmisten tahallisilta tai tahattomilta uhilta. Huomioitavaa on myös ketkä ja millaiset ihmiset pääsevät varmistamaan tietoturvallisuutta. Siihen kuuluvat myös organisaation varamiesjärjestelyt, vastuiden ja oikeuksien määrittelyt, sekä koulutuksen järjestäminen tietojärjestelmiin liittyen. Henkilöturvallisuus ei rajoitu vain omaan henkilökuntaan, kaikki muutkin organisaation toimintaan liittyvät sidosryhmät on otettava suunnittelussa huomioon esimerkiksi ulkopuoliset työntekijät, asiakkaat sekä vierailijat. Yhä tärkeämmäksi on havaittu uuden työntekijän taustatietojen tarkistamisen ennen sopimussuhteen alkamista. Toimenpide on omiaan hallitsemaan riskiä, jossa työntekijä osoittautuukin rikolliseksi tai epäpäteväksi. Julkisuudessa on ollut tapauksia joissa muun muassa opettaja, lääkäri ja sairaanhoitaja ovat toimineet työsuhteessa, vaikka heillä ei ole ollut pätevyyttä tai heillä on jopa ollut väärennetty todistus koulutuksesta. (Miettinen, J. 1999, 180, 182). Kriittisiin tehtäviin hakevista henkilöistä voi myös teettää Suojelupoliisilla turvallisuusselvityksen, jossa Suojelupoliisi selvittää työntekijän taustat. Kohteena olevan henkilön suostumus tarvitaan ennen kuin turvallisuusselvitys voidaan tehdä. (Turvallisuusselvityslaki 2014/726).

Henkilöstöturvallisuuteen kuuluu myös henkilön taustojen tarkistaminen rekrytointiprosessin yhteydessä, kuten myös henkilöstön kouluttaminen, ohjeistaminen sekä perehdytys, kouluttaminen sekä mahdolliset salassapito- ja kilpailukieltosopimukset. Henkilöstöturvallisuuden tavoitteena on vähentää henkilökunnan tahattomia vahinkoja. Siten hyvä henkilöstöturvallisuus perustuu osaavalle ja sitoutuneelle henkilöstölle. Henkilöstöä rekrytoitaessa lisää suositeltavaa on varmistua rekrytoitavien taustoista, sillä voidaan vähentää uuden henkilön rekrytointi prosessiin liittyviä riskejä. (Leppänen 2006, 205.)

Asiakkaiden, sekä vierailijoiden turvallisuus kuuluu myös tärkeänä osana henkilöturvallisuutta. Sidosryhmien kannalta turvallisuusjärjestelyn asiallinen järjestäminen sekä toimivuus vaikuttavat vierailijan mielikuvaan organisaation tai yrityksen toiminnasta. Sillä saattaa olla merkittävä vaikutus asiakkaiden käsitykseen yrityksestä. Liioitellut ja selvästi alimitoitetut turvajärjestelyt, antavat helposti vierailijalle huonon kuvan yrityksestä ja sen toiminnasta. Näihin turvallisuusjärjestelyihin kuuluu esimerkiksi sisäänkirjautumiseen liittyvät turvallisuusjärjestelyt sekä vaitiolovelvollisuussitoumukset ja selkeästi havaittavat ja ohjaavat kyltit, sekä opasteet. (Leppänen 2006, 204.)

Yleensä avainhenkilöitä ovat henkilöt, joilla on erityistä osaamista tai asiantuntemusta. Heidän olemassaolo on kriittistä organisaation jatkuvalle toiminnalle. Pääasiassa heidän asiantuntevuutensa liittyy johtamiseen, tekniseen osaamiseen tai asiakassuhteisiin. Ongelmallista on, että heidän todellinen merkitys organisaatiolle havaitaan vasta kun heidät menetetään.(Leppänen 2006, 206.) Henkilöturvallisuuteen kuuluu olennaisesti sijaisjärjestelyt. Niiden tavoitteena on varmistaa organisaation häiriötön ja jatkuva toiminta. Odottamattomissa tilanteissa, joihin kuuluu esimerkiksi onnettomuudet tai sairastumiset, suositeltavaa olisi, että vähintään kaksi henkilöä pystyy hoitamaan samoja työtehtäviä. Henkilökunnan jatkuvalla kouluttamisella, sekä sijaisjärjestelyillä kyetään minimoimaan avainhenkilöriskien vaikuttavuus, niiden konkretisoituessa, organisaatiossa. (Leppänen 2006, 208.)

4.3 Fyysinen turvallisuus

Fyysiseen turvallisuuteen kuuluu tilojen, sekä niihin sijoitettujen laitteiden suojaaminen erilaisilta fyysisiltä uhilta joita ovat esimerkiksi tulipalot, murtautumiset, sekä ilkivalta. Ne voivat olla myös erilaisia ympäristöön liittyviä uhkia joista aiheutuu esimerkiksi vesivahinkoja. Lämpötilaan liittyvät ongelmat, sekä sähkökatkokset kuuluvat myös fyysisen turvallisuuden piiriin joilta on suojauduttava. Fyysisen turvallisuuden tavoitteena on taata turvallinen, häiriötön ja jatkuva toimintaympäristö. Toimitilojen suojaus toimii perustana kaikille suojaustoiminnoille, joita tietoturvallisuuden ylläpitämiseen on tarpeellista. (Laaksonen 2006, 125–127; Hakala, Vainio ja Vuorinen 2006, 11; SFS 27001 2006, 38.)

Fyysinen turvallisuus käsittelee asioita, joilla pyritään estämään tietojen tuhoutuminen, tietojen vahingoittuminen tai tietojen joutuminen vääriin käsiin. Kannettavat tietokoneet ovat muodostaneet vakavan tietoturvallisuus ongelman tai tarkemmin niihin kohdistuvat varkaudet. Nykyisin varkaudet kohdistuvat kasvavassa määrin tietokoneiden sisältämiin komponentteihin, kuten kovalevyihin, muistipiireihin ja muistikortteihin. Varkaudet tapahtuvat usein keskellä päivää, jolloin hälytysjärjestelmät ovat usein pois päältä. Keskeistä tietoturvallisuudessa on pääsyn valvominen tietojenkäsittelytiloihin. Avainhallinta on merkittävä osa fyysistä

turvallisuutta. Siinä huomioidaan paitsi sähköiset järjestelmät, niin myös fyysiset avaimet, joita voi olla eri sidosryhmillä. (Laaksonen 2006, 125–127; Hakala, Vainio ja Vuorinen 2006, 11; SFS 27001 2006, 38.)

4.4 Toimitilaturvallisuus

Toimitilaturvallisuudella tarkoitetaan toimitilojen fyysistä suojaamista, jonka tavoitteena on huolehtia yrityksen häiriötön toiminta. Sen pääasialliset suojattavat kohteet ovat paitsi toimitilat niin myös niissä sijaitsevat suojattavat kohteet. Lukitukset, kulunvalvonta sekä murtosuojaus ovat tyypillisiä toimitilaturvallisuuden keinoja. Niiden tavoitteena on estää vesi- sekä palovahinkoja, suojattavien kohteiden varastaminen, salassa tapahtuva televalvonta sekä asiattomien henkilöiden pääsy, yrityksen toimitiloihin. Toimitilaturvallisuuden suorittamiseksi valittaviin turvajärjestelyihin vaikuttavat olennaisesti esimerkiksi toimitilojen sijainti, kiinteistön aidat ja portit, valaistus kiinteistön alueella, rakennuksen fyysiset rakenteet, lukitus ja avainten hallinta kiinteistössä. Teknisiä ratkaisuja, jotka liittyvät olennaisesti osaksi toimitilaturvallisuutta ovat rikosilmoitinjärjestelmät sekä paloilmoitinjärjestelmät, videovalvontajärjestelmät sekä kulunvalvontajärjestelmät ja sammutusjärjestelmät, sekä savunpoistojärjestelmät. Yrityksen kaikki tilat eivät ole fyysisen turvallisuuden kannalta samanarvoisia. Tilat tulee siten luokitella turvallisuuden tarpeellisuuden perusteella, pääasiassa korkeampia suojauksia vaativat kohteet liittyvät yrityksen vahvuus alueisiin siten hyvä työkalu suojaustarpeiden suunnittelulle ja määrittelylle on toimitilojen tärkeysluokittelu. Tilojen merkitys tietoturvallisuuden näkökulmasta saadaan näin määriteltyä, jos luokittelua ei suoriteta vaarana on virhe arvioinnit, sekä resurssien hukkaaminen. (Laaksonen, Nevasalo ja Tomula 2006, 125.)

Yrityksen toimitilat voidaan jaotella esimerkiksi kolmeen osaan: ei-tärkeisiin, tärkeisiin ja erittäin tärkeisiin tiloihin. Näistä tyypillisiä esimerkkejä ovat ei tärkeistä alueista yrityksen piha-alue, sekä aula- ja odotustilat. Tärkeistä tiloista esimerkkejä ovat työhuoneet, avokonttorit ja valtaosa tuotantotiloista. Esimerkkejä erittäin tärkeistä tiloista ovat laitekehitystilat, tuotekehitystilat sekä johdon kokous- ja neuvottelutilat. (Miettinen, J. 1999, 178 – 179.)

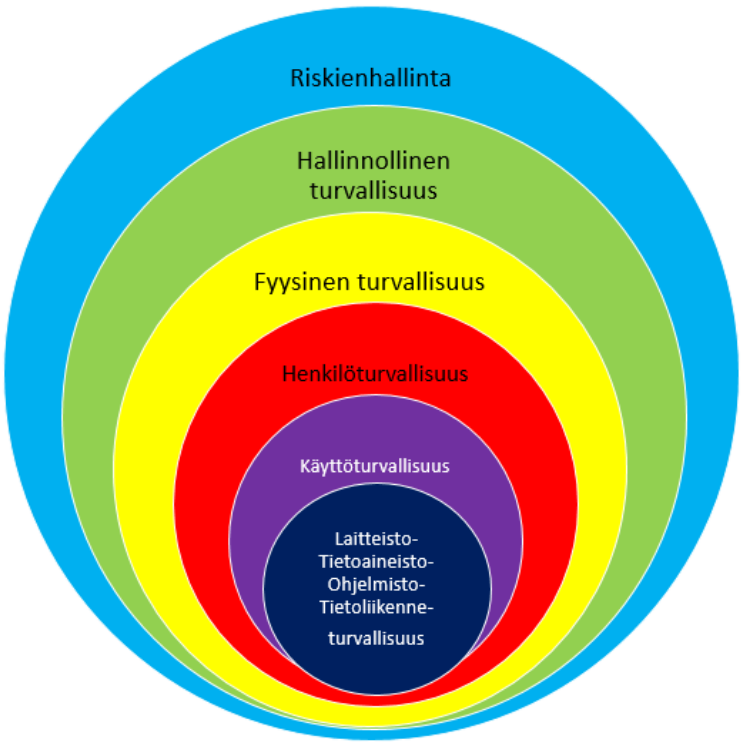
Merkittävimpiä tekijöitä toimitilaturvallisuudessa, on kiinteistön kulunhallinta ja siinä kulunvalvonta, joka koostuu erilaisista teknisistä menetelmistä. Niiden tarkoituksena on valvoa ja rajoittaa ihmisten liikkumista yrityksen kiinteistön alueella. Sen työkaluja ovat erilaiset mekaaniset ja sähköiset lukitukset. Mekaanisella lukituksella tarkoitetaan toimitilojen ovissa olevia lukkoja, mitkä toimivat mekaanisilla avaimilla. Sähköisiä lukituksia ovat esimerkiksi työntekijöiden avainkortit, joihin voidaan ohjelmoida henkilöille erilaisia kulkuoikeuksia. Sähköisillä lukituksilla on etuina joustava kulkuoikeuksien määritteleminen, sekä niiden kokonaan poistaminen ohjelmallisesti kulunvalvontajärjestelmästä erilaisissa katoamistapauksissa.(Miettinen 1999, 180.)

Yrityksen toimitiloissa voidaan videovalvonnalla seurata toimitilojen tapahtumia asennettujen videokameroiden avulla. Videovalvontaa tulee suorittaa 24 tuntia vuorokaudessa ja sen tulee olla tallentavaa videovalvontaa. Tallenteita tulee säilyttää riittävän pitkän aikaa parhaan tuloksen saamiseksi videovalvonnasta. Muistettavaa on, että sen olemassaolosta tulee löytyä selkeät merkinnät toimitiloissa ja voimassa oleva lainsäädäntö sen osalta kannattaa tarkistaa säännöllisin väliajoin. (Miettinen 1999, 181 – 182.)

Palosuojauksen avulla pyritään suojaamaan käytössä olevat tilat sekä siellä olevat suojattavat kohteet palovahinkoja vastaan. Paloturvallisuudesta huolehditaan Suomessa pääsääntöisesti hyvin johtuen kiinteistöjen teknisistä rakennemääräyksistä ja vakuutusyhtiöiden tiukoista paloturvallisuus vaatimuksista. Tärkeät, sekä erittäin tärkeät tilat on suojattava automaattisella paloilmoitinjärjestelmällä. Siihen kuuluu ilmaisimia, jotka tarkkailevat tilaa, sekä keskusyksikkö, joka tekee tarvittaessa palohälytyksen palolaitokselle tai vartiointiliikkeeseen. Erittäin tärkeät tilat tulee suojata lisäksi automaattisella sammutusjärjestelmällä, joka on alkaneen tulipalon sammutusjärjestelmä, joka suihkuttaa korkealla paineella vesijohtovettä, laitetiloissa sammutusaineena voidaan käyttää esimerkiksi tukahduttavia kaasuja. (Miettinen 1999, 182 – 184.)

4.5 Tietoturvallisuuden johtaminen

Tietoturvallisuuden osa-alueet on esitetty kuviossa 2.



Kuvio 2 Tietoturvallisuudenjohtamisen osa-alueet

Tietoturvallisuuden merkittävin osuus on riskienhallinta, sen avulla tavoitteena on suunnitella tulevaisuutta ja siten pienentää yritykseen vaikuttavien uhkien toteutumismahdollisuutta. Riskienhallinta toimii myös työkaluna, jolla kyetään havaitsemaan ja hallinnoimaan toimintaan kohdistuvia riskejä. Tavoitteena on pienentää riskejä hyväksyttävälle tasolle. Testaamalla tietojärjestelmien tietoturvallisuutta havaitaan tietoturvallisuusheikkouksia, voidaan arvioida suojaustoimenpiteiden tehokkuutta, sekä havaita mahdollisia puutteita tietojärjestelmän toiminnassa. (Krutz–Vines 2003, 16; Laaksonen ym. 2006, 150). Yrityksellä tulee olla määritelty tapa arvioida riskejä, sekä menetelmä tietoturvallisuuden testaamiseksi, riskien arviointi tulee ulottaa aina ulkoistettuihin palveluihin asti, näiden säännöllinen tarkistaminen, sekä testaaminen ja löydettyjen ongelmien korjauksen aikatauluttaminen, sekä korjauksien vastuuttaminen muodostavat tehokkaan riskienarviointikokonaisuuden. (SFS 27001 2006b.)

Tietoturvallisuuden hallinnointiin on luotu runsaasti erilaisia malleja, osa niistä käsittelee ainoastaan tietoturvallisuutta ja osa huomioi laajemmin liiketoiminnan kokonaisuuden. Malleissa esitetään tietoturvallisuuden kannalta keskeisiä osa-alueita, prosesseja ja kontrolleja. Laajemmassa käytössä olevia malleja hyödyntämällä voi yritys, sekä tietoturvallisuudesta vastaavat henkilöt olla varmoja ettei mikään tietoturvallisuuden kannalta oleellinen osa-alue, ole jäänyt huomioimatta suunnittelu vaiheessa. (Laaksonen, Nevasalo ja Tomula 2006, 91, 104.)

Tietoturvallisuuden johtaminen on kokonaisuutena hyvin laaja ja se on hyvä jakaa pienempiin osiin. Näin siitä saadaan helpommin käsiteltäviä osia, lisäksi pienemmistä osa-alueista laadittavista dokumenteista saadaan rakenteeltaan selkeämpiä. Näitä osa-alueita ovat hallinnollinen turvallisuus, fyysinen turvallisuus, henkilöturvallisuus, tietoaineistoturvallisuus, ohjelmistoturvallisuus, laitteistoturvallisuus, tietoliikenneturvallisuus. (Hakala, Vuorinen ja Vainio 2006, 10.) Hallinnollinen turvallisuus, fyysinen turvallisuus, sekä henkilöstöturvallisuus on jo käsitelty turvallisuusjohtamisen yhteydessä, tietoturvallisuuden johtamisen yhteydessä tuon vielä esiin tietoaineistoturvallisuuden, ohjelmistoturvallisuuden, laitteistoturvallisuuden, sekä tietoliikenneturvallisuuden osa-alueet.

4.5.1 Tietoturvallisuuspolitiikka

Tietoturvallisuuspolitiikan muodostaminen on yrityksen tai organisaation ylimmän johdon tehtävä, se laaditaan yleensä 5-10 vuoden tähtäimellä. Sen sisällön tulee olla paitsi käyttökelpoista tietojärjestelmien ylläpitäjille, sekä toimintaprosesseista vastaaville niin myös kirjoitettu siinä muodossa, että se on ymmärrettävissä ilman että on hallinnon tai tietotekniikan ammattihenkilö, lisäksi se on myös selkeä viesti ja osoitus organisaation sidosryhmille, että organisaatio pyrkii suojata paitsi omat niin myös sidosryhmien tiedot. Sen ollessa pääasiassa julkinen niin siihen ei tule sisällyttää sellaista tietoa, jota voi käyttää hyväksi tietomurroissa tai tietoverkkojen kautta tehtävissä hyökkäyksissä. Tietoturvapolitiikan julkisuudesta huolimatta sen tulisi olla sisällöltään laaja ja ottaa kantaa organisaation tietoturvakäytäntöihin ja olla ohjaava tekijä tietoturvallisuuden prosesseja suunniteltaessa. Tietoturvapolitiikka tehdään pitkälle aikavälille ja sitä tulisi tarkastella vuosittain. Näin varmistutaan siitä, että se vastaa organisaation turvallisuustarpeita sekä toimintaa. (Hakala, Vainio, Vuorinen 2006, 7 – 9.)

4.5.2 Tekninen tietoturvallisuus

Tietoturvallisuudesta puhuttaessa hyvin usein ajatellaan olevan tietokoneen virustentorjuntaa tai erilaisia palomuureja. Ne ovat kuitenkin vain pieniä osia tietoturvallisuudesta. Käytännössä tietoturvallisuus kattaa kaikki ne toimet tietojen säilyttämisessä, mitkä liittyvät saatavuuteen, oikeellisuuteen ja luottamuksellisuuteen. Tietoturvallisuuden tavoitteena on osa-alueiden ja niiden periaatteiden turvaaminen, esimerkiksi laitteiston vikaantumisen, sekä ohjelmistovikojen, aiheuttamilta uhilta ja vahingoilta. (Järvinen 2002, 20 - 21). Tietoturvallisuudella tarkoitetaan tietojen ja niitä tukevien järjestelmien suojaamista, sekä tietoliikenteen suojaamista. Tietoturvallisuuden tarkoituksena on lisäksi myös varmistaa kyseisiin asioihin kohdistuvien riskien hallintaa, teknisillä ja muilla toimenpiteillä. (Valtionvarainministeriö 2007.)

Tiivistettynä toimiva tietoturvallisuus on riskien ennakointia ja sovittujen tietojen suojaamista lain edellyttämällä tavalla. Tietoturvallisuuden ylläpitäminen on suunnitelmallista sekä jatkuvaa ja kehittyvää toimintaa. Tietoturvallisuuden periaatteet jaetaan pääasiassa kolmeen osa-alueeseen, joihin toiminnalla pyritään vaikuttamaan. Niitä ovat tiedon luottamuksellisuus, eheys sekä saatavuus. Tietoturvallisuus edellyttää lisäksi vielä kolmen muun periaatteen toteutumista, joita ovat todentaminen, pääsynvalvonta sekä kiistämättömyys. (Järvinen 2002, 22 – 28.)

4.5.3 Tietoturvallisuuden periaatteet

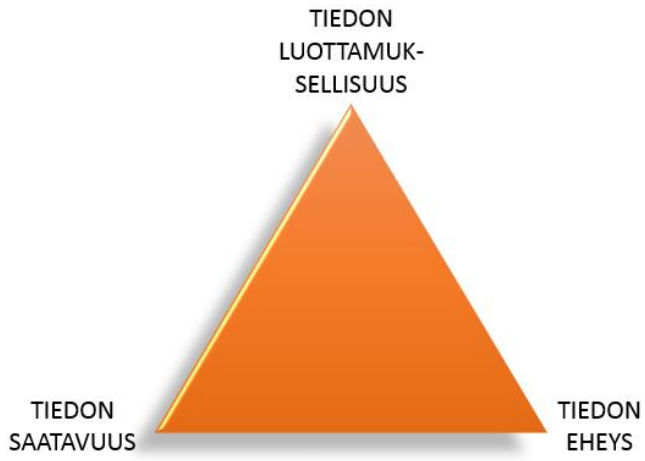
Luottamuksellisuudella tarkoitetaan, että henkilöille jaetaan ennalta määrätyt oikeudet järjestelmään. Tietoja pääsevät lukemaan, sekä muokkaamaan vain henkilöt, joilla on ennalta annettu oikeudet niihin. Tiedon luottamuksellisuus jaetaan organisaatioissa neljään luokkaan, joita ovat julkinen, sisäinen, luottamuksellinen ja salainen. Luottamuksellisuus korostuu erityisesti käsiteltäessä arkaluontoista tietoa, esimerkiksi henkilörekisteriä tai yrityksen taloudellisia asioita. Tiedot saattavat joutua myös vääriin käsiin, mikäli tietoverkkoon päästään sisälle murtautumalla, mistä syystä myös tietoverkot on suojattava asianmukaisesti. Mikäli tietoja pääsee käsittelemään henkilö, jolla ei ole tiedon käsittelemiseen oikeuksia, niin luottamuksellisuus vaarantuu välittömästi. Huomioitavaa on myös, että yrityksen henkilökunta on tietoinen tietojen luokittelemisesta. He ovat sitoutuneita sen edellyttämien käytäntöjen noudattamiseen, eivätkä siten luovuta tai saata luottamukselliseksi tai salaiseksi määriteltyä tietoa sellaiselle henkilölle tai taholle, jolla siihen ei ole annettu oikeutta. Tiedon luottamuksellisuus voidaan menettää, jos näin kuitenkin tapahtuu. (Hakala, Vainio ja Vuorinen 2006, 4; Järvinen, 2002, 22; Laaksonen, Nevasalo ja Tomula 2006, 157; Miettinen 1999, 25.)

Eheydellä tarkoitetaan sitä, että tietoja ei pääse luvatta muokkaamaan. Tietoja ei synny eikä häviä itsestään eikä näin tapahdu myöskään tietoihin oikeudettoman henkilön toiminnan kautta. Tietojärjestelmään murtautuminen voi aiheuttaa tietojen eheyden menettämisen. Samoin virukset rikkovat tiedostojen eheyden tarttuessaan niihin tai jos esimerkiksi kiintolevyt tai muut tallennusmediat vikaantuvat. Tiedon eheyden kannalta on tärkeää ottaa varmuuskopioita säännöllisesti ennalta sovitun protokollan mukaisesti tiedoista, jotka ovat yritykselle tärkeitä. Huomioitavaa varmuuskopioinnissa on, että niitä otetaan riittävän usein ja ne pidetään tallessa riittävän pitkän aikaa, koska tiedostossa oleva eheys vika saattaa olla hyvinkin vaikea ongelma. Jos vikaa ei huomata riittävän ajoissa, on mahdollista, että automaattinen varmuuskopiointi tallettaa vioittuneen tiedoston varmuuskopioksi. (Järvinen 2002, 22 – 23.)

Tiedon saatavuus, jota toisinaan kutsutaan myös käytettävyydeksi, tarkoittaa sitä, että tieto on saatavilla, kun siihen oikeutetut henkilöt tai erilaiset palvelut juuri sitä tietoa tarvitsevat.

Se voidaan mieltää ominaisuudeksi, jolla arvioidaan palvelun, laitteen, ohjelman tai järjestelmän saatavuuden varmuus niitä tarvittaessa. Saatavuus riippuu esimerkiksi luotettavuudesta, laitteiston määrästä, ohjelmistolisensseistä, tietoliikennekapasiteetista, käyttäjän omista toimista, erilaisten huolto- sekä tukitoimintojen tehokkuudesta. Näiden lisäksi sitä koskettaa laitteisto-, ohjelmisto-, sekä tietoliikennehäiriöt. Tiedon saatavuuteen liittyy hyvin merkittävästi tietojärjestelmien toimivuus. Kun jotakin tietoa on tarve käsitellä ja se on estynyt tietokoneiden tai verkkoyhteyksien toimimattomuuden vuoksi, on tiedon saatavuus uhattuna. Tiedon saatavuuden varmistamiseksi on monia erilaisia tekniikoita olemassa, joista tunnetuimpia ovat sähkökatkoksien varalta UPS-laitteet ja varmuuskopiointi, sen eri muodoissa. Tiedon saatavuus voidaan menettää paitsi tahallisen toiminnan vuoksi, niin myös tahattomasti. Tahallisesti saatavuutta voidaan häiritä esimerkiksi palvelunestohyökkäyksellä, jolla tukitaan organisaation tietoverkko ylimääräisellä liikenteellä. Verkon kaatuminen tai jonkin aktiivilaitteen hetkellinen vikaantuminen aiheuttaa hetkellisesti saatavuuden menetyksen. Inhimillisten virheiden vuoksi on mahdollisimman laajalti pyrittävä tiedon automaattiseen jalostamiseen. (Järvinen 2002, 24; Miettinen 1999, 28, Paavilainen 1998, 23; SFS 2006, 5.)

Kuviossa 3 on esitettyä tietoturvallisuuden kolme oleellisinta periaatetta.



Kuvio 3 Tietoturvallisuuden oleellisimmat periaatteet

Todentamisen periaatteella tarkoitetaan sitä, että tietoihin pääsevät käsiksi vain ne henkilöt, joilla siihen on oikeus, tällöin heidät pitää ensiksi jollakin tapaa todentaa. Tiedon suojaamiseksi muilta, tarvitaan tiedoille salausta. Tietojärjestelmässä käyttäjän todentamista käytetään todennusmenetelmänä. Käyttäjällä on salasana, joka todentaa tietojärjestelmälle, että hän on oikeutettu käyttämään tietoa tietojärjestelmässä. Todentamista varten on käytettävissä kolme tapaa, joita ovat yksilölliset ominaisuudet, esine sekä tieto. Yksilöllisiä ominaisuuksia ovat esimerkiksi käsiala, ääni tai ulkonäkö. Vain elävät henkilöt voidaan todentaa tällä menetelmällä. Tekniseen todentamiseen voidaan käyttää esimerkiksi sormenjälkeä

tai verkkokalvon tunnistusta, jolloin puhutaan biometrisestä tunnistamisesta. Salaustekniikoita käyttävissä tunnistusmenetelmissä käytetään esimerkiksi älykortteja, joihin tallennetaan henkilötiedot sekä käyttölupa, jota kutsutaan myös sertifikaatiksi. Se on voimassa vain ennalta määritellyn ajan. Ainoastaan hallussa olevaan esineeseen pohjautuva todentamismenetelmä on heikko tapa ja nitä kyetään usein helposti väärentämään. Kun esinettä käytetäänä todennuksessa, sitä kannattaa tehostaa käyttämällä vielä lisäksi jotakin toista todentamistapaa. Todennuksessa tiedolla tarkoitetaan sellaista tietoa, jonka tulisi olla vain käyttäjällä tiedossa. Näitä ovat esimerkiksi PIN-koodit puhelimissa ja pankkikorteissa sekä erilaiset salasanat. (Hakala, Vainio ja Vuorinen 2006, 7; Järvinen 2002, 24 - 27.)

Pääsynvalvonta varmistaa, että sisälle tietojärjestelmään pääsevät ainoastaan siihen oikeutetut, todennetut henkilöt. Olennaisesti siihen liittyy käytön seuranta sekä lokitiedostot. Lokitiedostoihin tallentuu tietoa käyttäjistä, esimerkiksi tiedostojen avauksista, sekä niiden muokkaamisesta. Niistä on merkittävästi apua, kun selvitetään tahallisesti tai tahattomasti tapahtunutta tietoturvallisuusrikkomusta. Tietojärjestelmien pääsynvalvonnalla pyritään estämään niiden luvatonta käyttämistä, joka saattaa altistaa tai edesauttaa erilaisten haittaohjelmien leviämistä, mikä edelleen voi johtaa tietojen eheyden sekä luottamuksellisuuden menettämiseen. Pääsynvalvonnassa kannattaa kiinnittää erityistä huomiota langattomiin verkkoihin, kuka niitä saa käyttää ja mikä on sallittua siellä erilaisille käyttäjäryhmille. (Hakala, Vainio ja Vuorinen 2006, 6; Järvinen 2002, 27.)

Kiistämättömyydellä tarkoitetaan ominaisuutta tietojärjestelmässä joka tunnistaa sekä tallentaa järjestelmää käyttävän henkilön tiedot. Pääasiallisesti siihen on kaksi syytä. Ensiksi halutaan varmistaa, keneltä tieto on peräisin ja toiseksi kuka tietoa käyttää. Tiedon käytön ollessa luvatonta on käyttäjän identiteetin tietämisellä suuri merkitys, etenkin jos tietojärjestelmän omistaja joutuu harkitsemaan oikeudellisia toimenpiteitä luvattomasti tietoa käyttänyttä kohtaan. Kiistämättömyyden varmistamiseksi on luotu runsaasti menetelmiä, joita on käsitelty todentamisen yhteydessä jo aiemmin. (Hakala, Vainio, Vuorinen 2006, 5.)

4.5.4 Tietoturvallisuuden johtamisen osa-alueet

Tietoaineistoturvallisuus on asiakirjojen, tiedostojen sekä erilaisten muiden tietovälineiden suojausta, turvaluokittelua sekä tietovälineiden hallitsemista, säilyttämistä, sekä käsittelyä asianmukaisesti, kaikissa tiedonkäsittelyprosessien ja tiedon eri vaiheissa. (Paavilainen 1998, 241.) Tietoaineistoturvallisuus tarkoittaa tietojärjestelmän tietojen suojausta erilaisissa tallennusmuodoissa. Sillä halutaan varmistaa, että tiedot pysyvät niillä henkilöillä, jotka ovat paitsi oikeutettuja tietojen käyttämiseen, niin myös tarvitsevat niitä päivittäisten työtehtäviensä suorittamiseen. Tietojen turvaluokitusjärjestelmä toimii perustana tietoaineistoturvallisuuden toteuttamiselle. (Miettinen 1999, 22-23.) Tietoaineistoturvallisuus koskee paperisia

asiakirjoja, optisia muistivälineitä sekä USB–muistivälineitä, äänitteitä sekä mahdollisia muita tallennusvälineitä. Tietoaineistoturvallisuus koskee koko tietoaineiston elinkaarta ja siitä vastaa koko yrityksen henkilöstö. Tietoaineiston elinkaareen kuuluu tietojen säilyminen, varmistaminen ja palauttaminen, sekä lopuksi tiedon tuhoaminen. Tietoaineistoturvallisuuden piiriin kuuluvat manuaalisen ja automaattisen tietojenkäsittelyn avulla tuotetut tulosteet. Tietohallinto ja organisaation arkistotoimi vastaavat tietoaineistoturvallisuudesta yhdessä. (Hakala, Vainio, Vuorinen 2006, 11; Valtiovarainministeriö 2014.)

Ohjelmistoturvallisuus käsittää tietojärjestelmissä käytettävien ohjelmistoihin liittyvät asiat. Näihin kuuluvat muun muassa lisenssien ja ohjelmistoversioiden hallinta. Jotkut mieltävät ohjelmistoturvallisuuden lähes merkityksettömäksi tietoturvallisuuden näkökannalta, kuitenkin jo pelkästään virustorjuntaohjelmiston lisenssin päättyminen voi aiheuttaa sen, että ohjelma lakkaa toimimasta ja altistaa koko tietojärjestelmän viruksille sekä haittaohjelmille. Järjestelmässä olevien ohjelmistojen tulee olla yhteensopivia lisättävien ohjelmistojen kanssa, sekä ohjelmistojen yleensä tulee olla käyttötarkoitukseensa sopivia. Välttyäkseen suuremmilta ongelmilta on hyvä varmistua ennen ohjelmiston päivittämistä tai uuden ohjelmistoversion asentamista, että ne toimivat. Virustorjuntaohjelmistot pyrkivät suojaamaan käyttäjän viruksilta sekä muilta haittaohjelmilta. Näihin haittaohjelmiin lukeutuvat madot, Troijan hevoset sekä vakoiluohjelmat. Nämä haittaohjelmat aiheuttavat ongelmia paitsi koneelle, johon ne ovat asentuneet, niin myös mahdollisesti tietojärjestelmälle sekä koko organisaatiolle. Tietoturva aukkoja käyttöjärjestelmissä hyväkseen käyttävät verkkomadot pyrkivät levittäytymään muihin verkossa oleviin koneisiin välittömästi järjestelmään päästyään. Siksi on tärkeää, että ylläpito seuraa virustilannetta maailmalla ja varmistaa, että virustorjunta ohjelmistojen tunnistetietokannat ovat ajan tasalla. (Miettinen 1999, 21; Järvinen 2006, 27, 29, 47.)

Organisaation ohjelmistoturvallisuuden tärkeimmät perussuojausmenetelmät ovat ohjelmiston pääsynvalvonta, tapahtumatietojen seuranta, varmuuskopiointi, asianmukainen ohjelmiston dokumentaatio, sekä asianmukaisesti laaditut ylläpito ja huoltosopimukset. Käytetyin suojaustekniikka on tietojen ja ohjelmien varmuuskopiointi. Niiden avulla varmistetaan mahdollisimman ajantasaisen version käytön varmistaminen, vaikka alkuperäiset tiedot vaurioituvat tai tuhoutuvat erilaisista syistä. Organisaation käyttämät ohjelmistot tulee dokumentoida tarkasti. Ohjelmistojen tulee olla laillisesti hankittuja ja ne on syytä rekisteröidä, koska rekisteröinti on usein vaatimuksena ohjelmistojen päivittämiselle. Lisäksi lisenssien ajantasaisuus ja ohjelmistojen häiriötön toiminta pystytään varmistamaan ohjelmistolisenssien hallinnalla. Tietokoneen ja ohjelmistojen epänormaaliin käyttämiseen sekä ilmoituksiin on kiinnitettävä huomiota aina. Tarvittaessa raportoitava ylläpidolle. Ohjelmistoturvallisuuteen voidaan vaikuttaa käyttämällä muita teknisiä turvakeinoja, esimerkiksi eriyttämällä tietoverkot toisistaan. (Miettinen 1999, 226 - 228; Valtionvarainministeriö 2007.)

Ohjelmistopolitiikan laatiminen organisaatiolle on yksi standardin ISO 27001 asettamia vaatimuksia ohjelmistoturvallisuudelle. Kielletyt, sekä sallitut ohjelmistot organisaatiossa tulee listata. Henkilöstön kouluttaminen on myös merkittävä tekijä ohjelmistoturvallisuudelle. Hhenkilöstöä tulee ohjeistaa kirjallisesti sekä suullisesti ohjelmistojen turvallisesta käyttämisestä, päivityksien asentamisesta ja arkaluonteisten tietojen salaamisesta. Standardissa edellytetään tekemään myös järjestelmien kuvaukset. Lisäksi on dokumentoitava mahdolliset ohjelmistoihin liittyvät tukisopimukset ja niihin liittyvät avunpyyntöperiaatteet. (SFS 27001 2006, 29–31.)

Laitteistoturvallisuuteen kuuluu kaikki organisaation käyttämät tietotekniset laitteet, sen tavoite on toimintojen jatkuminen, sekä omaisuuden häviämisen ja vahingoittumisen estäminen. Laitteistoturvallisuuteen kuuluu, että laitteistot ovat tarkoituksenmukaisiksi mitoitettu ja, toimivuus on testattu ja huoltotoiminnot, sekä varaosien hankinta on asianmukaisesti järjestetty, siihen kuuluu myös laitteiden käyttämisestä aiheutuvien vaaratekijöiden riskien arviointi ja riskien hallinnointi. Laitteistoon kohdistuu useita erilaisia riskejä, joihin organisaatiossa tulee varautua. Osa riskeistä kuuluu myös osaksi fyysistä turvallisuutta. Riskejä joihin tulee ainakin varautua, ovat vesi, tulipalo, savu, tärinä, pöly, lämpötila, sähköhäiriöt, erilaiset kemialliset vaikutukset, sekä tarvittaessa sähkömagneettinen säteily. Alkusammutuskalustoa tulee henkilökunnan osata käyttää ja se tulee olla käyttöympäristöön sopivaa, laitehuoneeseen hiilidioksidisammutin, ei jauhe tai nestesammuttimia. Huollon toiminta ennaltaehkäisevästi on hyvin merkityksellistä laitteiston käyttöiälle ja on myös tiedon saatavuuden ja eheyden kannalta tärkeää. Laitteistosta tulee pitää rekisteriä mistä saadaan selville laitteiden mallit, merkit, sarjanumerot sekä niiden sijoituspaikat, ongelmia selvitettäessä auttaa, kun laitteista on arkistoituna käyttöohjeet sekä muu olennainen siihen liittyvä dokumentaatio, joista esimerkkinä tekninen rakenne. Laitteiden elinkaaren lopussa on huolehdittava, että niissä olevat tiedot eivät joudu ulkopuolisten käsiin. Ne on hävitettävä hallitusti, organisaatiossa etukäteen sovitulla tavalla. (Hakala, Vainio, Vuorinen 2006, 12; Leppänen 2006, 300 - 301; Miettinen 1999, 221.)

Laitteistoturvallisuuden tavoitteena on estää omaisuudelle tapahtuvat vahingot, joita voivat olla omaisuuden häviäminen, vahingoittuminen tai varastaminen. Laiteturvallisuudesta huolehtimalla varmistetaan organisaation toiminnan jatkuminen. Laitteiden sijoittelulla sekä suojauksella, joilla pyritään torjumaan ympäristövaaroja ja luvattomien tunkeutumisen riskejä voidaan vaikuttaa laiteturvallisuuteen. Lisäksi laitteiden suojaaminen sähkökatkoksilta edesauttaa laiteturvallisuutta. Tietoliikennekaapelointi, sekä sähkökaapelointi tulee suojata fyysisiltä vaurioilta sekä salakuuntelulta. Ohjelmia, laitteita tai tietoaineistoja ei saa siirtää pois työpaikalta ilman siihen oikeuttavaa lupaa. Laitteiden matkakäytön sekä kotikäyttämisen edellytyksenä on, että niiden aiheuttamat riskit on huomioitu laitteistoturvallisuudessa. Myös

yrityksen ulkopuolella työskentelyn riskit on huomioitu sekä tarvittavat turvamekanismit ovat käytössä. (Hakala, Vainio, Vuorinen 2006, 308; SFS 27001 2006, 38.)

Tietoliikenneturvallisuuteen kuuluvat kaikki viestijärjestelmät, LAN- sekä WAN-yhteydet ja erilaiset muut mahdolliset tiedonsiirtoratkaisut. Sen tavoitteena on varmistaa tietoliikenteen häiriötön toiminta, sekä tiedon suojaus tiedon käsittelemisen, varastoinnin, sekä siirron aikana paitsi omassa, niin myös yleisissä verkoissa organisaatiossa. Tietoliikenneturvallisuuden suunnittelemisessa on otettava huomioon, paitsi verkon, sekä kapasiteetin riittävyys niin myös palvelunestohyökkäysten, sekä tietomurtojen torjunta. Tietoverkon kapasiteetin käyttämisessä on usein piikkejä, tällöinkin tarpeellisten tietojen on oltava saatavilla. Erilaiset laitteistossa tai ohjelmistossa ilmenevät viat voivat aiheuttaa verkon ruuhkautumista tai estää verkon toiminnan. Myös ruuhkahuiput voivat ylikuormittaa verkon. Ruuhkautumisia voidaan ehkäistä suunnittelemalla ja mitoittamalla verkon tiedonsiirtokapasiteetti riittävän suureksi. Tyypillisiä uhkia tietoliikenteelle ovat yhteyskatkot, tietovuodot, luvaton käyttäminen, eheysvirheet, sekä verkon käytön estyminen. (Paavilainen, J. 1998, 108 - 109, 115, 138.)

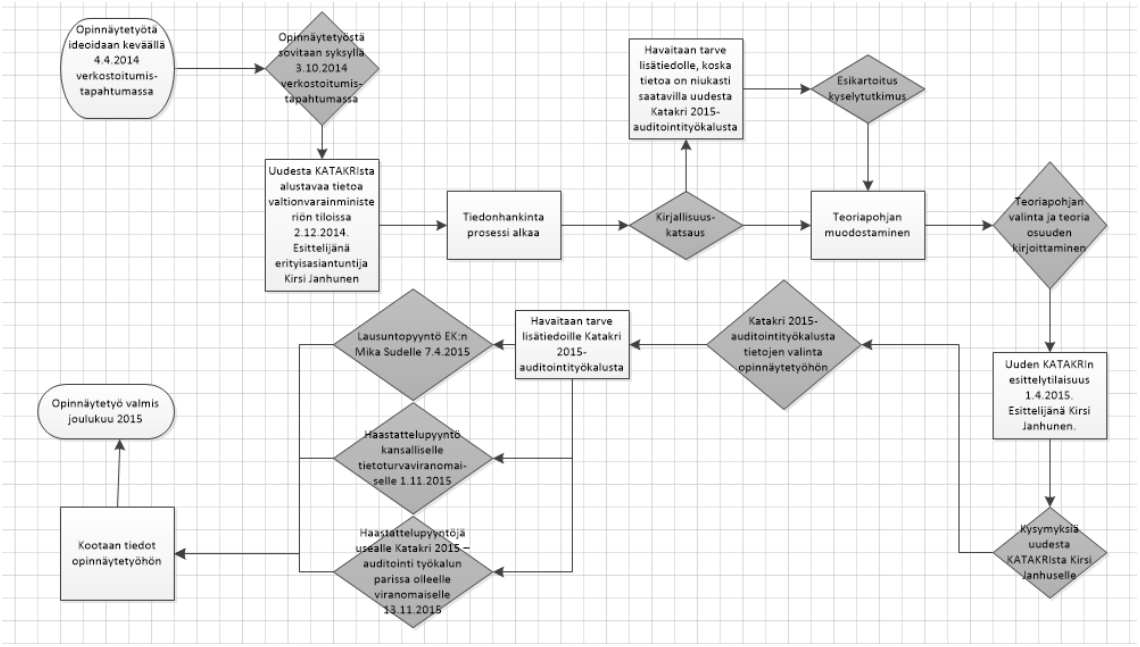
Palomuurilla mahdollistetaan verkossa olevat palvelut, sekä verkon käyttäminen organisaatiolle, siihen tulee tehdä tarvittavat määritykset verkonkäyttöpolitiikan mukaisesti, hyvin määritellyllä palomuurilla voidaan jopa estää palvelunestohyökkäykset, tämä puolestaan varmistaa osaltaan verkon käytettävyyden. Yrityksen sisäverkon ja ulkoverkon tulisi olla yhtä hyvin suojattuja. Jos ulkoverkosta löytyy heikko kohta ja sisäverkossa ei ole suojausta, pääsee yrityksen luottamuksellisiin tietoihin helposti käsiksi. Sisäverkko tulee suunnitella niin, että vain käyttäjät, joilla on oikeus, pääsevät tietoihin käsiksi. (Järvinen, P. 2006, 105 - 107; Leppänen 2006, 296 - 297.)

Etäkäyttäjien, internet-/intranet -käyttäjien sekä ekstranet -käyttäjien liittymisellä organisaation hallinnoimaan verkkoon mahdollistetaan etäkäyttötekniikoilla, tietojen luottamuksellisuus, saatavuus sekä eheys. Näiden tekniikoiden hallinta sekä toimivuus ovat keskeinen osa tietoliikenneturvallisuutta. (Krutz–Vines 2003, 118.)

Tietoliikenneturvallisuuden hallinnassa tavoitteena on verkossa kulkevan tiedon ja tukena olevan verkon rakenteen suojauksen varmistaminen. Tarvittava verkkojen hallitseminen sekä valvonta edesauttavat uhilta suojautumisessa. Lisäksi sillä varmistetaan verkkoa käyttävien sovellusten ja järjestelmien sekä niissä liikkuvan tiedon turvallisuus. Sisäisten ja ulkoistenverkkopalvelujen turvaaminen on osa tietoliikenneturvallisuutta. Turvallisuusominaisuuksien ja palvelutason yksilöinti sekä niiden sisällyttäminen verkkopalvelusopimuksiin on tärkeää. (SFS 27001 2006, 42.)

5 Opinnäytetyön toteutus

Opinnäytetyö lähti liikkeelle ideoinnista keväällä 2014 ja kunnolla se sai tuulta alleen Laurean alumnien verkostoitumistilaisuudessa syksyllä 2014, mistä prosessi lähti etenemään Janhusen esiteltyä Katakri 2015 valtiovarainministeriössä. Opinnäytetyön toteutus on esitetty kuviossa 4.



Kuvio 4 Opinnäytetyöprosessi

Opinnäytetyö eteni pitkän aikajakson aikana, mutta edeten kuitenkin koko ajan. Opinnäytetyö valmistui joulukuussa 2015.

Päädyin muodostamaan tästä aiheesta Laurean Alumnien verkostoitumistilaisuuksien kautta, joissa etsin mielenkiintoista opinnäytetyöaihetta. Tilaisuuksia on lähdetty järjestämään, jotta alalla toisten tunteminen paranisi ja ne tarjoaisivat tilaisuuksia verkostoitua, sekä löytää työharjoittelupaikkoja, opinnäytetyöaiheita ja töitä. Keskustelimme aiheesta Kirsi Janhusen kanssa jo aiemmassa tilaisuudessa keväällä 2014, mutta Lokakuussa 2014 pääsimme kunnolla keskustelemaan aiheesta ja siitä miten siitä saisi työstettyä opinnäytetyön, siitä lähti opinnäytetyö prosessi liikkeelle aiheena uudistettu Katakri 2015 – Tietoturvallisuuden auditointikriteeristö viranomaisille.

Lähdin ensin keräämään kirjallista, sekä sähköistä materiaalia turvallisuusjohtamisesta ja siihen liittyvistä osa-alueista, Katakrista, lainsäädännöstä, sekä aiemmin tehdyistä opinnäytetöistä. Uuden Katakrin sen hetkinen tilanne esiteltiin Kirsi Janhusen toimesta joulukuussa

2014. Näiden pohjalta lähdin tutkimaan asiaa syvällisemmin sekä loin esikartoituksena toimivasta haastattelusta kyselyn kysymykset. Kysymysten luonnin jälkeen tein survey-monkey kyselyohjelmistolla kyselylomakkeen, jonka suuntasin Katakrin ja/tai turvallisuusasiantuntijoille vastattavaksi. Näistä lähtökohdista kirjoitin teoriapohjan opinnäytetyöhöni, sekä muodostin työhöni rakenteen ja työstin tutkimuskysymystäni edelleen.

Pienen tauon jälkeen pääsin kirjoittamaan opinnäytetyötäni edelleen maaliskuun lopussa 2015 kun uusi Katakri 2015 – auditointityökalu alkoi olla valmis ja pääsin siihen tutustumaan, sekä se esiteltiin minulle valtioministeriön tiloissa Katakri - ohjausryhmän erityisasiantuntija Kirsi Janhusen toimesta, samassa tilaisuudessa tuli vastauksia käymissämme keskusteluissa esikartoitus haastattelututkimuksessa esiin tulleisiin aiempien Katakri - versioiden sekä uuden Katakrin vahvuuksiin ja kehityskohteisiin, esikartoitus kysely tutkimuksessa jo esiin tulleita toiveita uudelle Katakrille käytiin lyhyesti läpi ja pohdittiin niiden onnistumista. Tästä lähdin työstämään opinnäytetyöni osuutta uudesta Katakrista, sekä toiminnallisen opinnäytetyöni pohjalta muodostettavaa opasta uuteen Katakriin.

Opinnäytetyöprosessin edetessä keväällä 2015 tuli eteen tarve työstää lisää teoriaa osaksi opinnäytetyötäni ja täydensin teoriaosuutta. Keväällä myös pyysin lausuntoa Elinkeinoelämän keskusliiton Sudelta, joka oli osallistunut uuden Katakrin. Edelleen lisäteorialle havaitsin tarvetta. Marraskuun 2015 aikana sain haastattelupyyntöihini vastauksia, joista saadut tiedot muuttivat opinnäytetyön tuloksia merkittävästi.

5.1 Miten opinnäytetyö on toteutettu

Opinnäytetyöni alun ideointivaiheessa aloitin aineiston keräämisen systemaattisella tiedonhaualla turvallisuusjohtamisesta, Katakrista ja kansallisen turvallisuuden auditointikriteeristöstä. Aloitin hakujen tekemisen kirjaston Laurus-tietokannasta, sekä Theseus-opinnäytetyö tietokannasta. Jatkoin hakujen tekemistä muun muassa google scholarista sekä käytin löytyneiden aineistojen lähteitä. Tutkin myös, mitä Suomen laki sanoo turvallisuuden johtamisesta. Samoin etsin tietoa turvallisuutta käsitteleviltä tunnetuilta verkkosivuilta, kuten työsuojeluhallintosta, Finanssialan Keskusliitosta, pankeista, vakuutuslaitoksista, sisäministeriöstä, ulkoministeriöstä, puolustusministeriöstä, Suojelupoliisista, valtiovarainministeriöstä sekä eduskunnasta. Tutustuin myös opinnäytetöihin, joita oli tuotettu turvallisuusjohtamisesta tai Katakrista.

Opinnäytetyön materiaalit valitsin turvallisuuden johtamista ja sen osa-alueita käsittelevistä teoksista sekä Katakria eri näkökulmista käsittelevistä teoksista. Löydetyn materiaalin otsikon tuli jollakin tavalla liittyä opinnäytetyöhön ja tiivistelmistä tuli löytyä tietoa, joka liittyi suoraan opinnäytetyöhöni. Näistä luin aineiston kokonaan läpi ja valikoin teoriaosuuteen mukaan

materiaalia, jotka käsittelivät turvallisuusjohtamista hyvinkin eri näkökulmista. Uudesta Katakrista tietoa oli hyvin niukasti tarjolla, joten keskityin alkuvaiheessa Katakrin aiempiin versioihin. Myöhemmässä vaiheessa, kun materiaalia tuli tarjolle uudesta Katakrista, suuntasin materiaalitarkasteluni siihen suuntaan. Esikartoituksena toimivassa kyselytutkimuksessa esiin tulleet asiat auttoivat osaltaan suuntaamaan ja rajaamaan opinnäytetyöni käsittelyaluetta. Tutkimuskysymys ohjasi aineiston valinnassa sekä aineiston analyysissä.

Opinnäytetyössä tuodaan esiin kirjallisuuskatsauksessa, sekä esikartoituskyselyn kautta Katakri toisen version kehityskohteita, sekä vahvuuksia, tuon myös esiin odotuksia, joita näiden pohjalta ilmeni koskien Katakri 2015 - versiota samoin myös mitä odotuksia yleensä Katakrille jatkossa on. Opinnäytetyössä käydään Katakri ja sen aiempi Katakri toinen versio lyhyesti läpi ja opinnäytetyön pääpaino on Katakri 2015 - auditointityökalun muutoksissa, sekä syissä muutosten taustalla.

Esikartoituskyselyyn osallistunut joukko ei edusta koko Suomen turvallisuusalan asiantuntijoita taikka Katakrin asiantuntijoita, mutta ovat hyvin heitä edustava otos ja tiedonkeruullisiin tarpeisiin peilaten riittävä. Tiedonkeruudellinen tarve oli saada kuva asiantuntijoiden näkemyksistä Katakri II -version, sekä uudistettavan Katakrin vahvuuksista, sekä kehityskohteista. Tietoja käytettiin opinnäytetyön eri vaiheissa tarkastellessa uutta Katakria, sekä siihen liittyvissä keskustelutilaisuuksissa.

Muodostaakseni työni minun täytyy tutustua aiempiin opinnäytetöihin, kirjallisuuteen, sekä sähköisiin lähteisiin koskien turvallisuusjohtamista, Katakria, sekä niihin olennaisesti liitettävään keskeiseen käsitteistöön. Näiden pohjalta punnitsen itse tutkimustehtävää sekä valittavaa näkökulmaa ja tutkimuksen rajausta. Aineiston kerääminen, sekä valmistelu, aineiston pelkistäminen, aineistossa toistuvien rakenteiden tunnistaminen, kriittinen tarkastelu, tulkinta ja ulottuvuuksien luominen. Aineiston arvioimista tulee jatkaa koko tutkimus-prosessin ajan. (Hirsjärvi ym. 2009, 105.) Ojasalo ym. (2010, 34-35) nimittävät kirjallisuuskatsausta myös nimellä tietoperustan muodostaminen, koska tämä kokoaa olemassa olevan tiedon yhteen muodostaen käsitejärjestelmän jolla tutkittavat käsitteet ja näiden suhteet tulevat määritellyksi. Tietoperusta on tavoitteellinen ajattelumalli jossa kuvataan teoriat, mallit ja tutkimustulokset, sekä ohjataan uuden tiedon löytämistä systematisoimalla tutkittavaa ilmiötä. Näiden joukosta rakentuvat teoriat ja mallit joilla aihealuetta kuvataan rakennuspalikoiden ja käsitekartan avulla.

5.2 Esikartoitus kyselytutkimus

Kyselytutkimus tehtiin kahdessa osassa joista ensimmäisessä osassa suoritin esikartoitusta Katakrin toisen version vahvuuksista, sekä siinä mahdollisesti olevista kehityskohteista. Toinen

osa kyselytutkimuksessa koostui mahdollisesta uuden Katakrin tuntemisesta ja siinä olevien vahvuuksien ja kehityskohteiden esiintuomisesta. Esikartoitus tutkimus tehtiin Surveymonkey - ohjelmalla ja kysely suunnattiin lähettämällä joko saate kirje linkin kera suoraan sähköpostiin tai asettamalle se tarjolle kahteen suljettuun asiantuntijaryhmään Linkedinissä, toinen rymistä oli Laureassa turvallisuutta, muodossa tai toisessa opiskelevien tai opiskelleiden verkostoitumisen, sekä asiantuntija ryhmä ja toinen oli turvallisuuden johtajille, tutkijoille, sekä asiantuntijoille suunnattu ryhmä. Myös Linkedinissä oli sama saate kirje ja sen lopussa linkki kyselyn suorittamiseksi.

Näiden lisäksi kyselyssä oli asiantuntijuudesta kertovia taustatieto kysymyksiä. Näitä olivat koulutustaso, työkokemus turvallisuusalalta, sekä onko henkilö hyödyntänyt Katakria jossakin tarkoituksessa. Asetin kyselyyn vastanneiden asiantuntijuuden rajaksi joko Katakrin hyödyntämisen tai vähintään 6 vuoden kokemuksen turvallisuusalalta. Näiden lisäksi koko kysely oli täytynyt tehdä loppuun asti, keskeneräisiä vastauksia en huomioinut. Nämä kriteerit täyttäneitä vastauksia tuli 33 kappaletta, kaiken kaikkiaan vastauksia tuli 61 kappaletta.

5.3 Keskustelut, lausunnot, haastattelut

Uuden Katakri 2015 - projektin eteneminen esiteltiin Kirsi Janhusen toimesta 2.12.2014. Tilaisuudessa pääsin kuulemaan ja keskustelemaan minne uusi Katakri oli menossa, sekä käytiin keskustelua siihen sillä hetkellä tehdyistä ratkaisuista.

Uuden Katakrin esittelytilaisuus Valtioministeriön tiloissa 1.4.2015. Uuden Katakrin esittelijänä toimi Kirsi Janhunen, joka toimi uuden Katarin ohjaustyöryhmässä erityisasiantuntijana ja myös minun kontaktinani opinnäytetyötäni varten. Hänen kanssa kävimme runsaasti keskustelua vanhasta, sekä uudesta Katarista, samoin asioista joita tuotiin tekemässäni esikartoitus haastattelututkimuksessa esiin. Lisäksi keskustelutilaisuudessa tuli esille mitä erilaisia näkökulmia oli prosessin aikana tullut esiin ja että runsaasti kompromisseja oli jouduttu tekemään. Yksi näkökulma joka liittyi paitsi opinnäytetyöhöni niin myös teoria osuuteen, oli Elinkeinoelämän Keskusliiton Mika Suden näkemys Katakrista tietynlaisena turvallisuuden käsikirjana, joka ei toteutunut uuden Katakrin yhteydessä.

Lähetin Sudelle 9.4.2015 lausuntopyynnön hänen näkemyksistään Katakri 2015 - auditoitityökalusta, sekä siitä pois jääneestä näkökulmasta. 13.4.2015 sain häneltä sähköpostiin kirjallisen vastineen asiasta ja olen sen tiimoilta kirjoittanut sen sisältöä ja näkemyksiä opinnätetyötäni koskeviin tuloksiin.

12.11.2015 haastattelin kansallisen tietoturvallisuusviranomaisen erityisasiantuntijaa koskien Katakri 2015 – auditointityökalua. 13.11.2015 sain vastauksen laatimiini kysymyksiin koskien

uutta Katakri 2015 – auditointityökalua tietohallintojohtajalta sisäministeriöstä. 16.11.2015 sain vastauksen laatimiini kysymyksiin koskien uutta Katakri 2015 – auditointityökalua yksikön päälliköltä valtiovarainministeriöstä. 18.11.2015 sain vastauksen laatimiini kysymyksiin koskien uutta Katakri 2015 – auditointityökalua, Katakri 2015 – auditointityökalun viimeistelytyöryhmän jäseneltä poliisihallituksesta. 23.11.2015 sain vastauksen laatimiini kysymyksiin koskien uutta Katakri 2015 – auditointityökalua kansallisen turvallisuusviranomaisen päällikön sijaiselta ulkoministeriöstä.

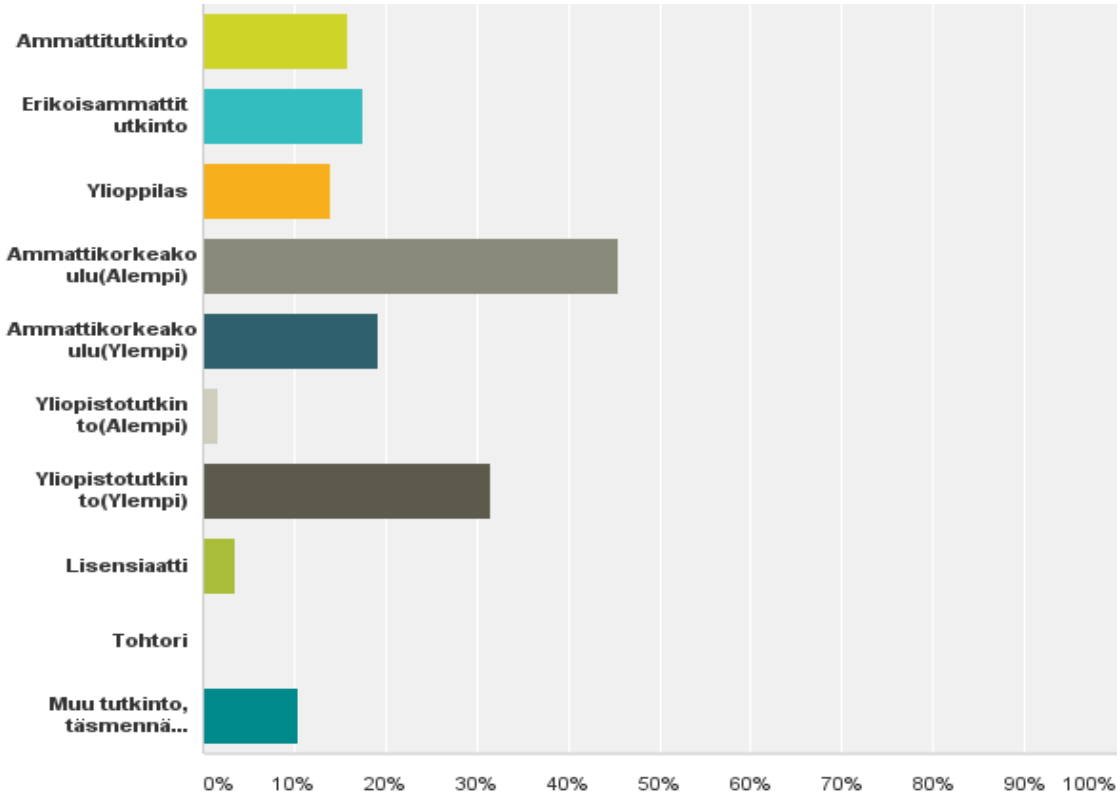
6 Opinnäytetyön tulokset

Tässä luvussa käsitellään opinnäytetyön prosessin aikana saatuja tuloksia. Opinnäytetyötä varten pyydettiin lausuntoja, käytiin keskusteluja ja tehtiin esikartoituksena kyselytutkimus, jossa aiheena olivat Katakrin aiemmat versiot, sekä tärkeimpänä Katakri 2015 – auditointityökalu.

6.1 Kyselytutkimuksen tulokset

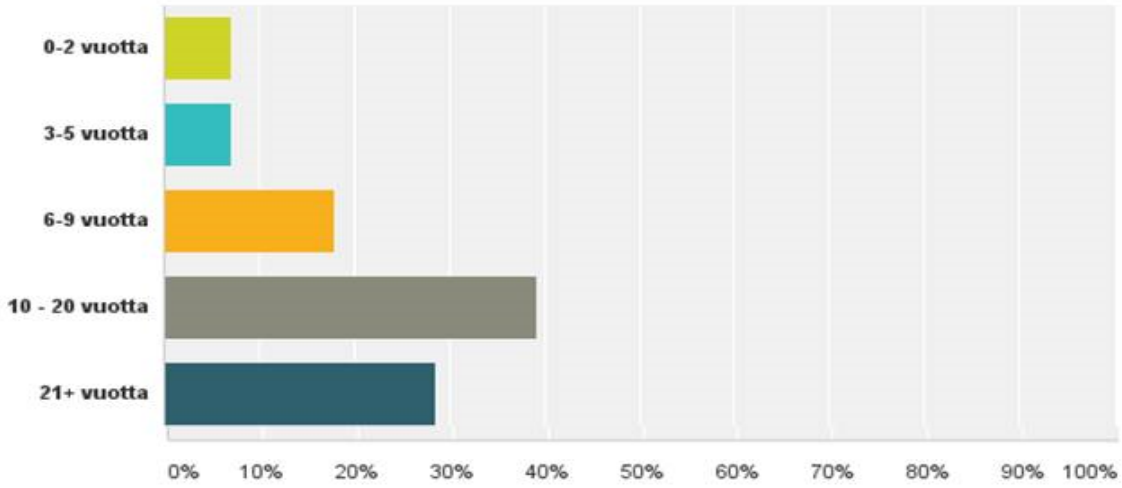
Esikartoituksena tehtiin kyselytutkimus, johon vastasi 61 vastaajaa. Heistä 32 täytti ennaltaasetetut kriteerit.

Kuviossa 5. Esiintetään kaikkien vastanneiden koulutuksellinen tausta.



Kuvio 5. Kyselytutkimukseen vastanneiden koulutus

Kuviossa 6 esitetään vastanneiden työkokemus turvallisuusalalta.



Kuvio 6. Kyselytutkimukseen vastanneiden työkokemus turvallisuusalalta

Kyselyyn vastnneista 64 % oli käyttänyt Katakria auditointityökaluna. Tässä tuloksessa ei näy se, että osa kyselytutkimukseen osallistuneista oli opettanut Katakrin käyttämistä auditointi-työkaluna tai muuten opetuskäytössä.

Kyselyyn vastanneista 80 % oli päässyt jollakin tavalla tutustumaan Katakri 2015 – auditointi-työkaluun, kun sen valmisteluprosessi oli kesken.

6.1.1 Katakri II vahvuudet

Tulosten mukaan Katakrin toisessa version vahvuudet ovat sen käytännönläheisyys sekä joustavuus verrattuna KatakrIn ensimmäiseen versioon. Katakri toisen version selkeyttä arvostettiin taulukkomuotoisuuden, esitystavan, arviointikokonaisuuksien, jaottelun sekä rakenteiden puolesta. Katakrin toisen version hyvinä ominaisuuksina pidettiin johdonmukaisuutta, hyvää jäsentelyä, samoin osa-alueiden yksityiskohtaisuutta sekä tulkinnanvaraisuuden vähyyttä. Täsmällisiä vaatimuksia osa-alueissa pidettiin hyvänä, kuten myös formaattisen mallin käyttämisen helppous tuli esille vahvuutena.

Katakri toisessa version osioista arvostettiin henkilöstöturvallisuutta sekä sen esityskaaviota. Lisäksi pidettiin hallinnollisesta osa-alueesta. Myös rakenteellisen turvallisuuden osiota kriittisen tiedon suojauksesta arvostettiin ja paloturvallisuuden mukaan ottamista pidettiin onnistuneena valintana.

Katakrin toisen version huomiokentissä olevia esimerkkejä sekä teknisluonteisia esimerkkejä pidettiin konkreettisempina, kuin muissa valtionhallinnon kriteeristöissä. Katakrin toisen version koettiin toimivan paremmin viitekehysten kanssa kuin ensimmäisen version, eikä se rajannut ulkopuolelle muita vaatimuksia. Sen ajateltiin huomioivan myös muita näkökulmia aiempaa paremmin. Viimeisenä sen tiiviyttä ja kokonaisuutta arvostettiin verrattuna VAHTIin tai ISO 27000-standardiperheeseen.

6.1.2 Katakri II kehityskohteet

Tulosten mukaan tietoturvaosiosta tulisi karsia liian suuri listaus teknologioista, ne tuovat esiin vain osan kaikista mahdollisuuksista, vaatimusten tarkempi kuvaus vain ja sen pohjalta etsittävä ratkaisuja. Tietoturvallisuusvaatimusten toistaminen eri kysymysosioissa, joilla tarkoitettiin samoihin kysymyksiin liittyviä kysymyksiä esimerkiksi henkilöstöturvallisuudessa, hallinnollisessa turvallisuudessa, sekä tietoturvallisuutta koskevissa osioissa. Koettiin, että Katakrin toisen version tulisi perustua riskienarviointiin ja skenaarioanalyysiin sekä kerättyihin luotettaviin tilastoihin ja empiiriseen tietoon, jotta kyetään arvioimaan täytetäänkö tietoturvaluokan III taso. Osa vaatimuksista miellettiin tarpeettomiksi.

Osioiden sisäisessä johdonmukaisuudessa löydettiin ongelmia. Samoin ongelmia havaittiin kysymysten keskinäisten sidonnaisuuksien yhteydessä. Niiden tarkat keskinäiset viittaukset olisi merkittävä selkeästi. Fyysistä turvallisuutta ei ollut tarpeeksi hyvin huomioitu.

Kriteeristöjen keskinäisessä yhtenevyydessä nähtiin ongelmia ja ristiriitoja VAHTI-ohjeiden ja Katakrin kesken. Kriteeristöt tulisi yhteensovittaa. Liikkumavaraa haluttiin vaatimusten toteuttamiseksi.

Katakri toisessa versiossa ei riskienhallintaa käytetty selvitystyön taustalla ja nyt tuotiin esiin käyttäjän velvollisuutta arvioida riskit. Myös arviointia olisi kehitettävä riskilähtöisempään suuntaan.

6.1.3 Katakri 2015 - auditointityökalun vahvuudet

Katakri 2015 - auditointityökalun nähtiin korjaavan riskienhallintaa koskevan tarpeen ja velvollisuuden, sen yhtenäisyyden koettiin parantuneen ja sen ajateltiin korjaavan aiempien versioiden virheet. Moduulirakenteita pidettiin hyvänä samoin tietoturvallisuuden olemista omana moduulina.

6.1.4 Katakri 2015 - auditointityökalun kehittämiskohteet

Katakri 2015 – auditointityökalu ei mielletty yhtä kattavaksi kuin Katakrin toista versiota. Katakri 2015 tietoturvallisuus ja turvallisuus ei ollut yhtä tiukkaa kuin Katakrin toisessa versiossa. Katakri 2015 - auditointityökalun vahvan viranomaislähteisyyden johdosta on vaara sen jäämisestä vain viranomaisnormistoksi, sille nähtiin myös jatkokehittämistarvetta yhteiskunnalliseksi työkaluksi. Vahvuutena ja kehittämistarpeena nähtiin Katakri 2015 – auditointityökalun tulkinnanvaraisuuden antama valinnan vapaus ja liikkumavara.

6.2 Kyselyt, keskustelut ja lausunnot

Tässä kohdassa tuon esiin kyselyissä, keskusteluissa sekä lausunnoista saatuja keskeisiä asioita Katakri 2015 – auditointityökalusta.

6.2.1 Katakri 2015 - auditointityökalu

Janhunen (2015) toi esiin sen, että ohjausryhmässä oli alussa hyvinkin erilaisia ajatuksia mitä Katakrin pitäisi olla nyt ja jatkossa. Kompromissiratkaisuna tuotettiin Katakri 2015 – auditointityökalu, joka toimii tietoturvallisuuden auditointityökaluna viranomaisille, Janhusen mielestä se vaatii edelleen ohjeistorakennetta tueksi, jotta sitä käytettäisiin tarkoitetulla tavalla. Katakrin käyttöä pohdittaessa osa näki, ettei kriteeristölle ei ole varsinaista tarvetta osa taas kaipasi täsmällisempää auditoijan vaatimuslistaa. Lisäksi toivottiin myös turvallisuuspäällikön näkökulmaa, missä Katakri 2015 – auditointityökalu olisi ollut eräänlainen käsikirja turvallisuudesta. Janhusen (2015) mukaan Katakri 2015 – auditointityökalu on tarkoitus pitää

suhteellisen pitkäaikaisena. Parin lähivuoden päivitykset olisivat pieniä. Katakri 2015 - auditointityökalusta on tulossa myös englanninkielinen versio arviolta 2015 vuoden lopussa.

Janhusen (2015) mukaan Katakri 2015 – auditointityökalu on tarkoitus pitää suhteellisen pitkäaikaisena. Parin lähivuoden päivitykset olisivat pieniä. Katakri 2015 - auditointityökalusta on tulossa myös englanninkielinen versio arviolta 2015 vuoden lopussa. Suden (2015) mukaan Katakri 2015 - auditointityökalun kokonaisuutta leimaa epäyhtenäisyys. Ongelmana on, että siinä sekoittuvat keskenään yleisen tiedon käsittelyn edellytykset ja paikoin yksityiskohtaiset suojausvaatimukset. Lähestymistapa toimii lähinnä vain tilaaja-tuottaja -mallissa, jossa tilaajan omistaman suojattavan tiedon määrä, luonne, käyttötarkoitus ja siihen kohdistuvat riskit ovat sekä tiedossa että arvioitavissa.

Susi (2015) kertoi, että yleisenä turvallisuuskäsikirjana Katakria ei nykymuodossaan ole kovin toimiva. Uuudistetun Katakrin kaltaiselle vaatimuslistalle taas on vaikea nähdä elinkeinoelämän kannalta merkittävää tarvetta, koska yksityiskohtainen vaatimuslista voi johtaa vain tehottomuuteen ja sulkea pois tarpeellisia kehittymismahdollisuuksia. Jotta uuden Katakrin kaltaiselle työkalulle olisi tarvetta, sen vaatimukset olisi vietävä huomattavasti yleisemmälle tasolle. Tällöin toteutus kykenisi ottamaan huomioon erilaisia ympäristöjä, sekä se olisi tehokasta. Nykymuodossaan Katakri 2015 - auditointityökalulla on vain rajalliset mahdollisuudet turvallisuuskäsikirjana toimimiseen. Se edellyttäisi koko rakenteen ja vaatimusperustan uudelleen muotoilua sekä riskienhallinnan todellista ymmärtämistä.

”Katakri on vain työkalu. Viranomaiset voisivat halutessaan käyttää mitä tahansa exceliä arviointinsa välineenä, mutta tällä viranomaisten yhdessä laatimalla työkalulla on ollut tarkoituksena yhdenmukaistaa arviointityötä. Arviointityökalun lisäksi on tärkeää, että arvioijat huolehtivat arviointiensa yhdenmukaisuudesta ja vertailtavuudesta.” (Yksikönpäällikkö, Valtiovarainministeriö 2015).

6.2.2 Miksi Katakri uudistettiin?

”Ensimmäinen Katakri –asiakirja laadittiin vuonna 2009. Toimintaympäristö ~~muutokset~~ sekä niiden asettamat vaatimukset toiminnalle olivat muuttuneet. Lähtökohtana Katakrin uudistamisessa on ollut käytettävyyden lisääminen, skaalautuvuus, riskiperusteisuus, vaatimusten läpinäkyvyyden parantaminen sekä osittaisten auditointien mahdollistaminen.” (Tietohallintojohtaja, Sisäministeriö 2015).

”(Katakrin kehittäminen) on pitkäjänteistä työtä niin kuin asiakirja versionumerokin osoittaa” (Tietohallintojohtaja, Sisäministeriö 2015). ”Alun perin oli tarkoitus SM:n johdolla vain päivittää arviointikriteerejä, mutta työn edetessä todettiin, ettei tuo uudistus ole riittävä, vaan on

syytä tavoitella kattavampaa uudistusta. Pyrittiin poistamaan aikaisempien Katakrien ja niiden virheellisen käytön aiheuttamia ongelmia.” (Yksikönpäällikkö, Valtiovarainministeriö 2015.)

”Aikaisemmissa Katakrin versioissa on pyritty tuottamaan arviointikriteeristön lisäksi eräänlainen yritysturvallisuuden käsikirja. Katakri 2015 - auditointityökalu selkeyttää ja tuo läpinäkyvyyttä siihen, että velvoittavat tietoturvavaatimukset tulevat lainsäädännöstä ja kansainvälisistä tietoturvavelvoitteista, ei tällaisesta arviointityökalusta. Aikaisemmin on harhaanjohtavasti puhuttu muun muassa ”Katakrin vaatimuksista”. Ei ole olemassa Katakrin vaatimuksia.” (Yksikönpäällikkö, Valtiovarainministeriö 2015).

”Lähtökohtana Katakrin uudistamisessa olivat käytettävyyden lisääminen, skaalautuvuus, riskiperusteisuus, vaatimusten läpinäkyvyyden parantaminen ja osittaisten auditointien mahdollistaminen. Koska uudistukset ovat mittavia, myös Katakrin rakenteeseen tehtiin muutoksia. Esitystavalla on pyritty korostamaan sitä, että edellytetty turvallisuuden taso voidaan toteuttaa usealla eri tavalla. Katakri 2015 itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Katakrissa esitettyjen vaatimusten yhteyteen on merkitty lähdeviittaus läpinäkyvyyden varmistamiseksi.” (Kansallisen turvallisuusviranomaisen päällikön sijainen, Ulkoministeriö 2015).

Aiemmissa Katakrin versioissa on koottu kaikki viranomaisvaatimukset yksiin kansiin. Katakri 2015 – auditointityökalussa lähdetään minimivaatimuksista, jotka tulee täyttää. Nämä kun täytetään niin pääsääntöisesti EU:n sekä NATO:n vaatimukset koskien organisaation kykyä suojata viranomaisen salassapidettävää tietoa luvattomalta käytöltä, sekä paljastumiselta täytetään. Huomioitavaa on, että Katakri 2015 – auditointityökalun käyttämisen yhteydessä kansainvälisessä kaupassa voit tulla yllätyksenä, että siellä onkin tiukemmat vaatimukset osassa maista kuin Katakri 2015 – auditointityökalussa. (Erityisasiantuntija, Kansallinen tietoturvallisuusviranomainen 2015).

6.2.3 Katakri 2015 - auditointityökalun käyttäminen ja käyttötarkoitus

Katakri 2015 – auditointityökalua käytetään kun viranomainen pyytää arvioimaan omia järjestelmiä käyttäen Katakri 2015 – auditointityökalua. Toinen käyttötarkoitus on FSC-prosessissa ja organisaatiot voivat käyttää sitä soveltaen oman turvallisuuden arviointiin. (Erityisasiantuntija, Kansallinen tietoturvallisuusviranomainen 2015).

Janhusen (2014, 2015) kanssa käymieni keskustelujen mukaan Katakri 2015 – auditointityökalu toimisi sen päätehtävässä, missä tärkeintä on suojata viranomaisen salassa pidettävää tietoa.

Sillä tarkoitetaan viranomaisen salassa pidettävän tiedon suojaamista paljastumiselta sekä viranomaisen salassa pidettävän tiedon suojaamista oikeudettomalta käytöltä.

”Katakria voidaan käyttää mm. yritysturvallisuusselvityksiin liittyvissä auditoinneissa. Jos yritysturvallisuusselvitys tehdään kansainvälisen tietoturvavelvoitteen perusteella, tulisi Katakria kuitenkin aina käyttää arviointiperusteena. Samoin asiakirjaa voidaan käyttää muussa viranomaisten tai yritysten tietoturvallisuustyössä, muuta ei sellaisenaan julkisen hankinnan turvallisuusvaatimuksena.” (Tietohallintojohtaja, Sisäministeriö 2015).

”Katakri on yksittäinen auditointityökalu, joka on tarkoitettu salassa pidettävän tiedon käsittelykyvyn arviointiin. Pääpaino on ollut yritysturvallisuustodistuksiin liittyvä arviointi, mutta tavoitteena on että Katakria voisi nyt hyödyntää myös valtionhallinnon arvioinneissa.”(Yksikönpäällikkö, Valtiovarainministeriö 2015).

Janhusen (2014, 2015) mukaan organisaatio voi käyttää Katakria käsikirjana oman toimintansa kehittämiseen. Samoin organisaatio voi arvioida, miten paljon sen toiminta eroaa Katakrin vaatimuksista. Tietoturvallisuuden kehittämisessä tulisi kuitenkin huomioida oman organisaation tarpeet. Ensin tulisi selvittää organisaation nykytilanne ja selvitetään mitkä ovat omat vaatimukset, sekä omat tarpeet tulevaisuudessa. Näiden selvittämisen jälkeen siirrytään suorittamaan riskienarviointia käyttäen esimerkiksi potentiaalisten ongelmien analyysiä, sekä mind mapping tekniikoita, jotta saataisiin selvitettyä missä organisaatiolla on kehittämistä edelleen, sekä missä ollaan jo joko halutulla tai riittävällä hallinta, sekä osaamisalueella. Osana tätä projektia vastuutetaan työt sekä asetetaan aikarajat kehittämistöille. Täytettyjen ja myöhemmin saavutettujen tavoitteiden, sekä vaatimusten tilaa seurataan säännöllisesti, sovitussa aikataulussa tai tarvittaessa aiemmin. Tietoturvallisuudenjohtaminen on jatkuvaa kehittämistä vaativa prosessi, jossa tavoitteena on viedä tietoturvallisuutta eteenpäin, toimintaympäristö muuttuu ja kehittyy jatkuvasti, joten paikoilleen ei voi jäädä. Tietoturvallisuudenjohtamisen kehittämisprojektityön saavutettua sille asetetut tavoitteet, voidaan lähteä käyttämään Katakri 2015 - auditointityökalua sille tarkoitetulla tavalla, työkaluna, välineenä jolla selvitetään täyttääkö organisaatio Katakri 2015 - auditointityökaluun vaatimuslähteissä esitetyt vaatimukset. Hyvänä oppaana tietoturvallisuuden johtamisen kehittämisprojektiin käy www.tietoturvatalkoot.fi sivuston kautta.

Omassa esikartoituskyselyssäni esiin tullutta ongelmaa Katakri 2015 - auditointityökalun vahvasta viranomaislähtöisyydestä on pyritty huomioimaan ottamalla jo suunnittelu vaiheessa muun muassa elinkeinoelämää mukaan. Katakri 2015 - auditointityökalua muodostettaessa toteutettiin myös kommenttikierros, missä oli mukana viranomaistahoja sekä elinkeinoelämää. Kommentointi on edelleen mahdollista. Susi (2015) toi kuitenkin esiin, että elinkeinoelämä oli

kriteeristön käyttötarkoituksen muutoksesta huolimatta edelleen mukana Katakrin uudistamistyössä ja tarjonnut kommentteja sekä osaamista ohjausryhmän ja alatyöryhmien käyttöön. Katakri 2015 - auditointityökalun käyttötarkoituksen muututtua elinkeinoelämän rooli on jäänyt aikaisempaa pienemmäksi. Elinkeinoelämän suositukset eivät ole enää mukana ja Katakri on nyt puhtaasti viranomaissääntelyyn perustuva auditointityökalu.

”Sisäministeriö on sisäisen turvallisuuden ja maahanmuuton ministeriö. Katakri 2015 on luonteva auditointityökalu meidänkin toiminnassa käytettäväksi.”(Tietohallintojohtaja, Sisäministeriö 2015).

”Katakria käytetään salassa pidettävän tiedon käsittelykyvyn viranomaisarviointiin. Katakria käytetään viranomaisen arvioidessa yrityksen turvallisuusjärjestelyjä yritysturvallisuusselvityksessä. Arviointikriteeristön käyttö tarkoituksiin, joihin sitä ei ole tarkoitettu ei ole järkevää. Katakria ei saa käyttää hankintojen turvallisuuskriteereinä.” (Yksikönpäällikkö, Valtiovarainministeriö 2015).

6.2.4 VAHTI ja Katakri 2015 – auditointityökalu

Janhunen (2015) kertoi VAHTI julkaisujen ja Katakri 2015 – auditointityökalujen rooleista jatkossa seuraavaSTI, VAHTI-ohjeiden rooli jatkossa olisi toimia uutta Katakria täydentävinä julkaisuina, missä asioita selvennettäisiin lisää tai syvemmin, sekä että se toisi esiin tärkeitä huomioita eri Kataria koskevista asioista. Tämä ratkaisu myös selventää uuden Katakrin ja VAHTIn rooleja joita koettiin päällekkäisiksi ja osin ristiriitaisiksi myös esikartoitus kyselyssäni.

”VAHTI –työssä on tehty iso määrä hyviä turvallisuuteen liittyviä asiakirjoja. KATAKRI III –asiakirjassa vaatimukset on kuvattu niin, että ne mahdollistavat erilaisia toteutustapoja. Vaatimusten yhteydessä oleviin lisätietokenttiin on kirjattu toteutustavoista esimerkkejä, jotka eivät kuitenkaan ole sitovia. Niissä kuvataan suosituksia ja parhaita käytäntöjä, joita löytyy muun muassa VAHTI-ohjeista.” (Tietohallintojohtaja, Sisäministeriö 2015).

”Katakri on yksittäinen auditointityökalu, joka on tarkoitettu salassa pidettävän tiedon käsittelykyvyn arviointiin. Pääpaino on ollut yritysturvallisuustodistuksiin liittyvä arviointi, mutta tavoitteena on että Katakria voisi nyt hyödyntää myös valtionhallinnon arvioinneissa. VAHTI eli Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä on valtionhallinnon tieto- ja kyberturvallisuuden yhteistyöelin, jossa ovat jäsenenä kaikki ministeriöt sekä keskeiset virastot. Suomen kyberturvallisuusstrategian mukaisesti VAHTI käsittelee keskeiset valtionhallinnon kyberturvallisuuden linjaukset. VAHTI toimii VM:n ohjaustoiminnan, kehittämisen ja yhteistyön

elimenä. VAHTIn alaisuudessa toimii jaostoja ja sen toimintamuotoja ovat kehittämishankkeet, koulutukset, ohjeiden ja linjausten laatiminen sekä julkaisu. VAHTIn toiminnassa on mukana tällä hetkellä noin sata henkilöä. Jos tarkoitat vain VM:n julkaisemia VAHTI-ohjeita, niin ne ovat eräs informaatio-ohjauksen muoto. Informaatio-ohjaus tarkoittaa ohjeita ja suosituksia verrattuna säädösohjaukseen, joka on velvoittavaa. VAHTI-ohjeista löytyy käytäntöjä ja toteuttamisohjeita, joiden avulla myös kuvattuja Katakri 2015 – auditointityökaluun koottuja vaatimuksia voidaan täyttää." (Yksikönpäällikkö, Valtiovarainministeriö 2015).

"Kun yritysturvallisuusselvitys tehdään kansainvälisen tietoturvallisuusvelvoitteen perusteella, arviointiperusteena on Suomea koskevat tietoturvallisuusvelvoitteet, joiden toteutumista arvioidaan Katakri 2015 –arviointityökalun avulla. Jos selvitys on tehty muun arviointiperusteen mukaisesti, selvityksen kattavuus arvioidaan ennen FSC-todistuksen myöntämistä ja tarvittaessa selvitystä täydennetään." (Kansallisen turvallisuusviranomaisen päällikön sijainen, Ulkoministeriö 2015).

6.2.5 Lisätietokenttien ja liitteiden rooli Katakri 2015 – auditointityökalussa

Janhunen (2015) kertoi, että ajatuksena olisi, että Katakri 2015 - auditointityökaluun itsessään ei puututtaisi, mutta lisätietokenttiin tuotaisiin tarvittaessa uutta tietoa sekä liitteitä voitaisiin lisätä tai muuttaa.

"Niissä on esimerkinomaisesti viittauksia hyviin käytänteisiin, mm. VAHTI - asiakirjoihin." (Tietohallintojohtaja, Sisäministeriö 2015).

"Lisätietokenttien tarkoituksena on ollut kuvata kriteerien toteutusesimerkkejä, ei ainoaa oikeaa tapaa kriteerin täyttämiseksi." (Yksikönpäällikkö, Valtiovarainministeriö 2015).

"Vaatimusten yhteydessä oleviin lisätietokenttiin on kirjattu esimerkkejä toteutustavoista, jotka eivät kuitenkaan ole sitovia. Niissä kuvataan suosituksia ja parhaita käytäntöjä, joita löytyy mm. vahti-ohjeista ja EU:n turvallisuussääntöjä täydentävistä suuntaviivoista ja ohjeasiakirjoista." (Kansallisen turvallisuusviranomaisen päällikön sijainen, Ulkoministeriö 2015).

Lisätietokentät avaavat vaatimuksia enemmän ja siellä on esimerkkejä toteuttamiseen. Lisätietokenttään on tulkinnan tueksi koottu toteutusesimerkkejä. Lisätietokentissä esitetyillä menettely tavoilla voidaan pääsääntöisesti ympäristöissä saavuttaa hyväksyttävä suojausten vähimmäistaso. Toteutusesimerkit voivat olla korvattavissa toisilla vastaavan tasoisilla suo-

jauksilla. Vaatimuksissa tai toteutusesimerkeissä ei kuvata tyhjentävästi ympäristöihin tai erikoistapauksiin riittäviä suojauksia. (Erityisasiantuntija, Kansallinen tietoturvallisuusviranomainen 2015).

6.2.6 Vaatimuslähteet Katakri 2015 - auditointityökalussa

Susi (2015) toi yritysten kannalta lähdenormistoon liittyvän mielenkiintoisen havainnon esiin valtionhallinnon tietoturvallisuudesta annetusta asetuksesta (681/2010) ja siihen liittyvän ohjeistuksesta käyttämisestä sellaisenaan markkinalähtöisestis toimivissa organisaatioissa. Tietoturva-asetus soveltamisohjeineen on laadittu ohjaamaan viranomaisten omaa tietoturvallisuus työtä. Tämän Katakri 2015 – auditointityökalu näyttää unohtavan. Tietoturva-asetuksen sääntely asettaa vaatimuksia ensisijaisesti tiedon omistajalle ja luovuttajalle, ei automaattisesti suoraan sen vastaanottajalle. Tietoturvavallisuusasetusta voisi pikemmin toimia suojaustavoitteena, jonka riittävään toteutumiseen voitaisiin päästä useilla erilaisilla keinoilla ympäristöstä riippuen. Sääntelyn soveltaminen uudessa Katakrissa velvoittavina vaatimuksina sellaisenaan yrityksissä on ongelmallista. Miksi yritykset haluttaisiin muuttaa viranomaisiksi ja olisiko se kovin järkevää? Kolmannen osapuolen tekemien auditointien yhteydessä vaatimusten suora velvoittavuus on hankalaa. Miten kolmas osapuoli esimerkiksi voisi arvioida riskejä tai hyväksyttävää jäännösriskiä tiedon omistajan puolesta?

Susi (2015) totesi, että on hyvä, että Katakria ei enää sovelleta varsinaisena arviointiperusteena, vaan vaatimukset pyritään johtamaan lähdenormistosta. Niiden soveltamisessa Katakrin vaatimusten perustana ei ole ongelmatonta. Katakri 2015 – auditointityökalussa on paikoin sotkettu lähdenormistoa ja tuotettu vaatimuskohtia, joiden sisältö ei enää vastaa alkuperäisiä normeja. Lopputuloksena on, että vaatimukset kytkeytyvät paikoitellen varsin löyhästi alkuperäisiin normilähteisiinsä, joten on ajoittain erittäin vaikea todentaa miten varsinainen vaatimus on muodostettu. Alkuperäislähteet olisi siksi ainakin epäselvissä tapauksissa syytä tarkistaa.

6.2.7 Riskienhallinta Katakri 2015 - auditointityökalussa

Suden (2015) mukaan vaatimusten ehdottomuuden poistuminen riskienhallinnasta on hyvä asia. Lähestymistapa nykymuotoisen Katakrin vaatimuksiin ei riskienhallinnan myötä voi enää olla: "täyttyy tai ei täyty". Riskienhallinta-ajattelu on siis tervetullut uudistus. Ongelmana on, että ymmärretäänkö riskienhallinta tässä tapauksessa oikein. Uuden Katakrin käyttötarkoituksen perusteella kyseessä on viranomaisten luokitellun tiedon suojaamiseen käytettävä työkalu. Kohdeyrityksen on kuitenkin mahdotonta tunnistaa viranomaisten tietoaineistoon kohdistuvia riskejä varsinaisen tiedon omistajan puolesta. Katakri 2015 – auditointityökalu jättää

käytännössä täysin auki, onko sen tarkoituksena arvioida yrityksen erilaisia riskienhallintamenetelmiä ja suojauskäytäntöjä, sekä niiden riittävyyttä ja kattavuutta vai tietoon itsessään kohdistuvia riskejä, jolloin tavoitteena olisi hallita niitä erilaisin keinoin. Tästä asiasta on edelleen epäselvyyttä jopa viranomaisten kesken. On jopa tuotu esiin kestämätön väite siitä, että riskienhallinta toimisi vain koventavana elementtinä esitetyille vaatimuksille. Väite veisi kuitenkin pohjan koko riskienhallinta-ajattelulta ja olisi melkoisessa ristiriidassa kaiken järkevän toiminnan kanssa. Onko Katakri 2015 – auditointityökalu, työkalu yrityksen yleisten salassa pidettävän tiedon käsittelyn edellytysten arviointiin vaiko riskien tunnistamista sekä arviointia hyödyntävä työkalu, jolla voitaisiin valita ja toteuttaa erilaisia suojaustoimia, jolloin nämä voitaisiin lopulta mitoittaa ainoastaan tunnistamalla riskejä? Näiden eri ulottuvuuksien toimiva yhdistäminen yhteen työkaluun on käytännössä hyvin vaikeaa ja se ristiriita paistaa läpi uudessa Katakrissa. Katakri 2015 – auditointityökalu soveltuu ainoastaan hyvin rajallisesti tiettyjen tilaaja-tuottaja - mallisten selkeästi rajattujen ja eriytettyjen hankkeiden auditoijan muistilistaksi, toteaa Susi (2015).

Janhunen (2014, 2015) toi lisäksi esiin, että on tärkeää huomioida, että riskilähtöisyys Katakri 2015 – auditointityökalun yhteydessä tarkoittaa, että on mahdollista valita turvajärjestelyitä riskien tarkastelunäkökulmasta. Se edellyttää kuitenkin hyvää organisaation lähtökohdista suoritettua riskienarviointia. Keskusteluissa tuli esiin myös painotettuna, että Katakri 2015 - auditointityökalua käytettäessä tulee ymmärtää, että vaatimusten lisätietokentät eivät ole velvoittavia, vaan niissä kerrotaan toteutusesimerkkejä, vaatimukset on mahdollista toteuttaa muillakin tavoilla. Katakri 2015 – auditointityökalu vaatii selvästi auditoijalta enemmän kuin aiemmat versiot.

”Korostaisin riskiperusteista arviointia ja sen näkymistä tässä versiossa. Turvallisuusjärjestelyjen suunnittelun ja toteutuksen avulla pyritään varmistamaan uhkiin nähden hyväksyttävä turvallisuustaso. Kohdeorganisaation tulee pystyä osoittamaan turvallisuusjärjestelyjen riittävyys luotettavasti. Turvallisuusjärjestelyjen riittävyyden arvioinnin tulee pohjautua järjestelmälliseen riskienarviointiin.” (Tietohallintojohtaja, Sisäministeriö 2015).

”Tässä se pihvi oikeastaan onkin. Kunkin tahon on arvioitava tätä asiaa omasta ydin/liiketoiminnastaan lähtien ja määriteltävä johdon hyväksymät jäännösriskit sekä suojautumiskeinot. Katakri III on siihen työhön liittyen oivallinen apuväline.” (Tietohallintojohtaja, Sisäministeriö 2015).

”Tavoitteena on ollut, ettei yksittäistä kriteeriä tarvitse täyttää tietyllä yhdellä ainoalla oikealla tavalla, vaan uhkiin nähden hyväksyttävän turvatason voi saavuttaa erilaisilla keinoilla. Tähän tarvitaan riskienhallinnan toimenpiteitä.” (Yksikönpäällikkö, Valtiovarainministeriö 2015).

Riskienarviointi on kaksivaiheinen, riskienarviointi lähtee liikkeelle kohdeympäristöön tehdystä organisaatiolähtöisestä riskienarvioinnista, toisessa vaiheessa viranomainen kartoittaa yleisiä uhkia esimerkiksi erilaisista tietoliikenneympäristöistä. Viranomainen omaa tieto-, sekä kokemuspohjaista osaamista joita hyödynnetään kartoitettaessa yleisiä uhkia. Näistä lähtökohdista voidaan tarvittaessa koventaa tai lieventää vaatimuksia. Osa vaatimuksista on kuitenkin luonteeltaan ehdottomia minimivaatimuksen osalta. (Erityisasiantuntija, Kansallinen tietoturvallisuusviranomainen 2015).

6.2.8 Turvallisuusjohtaminen Katakri 2015 - auditointityökalussa

Janhusen (2014) mukaan Katakri 2015 - auditointityökaluun on tarkoituksella jätetty turvallisuusjohtamisen-osioon mahdollisuus auki eri turvallisuustasojen määrittelemiselle. Siihen ei ole tarkoituksellisesti määritelty esimerkiksi turvallisuuden johtajalle koulutus-, kokemus- tai meriittivaatimuksia, vaan on kerrottu, mitä tulee hallita, osata ja tehdä. Tavoitteena tällä on ollut saavuttaa vaatimukset tarpeiden mukaan skaalautuviksi. Susi (2015) piti myös turvallisuusjohtamisen osa-aluetta onnistuneena. Katakri 2015 -auditointityökalussa aikaisempien A+P osuuksien yhdistäminen oli hänen mielestään perusteltua. Osa-alue ei myöskään perustu viranomaisten suojaustasoihin, vaan on yleinen kooste turvallisuusjohtamisen käytännöistä. Myös aiempien versioiden vaatimuskohtien päällekkäisyyksiä on onnistuttu vähentämään.

”Mielestäni turvallisuusjohtaminen on osa kokonaisjohtamista. Turvallisuusjohtamisen vaatimuksilla pyritään siihen, että organisaatiolla on toimiva turvallisuuden hallintajärjestelmä sekä riittävät menettelyt sen varmistamiseksi, että viranomaisen salassa pidettäviä tietoja käsittelevä henkilöstö toimii asianmukaisesti.” (Tietohallintojohtaja, Sisäministeriö 2015).

”Tiedon salassapidon varmistamiseen liittyy rakenteellisten ja teknisten näkökulmien lisäksi johtamisnäkökulma ja hallinnollisia toimenpiteitä. Kriteereissä on kuvattu myös tämä puoli.” (Yksikönpäällikkö, Valtiovarainministeriö 2015).

”Turvallisuusjohtamisen osio on yksi osio muiden joukossa, mutta se luo perustan muiden osioiden tarkastuksille.” (Kansallisen turvallisuusviranomaisen päällikön sijainen, Ulkoministeriö 2015).

Jos tämä ei ole kunnossa, mikään ei voi olla pidemmän päälle kunnossa. Rooli sinänsä ei eroa muista osioista. (Erityisasiantuntija, Kansallinen tietoturvallisuusviranomainen 2015).

6.2.9 Katakri 2015 – auditointityökalun vahvuudet

”Tässä kohtaa nostaisin esille kolme seikkaa: riskiperusteisuuden, selkeyden ja käytännöllisyyden.” (Tietohallintojohtaja, Sisäministeriö 2015).

”Onnistuneinta on ollut muutos kokonaisvaltaisempaan suuntaan yksittäisten kriteerien arvioinnista.” (Yksikönpäällikkö, Valtiovarainministeriö 2015).

Esitystapa sallii liikkumavaraa verrattuna aiempaan versioon. Oleelliseen keskittyminen, vaatimukset ovat perusteltuja, lähdetään liikkeelle todellisesta tarpeesta, rakenne on kevyempi. (Erityisasiantuntija, kansallinen tietoturvallisuusviranomainen 2015).

6.2.10 Katakri 2015 – auditointityökalun kehityskohteet

”Tätä on syytä arvioida säännöllisesti saadun palautteen perusteella. Ensimmäinen luonteva arviointiaika on mielestäni ensi vuoden aikana, kun tämä versio on ollut käytössä yli vuoden.” (Tietohallintojohtaja, Sisäministeriö 2015).

”Työkalua täytyy ylläpitää ja kehittää.” (Yksikönpäällikkö, Valtiovarainministeriö 2015).

Jatkossa olisi hyvä tuoda esiin miksi joitakin asioita vaaditaan, syyt näiden takana, tällä tavalla tuotettaisiin ymmärrystä vaatimusten tueksi, tapa tukisi myös riskienarviointia. (Kansallinen tietoturvallisuusviranomainen 2015).

Tulevaisuudessa voisi tuottaa esimerkkejä vaadittujen turvallisuustasojen tietoturvallisuus ympäristö kokonaisuuksista, niiden avulla saataisiin havainnollistettua selkeämmin kokonaiskuva, mitä vaaditaan tietoturvallisuudesta organisaatiolta. (Erityisasiantuntija, Kansallinen tietoturvallisuusviranomainen 2015).

6.3 Opinnäytetyön tuotos

Alla olevaan taulukkoon 6 olen koonnut merkittävimpiä eroavaisuuksia Katakrien eri versioissa.

Taulukko 1. Katakrien eroavaisuuksia

	KATAKRI I	KATAKRI II	KATAKRI 2015
Käyttötarkoitus	Viranomaisen työkaluna kohteen turvallisuustason auditointiin. Ja auttaa organisaatioita/viranomaisia sidosryhmien sisäisessä turvallisuustyössä.	Viranomaisen työkaluna kohteen turvallisuustason auditointiin. Ja auttaa organisaatioita/viranomaisia sidosryhmien sisäisessä turvallisuustyössä.	Tietoturvallisuuden auditointityökalu viranomaisille, jolla arvioidaan organisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Voidaan käyttää myös soveltaen apuna organisaation turvallisuuden kehitystyössä.
Rooli	Epäselvä. Tukeutuu lakeihin, asetuksiin ja standardeihin, mutta myös asettaa kriteerejä.	Epäselvä. Tukeutuu lakeihin, asetuksiin ja standardeihin, mutta myös asettaa kriteerejä.	Selkeä. Lait, normit ja asetukset ovat Katakrin yläpuolella, Katakri itsessään on ohje ja sen alapuolella on toiminta- sekä toteutustavat.
Tukeutuu	Valtionhallinnon tietoturvallisuusasetus, EU:n turvallisuus regulaation linjaukset, rinnakkaiset kriteeristöt valtiovarainministeriössä.	Valtionhallinnon tietoturvallisuusasetus, VAHTI, EU:n 2011 päivitetty turvallisuus-säännöstö. Varautumiseen, jatkuvuuden hallintaan, sekä huoltovarmuuteen keskittyvät kotimaiset ohjeet. Kansain-väliset standardit.	Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010), EU:n neuvoston turvallisuussääntöihin (2013/488/EU), sekä kansainväliset sopimuksiin.
Rakenne	Ei itsenäisiä kokonaisuuksia.	Ei itsenäisiä kokonaisuuksia.	Selkeästi eriytetty, modulaarinen.
Osa-alueet	Hallinnollinen turvallisuus ja turvallisuusjohtaminen(A) Henkilöturvallisuus(P) Fyysinen turvallisuus(F)	Hallinnollinen turvallisuus(A) Henkilöstöturvallisuus(P) Fyysinen turvallisuus(F) Tietoturvallisuus(I)	Turvallisuusjohtaminen (T) (A+P alueet yhdistetty) Fyysinen turvallisuus(F) Tekninen tietoturvallisuus(I)
Lisätietokentät	Tarkentaa ja selventää vaatimusta, sekä antaa toimintaohjeita.	Tarkentaa ja selventää vaatimusta.	Sisältävät toteutus esimerkkejä, sekä hyviä käytänteitä, ne eivät kuitenkaan ole velvoittavia.

Riskienarviointi	Riskienarviointi on osana kriteeristöä.	Riskienarviointi on osana kriteeristöä.	Vaatii kaksivaiheisen riskienarvioinnin. I vaiheessa kohdeympäristöön suoritettu organisaatiolähtöinen riskiarviointi. II vaiheessa viranomainen kartoittaa yleisiä uhkia hyödyntäen omaa tieto-, sekä kokemuspohjaista osaamista. Näistä lähtökohdista voidaan vaatimuksista osaa koventaa tai lieventää.
Vaatimukset/Kriteerit	Kriteerit ovat ehdottomia.	Kriteerit ovat ehdottomia.	Kriteereitä ei enää ole on vaatimuksia. Vaatimukset voidaan toteuttaa useilla eri tavoilla. Mahdollista myös vaadittavien turvajärjestelyiden valinta riskien näkökulmasta.
Auditointi	Joustamaton, ei osittaista auditointia.	Joustamaton, ei osittaista auditointia.	Joustava. Osittainen auditointi mahdollinen, kuitenkin turvallisuusjohtamisen osa-alue huomioitava auditoitaessa aina.
VAHTI	Rinnakkainen kriteeristö, suhde ristiriitainen.	Rinnakkainen kriteeristö, suhde ristiriitainen.	VAHTI-ohjeista löytyy käytäntöjä ja toteuttamisohjeita, joiden avulla myös Katakri 2015 – auditointityökaluun koottuja vaatimuksia voidaan täyttää. Katakri 2015 - auditointityökalua tulkitseva ja vaatimuslähteistä koottuja vaatimuksia selventävä väline.
Elinkeinoelämä	Elinkeinoelämän suositukset mukana.	Elinkeinoelämän suositukset mukana.	Ei sisällä elinkeinoelämän suosituksia. Elinkeinoelämä ollut kuitenkin mukana kehitystyössä.

7 Johtopäätökset ja oman työn arviointi

Katakri 2015 – auditointityökaluun vaatimuslähteistä koottuja vaatimuksia hyödyntämällä sekä sen osoittaminen virallisella auditoinnilla tarjoaa yrityksille mahdollisuuden osallistua kotimaisiin ja kansainvälisiin tarjouskilpailuihin sekä hankkeisiin, joissa käsitellään viranomaisen salassa pidettävää tietoa. Katakri 2015 – auditointityökaluun koottujen vaatimuksien hyväksytysti suoritettu auditointi on etenkin valtioiden välisissä hankkeissa usein vaatimuksena yhteistyön aloittamiselle. Kotimaisissa organisaatioissa Katakri 2015 – auditointityökaluun vaatimuslähteistä koottujen vaatimusten noudattaminen kokonaisuutena tai esimerkiksi tietoturvan osalta voi olla ehtona yhteistyölle sen eri muodoissa. Auditointiprosessin vieminen mahdollisimman pitkälle jo ennen viranomaisten hankkeisiin osallistumista ei viivästytä tarjouskilpailun kriteerien täyttöä ja siten estä tarjouskilpailuun tai itse hankkeeseen osallistumista. Auditointiprosessi vie aikaa ja resursseja sekä tietysti aiheuttaa myös kustannuksia. Auditointiin varautuminen on siksi syytä aloittaa hyvissä ajoin suorittamalla sisäinen auditointi. Mahdollisesti tehdään myös ulkoinen auditointi ennen kuin se suoritetaan virallisesti määrätyn turvallisuusviranomaisen toimesta.

Ristiriitaisuuksia, joita tuli esiin esikartoituskyselyssäni sekä kirjallisuuskatsauksessani, ei Katakri 2015 - auditointityökalussa ole. Katakri 2015 - auditointityökalu on selkeyttänyt toimintaympäristöänsä. Roolit ovat nyt selkeämpiä: ylimmällä tasolla ovat lait, normit sekä asetukset, joihin Katakri 2015 – auditointityökalu pohjaa. VAHTI toimisi jatkossa Katakri 2015 – auditointityökalua tulkitsevana, eikä VAHTI asettuisi ohjeistuksien kanssa ristiriitaan Katakri 2015 - auditointityökalun kanssa. Näiden alla on vielä toteutustavat, joita ovat tuotteet ja toimintatavat joilla pystytään toteuttamaan Katakri 2015 – auditointityökaluun vaatimuslähteistä koottuja vaatimuksia. Katakri 2015 - auditointityökalusta on pyritty tekemään paremmin aikaa kestävä kokonaisuus. Jatkossa tarkoituksena olisi, että liitteisiin voitaisiin tuoda enemmän yksityiskohtia ja ne esitettäisiin uudesta Katakrissa erillisenä dokumenttina. Lisätietokenttiin tuotaisiin samoin tarvittaessa uusia esimerkkejä tai muuta ohjausta.

Katakri 2015 – auditointityökaluun vaatimuslähteistä kootut vaatimukset ovat pääsääntöisesti tuotu selkeästi esiin suorine lähdeviittauksineen. Lähdeviittaukset kertovat mihin vaatimukset pohjautuvat, sieltä voidaan myös tuoda esiin, miksi jokin vaatimus on asetettu tietylle osaalueelle tai vaatimuksen toteutumiselle. Läpinäkyvyys on siten parantunut Katakri 2015 – auditointityökalussa. Kuitenkin on syytä tarkistaa myös annetusta lähteestä mitä siellä on asiasta sanottu.

Katakrin ensimmäisessä ja Katakrin toisessa versioissa esiintuodut elinkeinoelämän suositukset ovat Katakri 2015 - auditointityökalusta poistettu. Siihen kootut vaatimukset tukevat sen käyttämistä tietoturvallisuuden auditointityökaluna viranomaiskäyttöä varten. Katakria 2015 -

auditointityökalua muodostettaessa on haluttu myös palauttaa sen asema viranomaiskäytössä. Lisäksi on tuotu selvemmin esiin Katakri 2015 - auditointityökalun rooli auditointityökaluna, joka pohjaa olemassa oleviin lakeihin, normeihin ja asetuksiin. Karkeimmillaan Katakri 2015 - auditointityökalun voisi ajatella olevan tarkistuslista, kun kaikki sitä edeltävä suunnittelutyö ja sen toteuttaminen on tehty. Katakri 2015 – auditointityökalulla varmistettaisiin näiden jälkeen tarkistuslista luonteisesti, että kaikki on tullut sisäisissä ja ulkoisissa auditoinneissa huomioitua.

Katakrista tehdyissä aiemmissa opinnäytetöissä sekä esikartoituskyselyssäni toivottiin aikaisempien versioiden kaltaista elinkeinoelämän huomioimista KATAKRI 2015 –auditointi-työkalussa. Toistaiseksi Katakri 2015 kuitenkin on edelleen viranomaisille tarkoitettu auditointityökalu ja sen ajateltu ajan parempi kestäminen viestii myös, ettei elinkeinoelämän suosituksia siihen ole myöskään tulossa. Elinkeinoelämän suositukset ovat Katakri 2015 - auditointityökalusta poistettu- Elinkeinoelämä on kuitenkin ollut mukana kuultavana ja osallisena Katakrin uudistamistyössä.

Katakri 2015 – auditointityökalun käyttöönottamisen prosessia avatessa on selvää, miksi turvallisuusjohtaminen tulee liittää kiinteästi osaksi liikkeenjohtamista. Liikkeenjohdon tulee myös osoittaa oma sitoutumisensa turvallisuuteen, sen tulee olla selvää omalle organisaatiolle, sekä yhteistyötahoille. Turvallisuuspolitiikan luominen ja sen huomioiminen yrityksen strategiassa sekä visiossa ovat myös vahvoja viestejä johdon sitoutumisesta turvallisuuteen. Turvallisuusjohtamiseen tulee ottaa selkeä ote käyttämällä turvallisuusjohtamisjärjestelmää, mikä liitetään olennaisilta osin kiinteästi liikkeenjohtamiseen mukaan.

Turvallisuusjohtamisen vaatimusten tavoitteena on, että organisaatiolla on toimiva turvallisuuden hallintajärjestelmä sekä se kykenee menettelyillään varmistaman, että viranomaisen salassa pidettäviä tietoja käsittelevä henkilöstö toimii asianmukaisesti. Ilman selkeää ja järjestelmällistä dokumentointia sekä vastuuttamista yrityksen turvallisuutta on mahdotonta käsitellä selkeänä kokonaisuutena. Lisäksi selkeä ja järjestelmällinen dokumentaatio turvallisuuden osa-alueista sekä turvallisuudenjohtamisesta on edellytys, jotta organisaatio kykenee täyttämään Katakri 2015 – auditointityökaluun vaatimuslähteistä kootut vaatimukset. Kaikki lähtee liikkeelle dokumentaatiosta, jolla osoitetaan miten järjestelmän ja organisaation tulisi toimia. Sen jälkeen tarkastellaan, miten palaset toimivat käytännössä. Ilman sen hallitsemista KATAKRI 2015 - auditointityökalun koottujen vaatimusten täyttäminen ei ole mahdollista.

Katakri 2015 - auditointityökalussa muodostettu osa-alueiden modulaarinen rakenne mahdollistaa myös osittaisauditoinnit. Esikartoituskyselyssäni sekä aiemmissa opinnäytetöissä se tuli esiin aiempien versioiden kehityskohteena ja jopa ongelmana. Katakri 2015 – auditointityökalu vastaa siis myös näihin tarpeisiin ja on yksi niistä uudistuksista, joita itse siinä arvostan.

Turvallisuusjohtamisen (T) osiota pidetään Katakrin onnistuneimpana osuutena ja siihen on itsekin helppo yhtyä. Aiempien versioiden A+P osa-alueiden yhdistäminen oli hyvin perusteltu ja turhia päällekkäisyyksiä poistanut ratkaisu. Osa-alue on hyvä kooste yleisistä turvallisuusjohtamisen käytännöistä, kuitenkin on hyvä muistaa, että osittaisia auditointeja tehtäessä turvallisuusjohtamisen osa-alue pitää sisällyttää aina myös mukaan.

Katakri 2015 – auditointityökalu antaa hyvinkin paljon liikkumavaraa organisaatiolle vaatimusten täyttämiseksi. Tästä tuli hyvin erilaisia mielipiteitä esikartoituskyselyssäni, osa arvosti ehdottomia, selkeitä vaatimuksia Katakrin toisessa versiossa. Osa halusi liikkumavaraa Katakrin toisessa versiossa. Katakri 2015 - auditointityökaluun kohdistuneet odotukset liikkumavaran osalta olivat myös vaihtelevia, osa katsoi sen turvallisuutta heikentäväksi, toiset katsoivat sen ja riskilähtöisen ajattelun olevan sen selviä vahvuuksia. Itse näen sen Katakri 2015 – auditointityökalun suurena vahvuutena, vaikkakin se siirtää edelleen suurempaa taakkaa ja osaamisvaatimuksia auditoinnin suorittajan hartioille.

Riskienhallinnan integrointi osaksi turvallisuusjohtamista edesauttaa turvallisuuden hallintaa organisaatiossa merkittävästi. Järjestelmällinen, kokonaisvaltainen ja hyvin organisoitu turvallisuusjohtaminen vaatii myös selkeää dokumentointia, josta ilmenee kaikki yllämainitut asiat selkeästi esitetyssä ja ymmärrettävässä muodossa. Näin koko organisaation henkilökunta ymmärtää velvollisuudet, toimintatavat sekä vastuut. Hyvä ja kattava dokumentointi edesauttaa erilaisten auditointiprosessien läpivientiä ja on ehdoton vaatimus Katakri 2015 – auditointityökalun vaatimuslähteistä koottujen vaatimusten mukaisen auditoinnin läpiviemiseen hyväksytysti.

Kaksivaiheisen riskienarviointiprosessi vaaditaan, jotta Katakri 2015 – auditointityökalua voidaan käyttää tarkoitetulla tavalla. Ensimmäisessä vaiheessa suoritetaan kohdeympäristöön organisaatiolähtöinen riskienarviointi. Tämän jälkeen viranomainen suorittaa auditoinnin yhteydessä yleisiä uhkia kartoittavan riskienarvioinnin, jossa se hyväksikäyttää omaa tietoa sekä kokemuspohjaista osaamista. Riskienarvioinnista on myös hyötyä jokaisessa organisaatiossa, kun se on huolellisesti läpikäyty. Se tuo monitahoisesti esiin potentiaalisia ongelmia organisaatiossa sekä organisaation ja erilaisten sidosryhmien toiminnassa keskenään. Organisaatiolähtöinen riskienhallinta yhdistettynä viranomaisen suorittamaan yleisten uhkien kartoitukseen mahdollistaa myös vaatimusten tarkastelun riskien näkökulmasta, sekä osassa vaatimuksista niiden koventamisen tai lieventämisen. Tämä ei ollut aiemmin mahdollista, koska aiemmissa Katakrin versioissa kriteerit olivat ehdottomia, ne joko täyttyivät tai eivät täyttyneet. Katakri 2015 – auditointityökalu tarjoaa mahdollisuuden auditoijalle käyttää omaa harkintaa näissä tapauksissa ja sitä kautta on mahdollista tietyissä tapauksissa organisaation tehdä kustannustehokkaampia toimenpiteitä vaatimusten täyttämiseksi.

Katakri 2015 - auditointityökalussa käytetty lähdenormisto on kaikkien ulottuvilla ja tulkittavissa ilman Katakriakin. Missä on siis sen tuoma konkreettinen lisäarvo? Tämä kysymys tuli esiin muutamalta taholta opinnäytetyötä tehtäessä ja siihen opinnäytetyö on tuonut myös vastauksia. Katakri 2015 on viranomaiskäyttöön koottu auditointityökalu. Se on työkalu, jota hyödyntäen pystytään tarkastamaan, onko organisaation tietoturvallisuus vähintäänkin vaaditulla tasolla ja jotta voidaan sanoa, että se täyttää tietyt vaatimukset. Vaatimukset pysyvät näin myös yhdenmukaisempina auditoijalta toisella, kun jokainen ei tee auditointia omista lähtökohdista. Katakri 2015 – auditointityökalu vaatii enemmän auditoijalta. Se kuitenkin antaa myös runsaasti tukea auditoinnin suorittamiseksi juuri siksi että siihen on koottu ne oleellisimmat vaatimukset. Etukäteen suoritettu organisaatiolähtöinen riskienarviointi täydentää näitä.

Katarki 2015 – auditointityökaluun laeista, normeista, asetuksista ja kansainvälisistä sopimuksista kootut vaatimukset sekä riskilähtöisyys, turvallisuusjohtamisen osa-alue ja modulaarinen rakenne ovat perusteltuja syitä Katakri 2015 – auditointityökalun muodostamiseen.

Tarkastellessa Katakri 2015 – auditointityökalun selkeämpää modulaarista rakennetta huomaa, että siinä on selvästi erikseen asetettuna omiin moduuleihinsa osa-alueet T eli turvallisuusjohtamisen osa-alue ja F eli fyysisen turvallisuuden osa-alue, jotka käsittelevät toimintaympäristöä, sekä toiminnan hallinnointia. Varsinainen suojattava kohde (ASSET) eli I-osa-alue, mikä uudessa Katakrissa tarkoittaa viranomaisen salassa pidettävää tietoa, pienellä virittelyllä suojattavaksi kohteeksi voidaan asettaa esimerkiksi avainhenkilöstöä tai vaikkapa logistiikka ketju, tällöin asiat tulee käydä alusta lähtien riskilähtöisesti, arvioiden organisaation tarpeita, edeten projekti muotoisesti riskienarvioinnista, aina auditointi prosessin läpivientiin saakka.

Tulevaisuudessa Katakri 2015 – auditointityökalun vaatimuksia olisi F-osa-alueen osalta hyvä viedä osaksi rakennusmääräyskokoelmaa sekä RT-kortistoa. Niiden kautta saataisiin jo rakentamisen suunnitteluvaiheessa huomioitua rakennukselle asetettavia vaatimuksia. Rakennusmääräyskokoelman päätasolle vietäisiin lakien ja asetusten vaatimukset ja sieltä ne vietäisiin osaksi esimerkiksi paloturvallisuusosiota (E) sekä sieltä RT-kortteihin. Tätä kautta tieto vaatimuksista ja ratkaisumalleista saataisiin toimivalla tavalla suunnittelijoidenkin ulottuville. Lisäksi kokonaisten tietojenkäsittely- ja tietoliikenneympäristön kuvaus esimerkinomaisesti eri turvallisuustasoilla edesauttaisi kokonaiskuvan rakentumista ja siten Katakri 2015 – auditointityökaluun vaatimuslähteistä koottujen vaatimusten täyttämistä organisaatioissa. Syyt eri vaatimusten takana myös syventäisivät ymmärrystä ja avaisivat vaatimuksia organisaatioiden kaikilla tasoilla, joille ymmärrystä olisi hyvä tuottaa, jolloin organisaation kaikki osaset ovat

konkreettisesti mukana omalta osaltaan kehittämässä ja ylläpitämässä tietoturvallisuutta organisaatiossa.

Huomioitavaa on, että Katakri 2015 on auditointityökalu. Auditoinnit voitaisiin suorittaa useilla muilla tavoilla. Katakri 2015 – auditoinityökalu yhdenmukaistaa auditoijien auditointeja ja siten edesauttaa niiden keskinäistä vertailtavuutta.

Työ opinnäytetyöni parissa oli pääasiassa mielenkiintoista. Uutta asiaa tuli runsaasti ja vanha tieto syveni opinnäytetyötä työstettäessä. Etenkin auditointiprosessi avautui uudella tavalla ja palaset loksahtivat siinä kohdalleen. Katakrin historian kaari sekä asiantuntijoiden kanssa käymät keskustelut kasvotusten, verkossa ja muissa ympäristöissä koskien Katakria toivat runsaasti uutta tietoa ja näkemystä sekä hyvinkin yksityiskohtaista uutta tietoa itselle siitä. Työ kesti pitkään, koska aihe oli yllättävän laaja. Siinä oli yksinkertaisesti paljon mielenkiintoisia aiheita, joita olisi ollut mahdollista liittää osaksi opinnäytetyötä. Aneiston karsiminen oli ajoittain hyvin vaikeaa. Kaikkea uutta opittua ei pystynyt siten millään ottamaan mukaan tähän opinnäytetyöhön, koska se olisi rönsyillyt vielä runsaasti ja levinnyt yhä uusiin suuntiin. Kaikesta opitusta opinnäytetyön tekemisen yhteydessä on varmasti hyötyä tulevaisuudessa. Auditoinnit, arviointi ja ohjaus kiinnostavat myös jatkossa sekä syvemmät opinnot turvallisuuden parissa. Niiden pariin tulen siis pyrkimään.

Lähteet

Kirjalliset lähteet:

Birmingham, P. 2000. Reviewing the Literature. Teoksessa Researcher's Toolkit: The Complete Guide to Practitioner Research, 25–40.

Flink, A-L., Reiman, T. & Hiltunen, M. 2007. Heikoin lenkki – Riskienhallinnan inhimilliset tekijät. Helsinki: Edita Prima.

Hakala, M., Vainio, M.& Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Ohjeistus, toteutus ja lainsäädäntö Jyväskylä: Docendo Finland.

Hirsjärvi, S., Remes, P. & Sajavaara P. 2009. Tutki ja kirjoita. 15. painos. Hämeenlinna: Karisto n Kirjapaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2013. Tutki ja kirjoita. 15. - 17. painos. Helsinki: Tammi.

Hopkin, P. 2012. Fundamentals of risk management: understanding, evaluating and implementing effective risk management. 2. uudistettu painos. London, Philadelphia, New Delhi: KoganPage.

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

Järvinen, P. 2002. Tietoturva & yksityisyys. Porvoo: Docendo Finland.

Järvinen, P. 2006. Paranna tietoturvaasi. Jyväskylä: Docendo.

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

Krutz, R. & Vines, R. 2003. (Käännös Suominen E.) Tietoturvasertifikaatti, CISSP. Helsinki: IT Press.

Laaksonen, M., Nevasalo, T.& Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita Publishing.

Leppänen, J. 2006. Yritysturvallisuus käytännössä – Turvallisuusjohtamisen portfolio. Helsinki: Talentum.

Miettinen, J. 1999. Tietoturvallisuuden johtaminen: Näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari.

Miettinen, J. 2002. Yritysturvallisuuden käsikirja. Helsinki: Kauppakaari.

Mäkinen, K. 2007. Organisaation strateginen kokonaisturvallisuus. Helsinki: Edita.

Oedewald, P. & Reiman, T. 2006. Turvallisuuskriittisten organisaatioiden erityispiirteet. Espoo: VTT.

Oedewalt, P. & Reiman, T. 2008. Turvallisuuskriittiset organisaatiot. Helsinki: Edita.

Ojasalo, K, Moilanen T. & Ritalahti, J. 2010. 1.-2. painos. Helsinki: WSOYpro.

Paasonen, J. (toim.), Huumonen, T. ja Paasonen, L. 2012. Oppilaitoksen turvallisuusjohtaminen. Helsinki: Tietosanoma.

Paavilainen, J. 1998. Tietoturva. Jyväskylä: Suomen ATK-Kustannus.

Ruohonen, M. 2002. Tietoturva. Porvoo: Docendo Finland.

SFS-ISO 27001. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardisoimisliitto SFS.

SFS-ISO 31000. 2009. Riskienhallinta. Periaatteet ja ohjeet. Helsinki: Suomen Standardisoimisliitto.

Valli, R. 2007. Kyselylomaketutkimus. Teoksessa Aaltola, J. & Valli, R. (toim.) Ikkunoita tutkimusmetodeihin I - Metodin valinta ja aineiston keruu: virikkeitä aloittelevalle tutkijalle. 2.p. Jyväskylä: PS-kustannus.

Sähköiset lähteet:

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 02.05.2015. http://www.fsd.uta.fi/menetelmaopetus.

Haaga-Helia ammattikorkeakoulu 2014. Raportointi ja opinnäytetyö Haaga-Heliassa. Haaga-Helia ammattikorkeakoulu. Viitattu 1.4.2015. http://myy.haaga-helia.fi/~vanvu/office2013/word/ohjeet/raportointi_ja_opinnaytetyo_ohje.pdf

COSO-ERM - Enterprise Risk Management – Intergrated Framework tiivistelmä. Viitattu 19.5.2015. http://www.coso.org/documents/coso_erm_executivesummary_finnish.pdf

Euroopan neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä 23.9.2013/488/EU. Viitattu 12.7.2015. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2013.274.01.0001.01.FIN

Hallituksen esitys Eduskunnalle laiksi yksityisistä turvallisuuspalveluista sekä eräiksi siihen liittyviksi laeiksi (HE 69/2001). Viitattu 1.4.2015. http://www.finlex.fi/fi/esitykset/he/2001/20010069

Kansallinen turvallisuusauditointikriteeristö. 2009. Katakri I. Viitattu 30.12.2014. http://www.defmin.fi/files/1525/Katakri.pdf

Kansallinen turvallisuusauditointikriteeristö. 2011. KATAKRI versio II. Viitattu 30.12.2014. http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011). Viitattu 15.6.2015. https://www.finlex.fi/fi/laki/alkup/2011/20111406

Laki kansainvälisistä tietoturvallisuusvelvoitteista (2004/588). Viitattu 11.6.2015. https://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Laki kansainvälisistä tietoturvallisuusvelvoitteista annetun lain muuttamisesta (2014/731). Viitattu 11.6.2015. http://www.finlex.fi/fi/laki/alkup/2014/20140731

Laki tietoturvallisuuden arviointilaitoksista (2011/1405). Viitattu 11.6.2015. https://www.finlex.fi/fi/laki/ajantasa/2011/20111405

Nurmi, K. 2011. Tietoturvallisuuden hallinnan suunnittelu ja toteutus - Projektiopas valtionhallinnon organisaation tietoturvallisuudesta vastaavalle. Viitattu 15.5.2015. http://tietoturvatalkoot.fi/Projektiopas.pdf

Puolustusministeriö. 2009. Kansallinen turvallisuusauditointikriteeristö. Viitattu 5.10.2014. http://www.defmin.fi/files/1525/KATAKRI.pdf

Puolustusministeriö. 2011. KATAKRI. Viitattu 21.11.2014. http://www.defmin.fi/hallinnonala/puolustushallinnon_turvallisuustoiminta/kansallinen_turvallisuusauditointikriteeristo_%28katakri%29

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja. Viitattu 15.4.2015. https://docs.google.com/viewer?url=http%3A%2F%2Fwww.uva.fi%2Fmateriaali%2Fpdf%2Fisbn_978-952-476-349-3.pdf.

Sisäministeriön asetus poliisin suoritteiden maksullisuus vuonna 2015 (1023/2014). Viitattu 10.9.2015. http://www.finlex.fi/fi/laki/alkup/2014/20141023

Suojelupoliisi. 2014. Suojelupoliisi määrättynä turvallisuusviranomaisena. Viitattu 26.12.2014. http://www.supo.fi/poliisi/supo60/home.nsf/pages/BCCA55E2A478FD7CC22576010035B90C?opendocument.

Suomen Standardisoimisliitto SFS Ry. Mikä SFS on? Viitattu 16.5.2015. http://www.sfs.fi/sfs_ry

The Committee of Sponsoring Organizations of the Treadway Commission (COSO). What is Coso? Viitattu 20.5.2015. http://www.coso.org

Pohjola Pankki Oyj. Turvallisuusjohtaminen. Viitattu 19.12.2014. https://www.pohjola.fi/pohjola/yritys-ja-yhteisoasiakkaat/riskienhallinta/tyoturvallisuus/turvallisuusjohtaminen?id=328210

Työsuojeluhallinto. 2010. Turvallisuusjohtaminen. Viitattu 2.4.2015. http://tyosuojelujulkaisut.wshop.fi/documents/2010/08/TSO_35.pdf

Turvallisuusselvityslaki (726/2014). Viitattu 11.6.2015. http://www.finlex.fi/fi/laki/alkup/2014/20140726

Työturvallisuuslaki (738/2002). Viitattu 20.12.2014. http://www.finlex.fi/fi/laki/alkup/2002/20020738

Ulkoministeriö 2011. Yritysturvallisuuskäsikirja. Viitattu 20.12.2014. http://formin.finland.fi/public/download.aspx?ID=89013&GUID={1787C81D-6598-4469-AA23-FFB2A9DBC413}

Ulkoministeriö 2015. Turvallisuusviranomaisten käsikirja yrityksille. Viitattu 18.9.2015. http://formin.finland.fi/public/download.aspx?ID=89013&GUID={1787C81D-6598-4469-AA23-FFB2A9DBC413}

Ulkoasiainministeriö 2012. Hallinnollinen järjestely Suomen hallituksen ja Pohjois-Atlantin liiton (NATO) kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi. Viitattu 5.2.2015. http://www.eduskunta.fi/triphome/bin/thw/?${APPL}=akirjat&${BASE}=akirjat&${THWIDS}=0.37/1428953977_3890&${TRIPPIFE}=PDF.pdf

Ulkoministeriö 2014. Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje. Viitattu 3.4.2015. http://formin.finland.fi/public/download.aspx?ID=68032&GUID=%7B25313BDA-49BD-43EF-B106-3E9CE01AF6B0%7D.

Ulkoasiainministeriö. 2014. Kansallinen turvallisuusviranomainen. Viitattu 12.2.2014. http://formin.finland.fi/Public/default.aspx?nodeid=46935&contentlan=1&culture=fi-FI

Ulkoministeriö 2015. KATAKRI – tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 13.4.2015. http://formin.finland.fi/public/download.aspx?ID=142173&GUID=%7B7DF3B93D-6E25-4269-8A12-655D7FABEED6%7D

Valtionvarainministeriö 2007. Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Viitattu 25.8.2011. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/vahti3_07_netti.pdf

Valtiovarainministeriö. VAHTI. Viitattu 20.05.2015. http://www.hare.vn.fi/mHankePerusSelaus.asp?h_iId=19882

Valtiovarainministeriön johdon tietoturvaopas. Valtiovarainministeriö 2011. Viitattu 15.12.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20111207Johdon/Johdon_tietoturvaopas.pdf

Valtiovarainministeriön ohje koskien henkilöstöturvallisuutta. 2008. Valtiovarainministeriö 2008. VAHTI 2/2008. https://www.vahtiohje.fi/c/document_library/get_file?uuid=af5614a4-fa44-482c-9886-0af9e6a13929&groupId=10128&groupId=10229

VAHTI toimintasuunnitelma. Valtiovarainministeriö 2014. Viitattu 6.4.2015. http://www.2014.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20140306VAHTIn/VAHTIn_toimintasuunnitelma_2014.pdf

Asetus tietoturvallisuudesta valtionhallinnossa (681/2010). Valtioneuvosto 2010. Viitattu 2.4.2015. http://www.finlex.fi/fi/laki/alkup/2010/20100681

Viestintävirasto. 2013. NCSA-toiminto. Viitattu 12.12.2014. https://www.viestintavirasto.fi/tietoturva/viestintavirastontietoturvapalvelut/ncsa-fi.html
Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Kustannusosakeyhtiö Tammi.

VTT. 2010. PK-yritysten riskienhallinta - Mitä riskienhallinta on? Viitattu 6.4.2015. http://virtual.vtt.fi/virtual/pkrh/startti-riskienhallintaan.html

Yritysturvallisuus EK 2015. Yritysturvallisuuden osa-alueet. Viitattu 20.12.2014. http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

Julkaisemattomat lähteet:

Valtiovarainministeriö, erityisasiantuntija, Janhunen, K. Uuden Katakri projektin esittely. 2.12.2014.

Valtiovarainministeriö, erityisasiantuntija, Janhunen, K. Katakri 2015 – auditointityökalun esittely. 1.4.2015.

Elinkeinoelämän Keskusliitto, asiantuntija, Susi M. Lausunto Katakri 2015 - auditointityökalusta. 13.4.2015.

Kansallinen tietoturvallisuusviranomainen, erityisasiantuntija. Haastattelu 12.11.2015.

Tietohallintojohtaja, Sisäministeriö. Sähköinen haastattelu 13.11.2015.

Yksikönpäällikkö, Valtiovarainministeriö. Sähköinen haastattelu 16.11.2015.

Katakri 2015 – auditointityökalun viimeistelytyöryhmän jäsen, Poliisihallitus. Sähköinen haastattelu 18.11.2015.

Kansallisen turvallisuusviranomaisen päällikön sijainen, Ulkoministeriö. Sähköinen haastattelu 23.11.2015.

Kuvat

Kuviot

Taulukot

Liitteet

Liite 1 Esikartoitus haastattelututkimuksen taustakysymykset

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 1. Sukupuoli**

- Mies
- Nainen

Seur.

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 2. Ikä**

- Alle 24
- 24-34
- 35-44
- 45-54
- 55-64
- 65+

Edell. Seur.

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 3. Koulutus**

- [ ] Ammattitutkinto
- [ ] Erikoisammattitutkinto
- [ ] Ylioppilas
- [ ] Ammattikorkeakoulu(Alempi)
- [ ] Ammattikorkeakoulu(Ylempi)
- [ ] Yliopistotutkinto(Alempi)
- [ ] Yliopistotutkinto(Ylempi)
- [ ] Lisensiaatti
- [ ] Tohtori
- [ ] Muu tutkinto, täsmennä kommenttikentässä

Edell. Seur.

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 4. Työkokemus turvallisuusalalta vuosina**

- ( ) 0-2 vuotta
- ( ) 3-5 vuotta
- ( ) 6-9 vuotta
- ( ) 10 - 20 vuotta
- ( ) 21+ vuotta

Edell. Seur.

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 5. Oletko käyttänyt KATAKRIa auditointi työkaluna?**

- ○ Kyllä
- ○ Ei

*** 6. Kuvailkaa lyhyesti miten olette käytännössä hyödyntänyt KATAKRIa?**

Edell. Seur.

Liite 2 Esikartoitus haastattelututkimuksen kysymykset

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 7. Mitä vahvuuksia on KATAKRIn toisessa versiossa? (KATAKRI versio II)**

Edell. Seur.

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 8. Mitä kehityskohteita on KATAKRIn toisessa versiossa? (KATAKRI versio II)**

Edell. Seur.

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 9. Oletteko jo tutustuneet KATAKRIn kolmanteen versioon? (KATAKRI versio III)**

- ○ Kyllä
- ○ Ei (Tutkimus päättyy osaltanne tähän, painakaa lopuksi seuraavalle sivulle siirtyminen nappulaa vielä, kiitos)

Edell. Seur.

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 10. Mitä vahvuuksia on KATAKRIn kolmannessa versiossa? (KATAKRI versio III)**

Edell. Seur.

Esikartoitusta varten tehty kyselytutkimus koskien KATAKRI III opinnäytetyötä

*** 11. Mitä kehityskohteita on KATAKRIn kolmannessa versiossa? (KATAKRI versio III)**

Edell. Loppu

Liite 3 Esikartoitus haastattelututkimuksen saatekirje

Tervehdys!
Teen LAUREAssa tällä hetkellä opinnäytetyötä koskien KATAKRIn pian ilmestyvää kolmatta versiota. (KATAKRI versio III)

Tässä kyselyssä suoritan taustatutkimusta koskien KATAKRIa ja osana sitä suoritan esikartoitusta KATAKRIsta asiantuntijahaastattelujen muodossa.

Pyytäisin teitä käyttämään hetken ja vastaamaan muutamaan avoimeen kysymykseen koskien KATAKRIa, sekä tutkimuksen tarvitsemiin taustatietokysymyksiin.

Kaikki vastaukset käsitellään luottamuksellisesti.
Vastausaikaa on tutkimukselle 20.12.2014 kello 01.00 asti.

Alla linkki tutkimukseen:
https://fi.surveymonkey.com/s/Esikartoitus_KATAKRI3

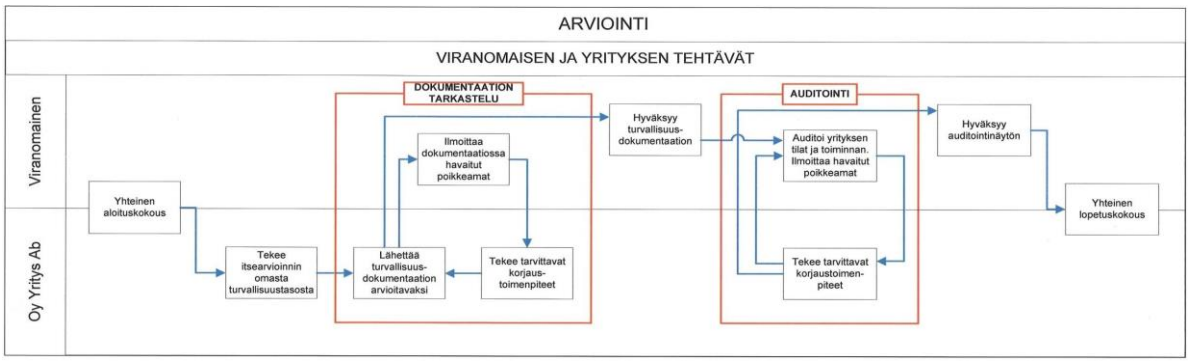
Kysymykset asian tiimoilta voitte esittää minulle suoraan alla olevin tavoin.
Opinnäytetyön tekijä:
Aki Roivainen
Turvallisuuden tradenomi opiskelija LAUREA
aki.roivainen@laurea.fi
aki.roivainen@gmail.com
+358 40 41 22 671

Tutkimuksessa edetään valitsemalla joko vaihtoehto/vaihtoehtoja tai vaihtoehtoisesti kirjoittamalla vapaa muotoinen vastaus kommenttikenttään. Tämän jälkeen painetaan seuraava - nappulaa ja tutkimus päättyy viimeisen kysymyksen yhteydessä loppu - nappulaa painamalla, jolloin vastaukset tallentuvat.
Vastauksia pääsette muuttamaan painamalla edellinen - nappulaa.

Kiitos ajastanne ja vastauksistanne!
Alla linkki tutkimukseen:
https://fi.surveymonkey.com/s/Esikartoitus_KATAKRI3

Liite 4 Katakrin käyttö osana yritysturvallisuusselvitystä

Yritysturvallisuusselvitykseen liittyvä arviointiprosessi on esitetty allaolevassa kuvassa. Prosessikaaviossa kuvataan viranomaisen ja yrityksen tehtävät arvioinnin eri vaiheissa. Arviointiin sisältyy yrityksen tietojärjestelmien auditointiprosessi silloin, kun se tehdään osana yritysturvallisuusselvitystä.



Yritysturvallisuusselvitys voidaan laatia osittaisena. Jos yritysturvallisuusselvityshakemuksessa yritykseltä ei edellytetä kykyä suojata viranomaisen salassa pidettävää tietoa toimitiloissaan (”FSC without safeguards”), arvioinnissa voidaan käyttää pelkästään turvallisuusjohtamisen osa-aluetta. Jos yritysturvallisuusselvityspyynnössä edellytetään myös kykyä suojata viranomaisen salassa pidettäviä tietoja yrityksen toimitiloissa (”FSC with safeguards”), arvioinnissa voidaan käyttää turvallisuusjohtamisen osa-alueen lisäksi fyysisen turvallisuuden osa-aluetta ja niitä teknisen tietoturvallisuuden osa-alueen vaatimuksia, jotka koskevat paperiasiakirjojen käsittelyä.

Valmistautuminen auditointiin

Ennen varsinaisen viranomaisarvioinnin aloittamista yrityksen tulee saattaa tietojenkäsittelyympäristönsä turvallisuusjärjestelyt ja jäännösriskit sellaisella tasolle, että ne ovat yrityksen riskienhallinnassa hyväksyttävissä. Yrityksen tulee toimittaa viranomaiselle arvioitavaksi riskienhallintatuloksensa sekä kuvaus turvallisuusjärjestelyjen vaatimustenmukaisuudesta. Riskienhallintatuloksille ja turvallisuusjärjestelyjen vaatimustenmukaisuuden kuvaukselle ei edellytetä tietyn määrämuotoisen lomakemallin käyttämistä.

Yrityksen riskienhallinta

Yrityksen turvallista toimintaa uhkaavien riskien hallinta toimii perustana turvallisuusjärjestelyjen oikealle mitoitukselle. Toimivaltainen viranomainen suhteuttaa vaatimuksensa lähtökoh-

taisesti siihen uhkaympäristöön ja niihin turvatoimiin (kontrolleihin), jotka yritys esittää. Viranomaisen käsitys uhkista saattaa kuitenkin poiketa siitä, mihin yritys on omista lähtökohdistaan päätynyt.
Tiedon suojaamiseen tähtäävä turvallisuusriskien hallintaprosessi voidaan kuvata yksinkertaistetusti neljään vaiheeseen:
riskien tunnistaminen,
riskien analysointi vaikutusten ja todennäköisyyksien määrittämiseksi,
riskien arviointi tarkoituksenmukaisten turvatoimienvalitsemiseksi, ja
riskien toteutumiseen varautuminen riskienhallintaprosessin seurantamenettelyjen kautta

Riskienhallinnan kattavuutta ja muita sille asetettuja vaatimuksia käsitellään yksityiskohtaisemmin osa-alueella T (erityisesti T 04).
Yrityksen tulee pystyä riskienhallintaprosessinsa kautta osoittamaan toimivaltaiselle viranomaiselle perusteensa valituille turvatoimille ja niiden riittävyydelle. Yritystä suositellaan keskustelemaan riskiensä määrittelystä ja turvatoimisuunnitelmistaan toimivaltaisen viranomaisen kanssa jo varhaisessa vaiheessa, jotta sekä yrityksen että toimivaltaisen viranomaisen arviot kyseisen ympäristön riskeistä pystytään huomioimaan jo turvatoimia suunniteltaessa.

Kuvaus yrityksen turvallisuusjärjestelyjen vaatimustenmukaisuudesta

Yrityksen turvallisuusjärjestelyjen vaatimustenmukaisuuden kuvauksen tavoitteena on esittää kootusti ne turvallisuusjärjestelyt, joilla yritys pyrkii täyttämään turvallisuusvaatimukset. Kuvausta hyödynnetään erityisesti viranomaisen auditoinnin suunnittelussa ja toteutuksessa 1.

Liite 5 Yritysturvallisuusselvityshakemus

Yritysturvallisuusselvityshakemus

(Turvallisuusselvityslaki 726/2014)

Hakemuksen diaarinumero (toimivaltainen viranomainen täyttää)

A1. HAKIJAN TIEDOT

Hakija (organisaatio)	Y-tunnus	
Lähiosoite	Postinumero	Postitoimipaikka
Yhteyshenkilön nimi ja asema		
Puhelinnumero	Sähköpostiosoite	

A2. SELVITYKSEN KOHTEEN TIEDOT

Organisaatio **HUOMIOI LIITE 1**	Y-tunnus	
Lähiosoite	Postinumero	Postitoimipaikka
Yhteyshenkilön nimi ja asema		
Puhelinnumero	Sähköpostiosoite	
Hyväksytty tietoturvallisuuden arviointilaitos (1405/2011) on laatinut arvioinnin organisaatiosta **HUOMIOI LIITE 2** ☐ kyllä ☐ ei		

A3. SELVITYKSEN LAATIMISELLE SÄÄDETTYJEN EDELLYTYSTEN TÄYTTYMINEN

Valitse yksi kohta. Tämän lisäksi liitä hakemukseen tarkemmat tiedot selvityksen laatimisen perusteista. Tarkemmat tiedot yritysturvallisuusselvityksen laatimisen edellytyksistä löytyvät lain 36 §:sta.

☐	Selvityksen kohteelle luovutetaan sopimuksen yhteydessä viranomaisen luokiteltuja tietoja (ST I -ST III) **HUOMIOI LIITE 3**
☐	Selvityksen kohde voi tulla valituksi kansainväliseen tarjouskilpailuun taikka toisessa valtiossa järjestettävään hankkeeseen **HUOMIOI LIITE 3 JA 4**
☐	Selvitys on laadittava kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi **HUOMIOI LIITE 3**
☐	Selvityksen kohde aloittaa yritystoiminnan toisessa valtiossa **HUOMIOI LIITE 3 JA 4**
☐	Selvityksen kohde harjoittaa ydin- tai räjähdysaineisiin liittyvää toimintaa (21§:n 1 mom. kohdat 5 ja 6) **HUOMIOI LIITE 3**
☐	Selvityksen kohteella tai sen työntekijöillä on pääsy 21§:n 1 mom kohdissa 5 ja 6 tarkoitettuihin tietoihin taikka tiloihin tai alueelle **HUOMIOI LIITE 3**
☐	Selvitys on laadittava lain tai sen nojalla annetun säännöksen mukaan **HUOMIOI LIITE 3**

A4. SELVITETTÄVÄ TIETOTURVALLISUUDEN TASO

Valitse yksi kohta molemmilta riveiltä, mikäli yritysturvallisuusselvityksen avulla on tarkoitus osoittaa yrityksen täyttävän määrätty tietoturvallisuuden taso. Muussa tapauksessa jätä kohdat täyttämättä.

Tietoturvallisuuden taso	☐ ST IV	☐ ST III / (EU-C/NC)	☐ ST II / (EU-S/NS)	☐ ST I / (EU-TS/CTS)
Käytettävä arviointiperuste **HUOMIOI LIITE 5**	☐ KATAKRI	☐ VAHTI-ohjeet		
	☐ Muu, mikä? _____			

A5. YRITYSTURVALLISUUSSELVITYKSEN LAAJUUS

Yritysturvallisuusselvitys voidaan tehdä myös osittaisena, jos se on selvityksen tarkoituksen toteuttamiseksi perusteltua. Valitse kohdat, jotka esitetään sisällytettäväksi yritysturvallisuusselvitykseen.

☐ Selvityksen kohteen vastuuhenkilöiden taustaselvitys (3§ 1 mom. kohta 7) **HUOMIOI LIITE 6**
☐ Selvityksen kohteen (organisaation) rekisteriperusteinen taustaselvitys
☐ Selvityksen kohteen hallinnollinen turvallisuus ja henkilöstöturvallisuus
☐ Selvityksen kohteen fyysinen turvallisuus
☐ Selvityksen kohteen tekninen tietoturvallisuus

A6. SELVITYKSEN KOHTEEN ALIHANKKIJOIDEN TIEDOT

Toimivaltainen viranomainen voi ulottaa yritysturvallisuusselvityksen koskemaan myös selvityksen kohteen alihankkijana toimivia yrityksiä. Hakemuksen liitteestä tulee ilmetä ne alihankkijat, joiden kanssa selvityksen kohde aikoo tehdä sopimuksen yritysturvallisuusselvityksen perusteena olevan hankkeen toteuttamisesta. Alihankkijoiden tiedot tulee ilmoittaa samassa laajuudessa, kuin kohdassa A2. Lisäksi liitteestä tulee ilmetä jokaisen alihankkijan osuus hankkeen toteuttamisessa. **HUOMIOI LIITE 2 JA 7.**

A7. HAKIJAN ALLEKIRJOITUS

Paikka ja aika	Allekirjoitus ja nimenselvennös

A8. HAKEMUKSEN LIITTEET

Yritysturvallisuusselvityshakemus on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) perusteella lähtökohtaisesti julkinen asiakirja. Hakija voi kuitenkin lisätä hakemuksen liitteeksi hakijan tai selvityksen kohteen salassa pidettäviä tietoja, joita käsitellään ja säilytetään viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaisesti salassa pidettävinä osana yritysturvallisuusselvitystä.

LIITE 1

☐ Suostumusasiakirja, josta ilmenee selvityksen kohteen suostumus yritysturvallisuusselvityksen laatimiseen (jollei selvityksen kohde ole hakija). Asiakirjasta tulee käydä ilmi, että selvityksen kohde on ennen suostumuksen antamista saanut tiedon yritysturvallisuusselvityksen ja luotettavuuden seurannan tarkoituksesta ja niiden käytöstä.

LIITE 2

☐ Kopiot tietoturvallisuuden arviointilaitoksen antamista todistuksista, jos selvityksen kohteesta tai alihankkijoista on laadittu tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitetun hyväksytyn arviointilaitoksen laatima arviointi

LIITE 3

☐ Asiakirjat, joista käy ilmi yritysturvallisuusselvityksen tarve, tarkat tiedot luovutettavasta tai muodostuvasta salassa pidettävästä tietoaineistosta ja tulevista tietojenkäsittely- ja säilytystiloista, mikäli tilat on päätetty jo hakemusvaiheessa.

LIITE 4

☐ Selvitys kansainvälisestä hankkeesta tai tarjouksesta, jos hanke tai tarjouskilpailu on selvityksen laatimisen perusteena sekä kansainvälisen järjestön tai toimielimen säännöt tai toisen valtion laki, jossa edellytetään yritysturvallisuusselvityksen laatimista

LIITE 5

☐ Yritysturvallisuusselvityksessä käytettävä arviointiperuste, jos kyseessä on muu kuin KATAKRI tai VAHTI-ohjeet

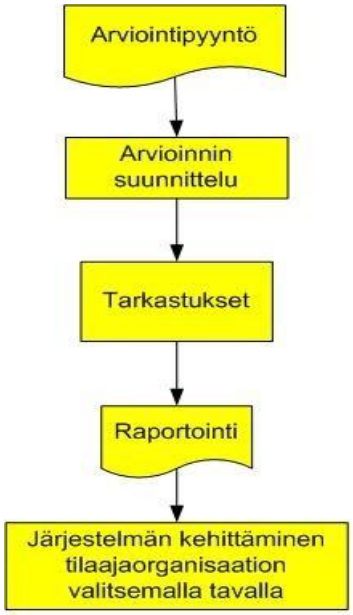
LIITE 6

☐ Selvityksen kohteen vastuuhenkilöiden henkilöturvallisuusselvityshakemukset, mikäli osana yritysturvallisuusselvitystä laaditaan selvityksen kohteen vastuuhenkilöiden taustaselvitys

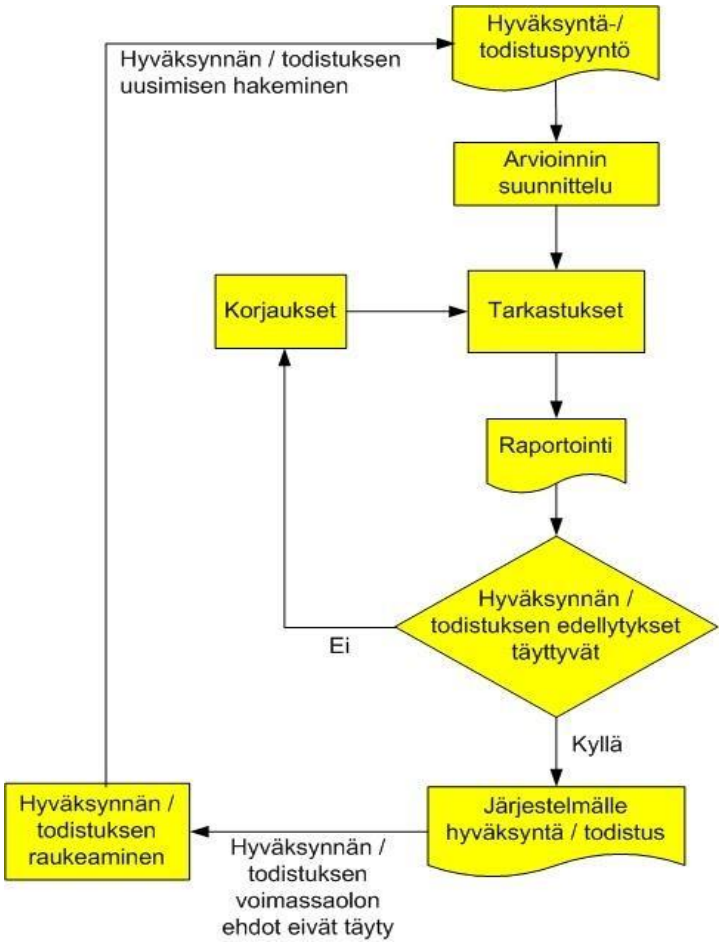
LIITE 7

☐ Alihankkijoiden A2.-kohdan mukaiset tiedot (pois lukien liitteen 1 suostumusasiakirja) sekä selvitys jokaisen alihankkijan osuudesta yritysturvallisuusselvityksen perusteenaolevan hankkeen toteuttamisessa

Liite 6 Tietojärjestelmän arviointiprosessi yksinkertaistettuna



Liite 7 Tietojärjestelmien hyväksyntäprosessi yksinkertaistettuna



Hyväksyntäprosessi kuvauksessa keskitytään yritysturvallisuusselvityksen ja viranomaisten tietojärjestelmien arvioinnin käyttötapauksiin, joissa toimivaltaisena viranomaisena on Viestintävirasto. Kuvaus on jaoteltu käyttötapausten, arviointi- ja hyväksyntäprosessien sekä hyväksynnän ja todistuksen esittelyyn. Kuvauksessa ei käsitellä muita käyttötapauksia, esimerkiksi käyttöä osana organisaation sisäistä turvallisuustyötä.

Liite 8 Henkilöturvallisuusselvityshakemus

Viivakoodi

Henkilöturvallisuusselvityshakemus 1 (2)

Turvallisuusselvityslaki (726/2014)

Lähettäen diaarietiedot

Salassapitoleima

A1. Turvallisuusselvityksen laajuus

☐ Suppea ☐ Perusmuotoinen ☐ Laaja

A2. Hakijan tiedot (Työnantaja/toimeksiantaja täyttää)

Hakija (organisaatio)	
Yhteyshenkilön nimi ja asema	
Puhelin	Sähköpostiosoite

A3.Selvityksen hakemisen peruste

☐ Nimitys virka- tai työsuhteeseen	☐ Kansainvälisen henkilöturvallisuustodistuksen hakeminen (PSC, KvTitaL 588/2004)
☐ Pääsy viranomaisen turvallisuusluokiteltuun tietoon/tilaan	☐ Henkilöturvallisuustodistuksen hakeminen (43 §)
☐ Koulutukseen hakeutuminen	☐ Turvallisuusselvityksen uusiminen

A4. Tehtävän tiedot

Tehtävänimike	Yritys/työnantaja
Tarkka tehtäväkuvaus (mitä tekee, missä tekee)	
Kuvaus suojattavasta tilasta tai tiedosta (mt.suojattavan tiedon taso)	
☐ Työ- tai virkasuhde on vakituinen/ toistaiseksi voimassa oleva	☐ Työ- tai virkasuhde on määräaikainen ajalle:

A5. Hakija hakee selvityksen kohteesta lisäksi itse

☐ Huumausainetestin ☐ Lääkärintodistuksen ☐ Luottotiedot

B1. Selvityksen kohteen henkilötiedot

Sukunimi	Etunimet
Entiset nimet	Henkilötunnus (jos ei ole, syntymäaika)
Sukupuoli ☐ Mies ☐ Nainen / Siviilisääty	Ammatti
Syntymäkotikunta	Syntymävaltio
Kansalaisuus	Äidinkieli
Entiset kansalaisuudet, muutospäivämäärät	
Muut kansalaisuudet	

B2. Selvityksen kohteen yhteystiedot

Lähiosoite	Postinumero Postitoimipaikka
Postiosoite, jos eri kuin yllä	Postinumero Postitoimipaikka
Puhelinnumero virka-aikana	Matkapuhelin
Sähköpostiosoite	

☐ Selvityksen kohteella on väestörekisterilain 36 §:n mukainen turvakielto (tietoja käsitellään suojausvaatimukset huomioiden)

C. Perusmuotoista henkilöturvallisuusselvitystä koskevat tiedot

Jos haettavana on perusmuotoinen henkilöturvallisuusselvitys, täyttäkää alla olevaan taulukkoon tiedot asuinpaikoistanne ulkomailla edellisen kymmenen vuoden ajalta (jatkakaa tarvittaessa erillisellä liitteellä).

Osoite	Valtio	Asumisen syy	Oleskeluajanjakso

D. Tiedoksiannot ja suostumukset (selvityksen kohde allekirjoittaa ja täyttää)

Turvallisuusselvityksen tekemisestä on ilmoitettu minulle etukäteen.
Olen saanut tiedon turvallisuusselvitykseen liittyvästä tietojenkäsittelystä.
Olen saanut tiedon, että osana turvallisuusselvitystä minua voidaan tarvittaessa haastatella.
Olen saanut tiedon oikeudesta saada tietoja turvallisuusselvityksen sisällöstä.
Olen saanut tiedon turvallisuusselvityksen sekä luotettavuuden seurannan tarkoituksesta ja käytöstä.
Annan suostumukseni henkilöturvallisuusselvityksen tekemiselle sekä siihen liittyvälle luotettavuuden seurannalle ja tietojenhankinnalle.
Annettu suostumus kattaa kaikki tilanteet palvelusuhteen tai tehtävän aikana sekä kaikki saman hallinnonalan tehtävät.

Vakuutan antamani tiedot oikeiksi ja annan suostumukseni niiden tarkistamiseen. Allekirjoituksellani vahvistan lukeneeni ja hyväksyväni yllaolevat kohdat.

Paikka ja päiväys	Allekirjoitus

E. Hakemuksen liitteet

- ☐ Passin henkilötietosivuja ____kpl (jos selvityksen kohteella ulkomaan kansalaisuus)
- ☐ Nimikirjaote tai muu selvitys koulutuksesta ja virka- ja työsuhteista (tarvitaan perusmuotoiseen ja laajaan turvallisuusselvitykseen)
- ☐ Laajan henkilöturvallisuusselvityksen henkilötietosivu (Laajaa henkilöturvallisuusselvitystä haettaessa tulee hakemukseen liittää tai erikseen toimittaa lain 28 §:ssä tarkoitettu henkilötietolomake . Lomake on saatavilla erikseen pyydettäessä).
- ☐ Laajan henkilöturvallisuusselvityksen kohteen läheisen henkilöturvallisuusselvityshakemuksia ____ kpl
- ☐ Ulkomaan viranomaisen myöntämä todistus (26 § 1 Mom)
- ☐ Muu, mikä?

F. Viranomaisen merkintöjä

Selvityksen nro	☐ Turvallisuusselvitystä ei tehdä (10 §)
☐ Turvallisuusselvitys tehdään suppeana	☐ Turvallisuusselvitys tehdään perusmuotoisena ☐ Haastatellaan

☐ Turvallisuusselvityksen antamisen yhteydessä työnantajaa pyydetään kiinnittämään huomiota tarpeeseen toteuttaa 17 §:n 2 momentin 4 kohdassa tarkoitettuja toimenpiteitä:

- ☐ Huumausainetestiä koskeva todistus
- ☐ Luottotietojen hankkiminen
- ☐ Lääkärintarkastuksen suorittaminen

☐ Laajan henkilöturvallisuusselvityksen kohteen läheisestä tehdään perusmuotoinen henkilöturvallisuusselvitys (erillinen hakemuslomake)

Liite 9 Haastattelukysymykset, jotka lähetettiin sähköpostitse viranomaisille

Tervehdys!

Teen opinnäytetyötäkoskien Katakri 2015 - auditointityökalua, lopputyöni valmistuu tämän kuluvan kuukauden aikana ja haluaisin vähän syventää sitä.

Voisiko teidän organisaatiostanne sopiva henkilö vastata kysymyksiin koskien Katakri 2015 - auditointityökalua?

Työhön ei välttämättä tarvitse laittaa nimiä, jos niin haluatte. Ainoastaan ohjaavalle opettajalle tuon nimenne esiin niin halutessanne.

Saatte myös kopion opinnäytetyöstä halutessanne jotta voitte etukäteen tarkastaa omaa lausuntoanne tai haastattelua koskevan osuutenne.

Arvostaisin erittäin paljon kirjallista vastausta ja yleensä vastaamistanne, jos millään kiireltänne ehditte.

Kiitos vastauksistanne jo etukäteen!

Syksyisin terveisin,

Aki Roivainen
Laurea turvallisuuden tradenomi opiskelija

aki.roivainen@gmail.com
aki.roivainen@laurea.fi
040 41 22 671

---

1. Miksi oli tärkeää muodostaa Katakri 2015?

2. Mitkä ovat oleellisimmat muutokset Katakri toisen version ja Katakri 2015 - auditointityökalun välillä?

3. Millä tavalla riskienhallinta tulisi huomioida ja millä tavalla se tulisi toteuttaa Katakri 2015 - auditointityökalun käyttämisen yhteydessä?

4. Mikä on turvallisuusjohtamisen osion rooli Katakri 2015 - auditointityökalussa?

5. Mikä on Katakri 2015 - auditointityökalun ja VAHTIn keskinäinen roolijako nyt?

6. Mikä on Katakri 2015 - auditointityökalun käyttötarkoitus? Entä voisiko sitä käyttää muuhun tarkoitukseen, kokonaan tai osittain?

7. Lisätietokenttien, sekä liitteiden rooli Katakri 2015 - auditointityökalussa?

8. Mikä on onnistuneinta Katakri 2015 - auditointityökalussa?

9. Mikä vaatisi vielä kehittämistä Katakri 2015 - auditointityökalussa?

10. Muuta kommentoitavaa koskien Katakri 2015 - auditointityökalua?

11.Mikä on mahdollisesti edustamanne määrätyn turvallisuusviranomaisen tehtävät Katakri 2015 - auditointityökalun avulla auditoitaessa kohdetta?