Katakri 2020 auditointityökalun osa-alue I:n hyödyntäminen arvioitaessa yrityksen teknistä tietoturvallisuutta

Jonas Ekman

2022 Laurea

Laurea-ammattikorkeakoulu

Katakri 2020 auditointityökalun osa-alue I:n hyödyntäminen arvioitaessa yrityksen teknistä tietoturvallisuutta

Jonas Ekman

Tietojenkäsittely

Opinnäytetyö

Toukokuu, 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittelyn koulutus

(AMK)

Jonas Ekman

Katakri 2020 auditointityökalun osa-alue I:n hyödyntäminen arvioitaessa yrityksen teknistä tietoturvallisuutta

Vuosi 2022 Sivumäärä 37

Tämän opinnäytetyön tarkoituksena oli tutustua Katakri osa-alue I:n asettamiin turvallisuusvaatimuksiin, ja tuottaa näihin vaatimuksiin perustuvan käytännön ohjeen uusille työntekijöille. Toimeksiantaja KPMG oli ottamassa käyttöön uusinta versiota Katakrista, ja varsinaista käyttöohjetta työkalulle ei ollut. Käyttöohje koettiin tarpeelliseksi, niin uusien työntekijöiden perehdyttämiseen, kuin yhtenäisten prosessien varmistamiseksi.

Opinnäytetyössä katsottiin Katakria yleisesti ja osa-alue I:n sisältämiä vaatimuksia tarkemmin. Näiden lisäksi katettiin tietojen turvallisuusluokittelua, arviointimenetelmiä, sekä perehdyttiin teoriaan käyttöohjeen kirjoittamisesta. Työn merkittävimpinä lähteinä toimi Ulkoministeriön ja Liikenne- ja Viestintäviraston tuottama materiaali.

Kehittämistehtävässä tutustuttiin Katakri 2020 – työkaluun kirjallisen materiaalin, osallistuvan havainnoinnin, sekä haastatteluiden avulla. Kattavan perehtymisen jälkeen suunniteltiin käyttöohjeen rakenne, huomioiden kaikki tarpeelliset ja tärkeimmät näkökulmat ja toimenpiteet.

Käyttöohjeen sisällön kirjoittaminen osoittautui arvioitua pidemmäksi prosessiksi. Vaikka käyttöohjeen sisältö ei täysin valmistunut opinnäytetyöprosessin aikana, suunniteltiin rakenne ja hankittiin kattavasti taustamateriaalia käyttöohjeen viimeistelyyn. Käyttöohje tulee täyttämään työlle asetetut tavoitteet ja on hyödyllinen toimeksiantajalle. Ennen kaikkea kehittämistyö on auttanut opinnäytetyön kirjoittajaa perehtymään aiheeseen, tuoden varmuutta juuri alkaneeseen työsuhteeseen.

Asiasanat: katakri, tietoturva, arviointi, käyttöohje

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology

Bachelor's thesis

Jonas Ekman

How to utilize Katakri 2020 subdivision I when assessing a company's information security

Year 2022 Pages 37

The purpose of this thesis was to discuss security requirements set by Katakri subdivision I, and to produce a practical guide based on these requirements for new employees. The commissioner of the thesis, KPMG, was about to start utilizing the latest version of Katakri, and proper instructions were lacking. There was a need for an induction manual, as much for new employees, as to ensure consistent processes.

In the thesis, Katakri was overlooked generally, and subdivision I more specifically. In addition to the aforementioned, the thesis covered security levels, audit procedures, and introduced theory regarding writing instructions. The most significant sources were material produced by the Ministry for Foreign Affairs and the Finnish Transport and Communications Agency.

During the development work the Katakri 2020 tool was examined through written material, participative observation, and interviews. After comprehensive studies, the structure of the induction manual was designed, considering all necessary and most important point of views and procedures.

Writing the contents of the induction manual turned out to be a longer process than estimated. Even though the contents of the induction manual were not finished during the thesis process, the structure was designed, and comprehensive background material was gathered to finish the induction manual. The induction manual will meet the objectives set and benefit the commissioner. The development work helped the writer of this thesis foremost to become acquainted with the subject, thus bringing confidence to a new employment relationship.

Keywords: katakri, information security, assessment, instructions

Sisällys

1 Johdanto

Tämän opinnäytetyön tarkoituksena oli perehtyä Katakri 2020 – työkalun I-osa alueeseen, ja luoda toimeksiantajan sisäiseen käyttöön ohjeet työkalun käyttöön. Opinnäytetyötä kirjoittaessa tietoturvallisuusalalla tapahtuu paljon, ja informaatio- ja kyberturva on tärkeämpi kuin koskaan. Lehdissä puhutaan kybersodista, ja myös Suomen valtiota vastaan tapahtuu hyökkäyksiä, muun muassa palvelunestohyökkäyksiä. Opinnäytetyön aihe voidaankin pelkästään tämän takia katsoa ajankohtaiseksi ja erittäin tärkeäksi.

Käyttöohjeen sisältö on luokiteltu yksinomaan toimeksiantajan sisäiseen käyttöön. Alla tullaan kuitenkin esittämään Katakri 2020 – työkalun sisältö, pääpainon asettuen osa-alue I:hin, eli tekniseen tietoturvallisuuteen. Itse työkalun lisäksi selostetaan arviointiprosessit, sekä Suomessa käytössä olevat tiedon turvallisuusluokat.

Lopullisessa käyttöohjeessa pyrittiin huomioimaan sekä uutta työntekijää, että jo pidempään alalla ja mahdollisesti työkalun aikaisempia versioita käyttäneen tarvetta käyttöohjeelle. Käyttöohjeessa vältettiin käyttämästä liian teknistä sanastoa, jotta uudet työntekijät ymmärtävät sisällön, ja pystyvät helposti omaksumaan työkalua. Samalla sisällytettiin kaikki oleellisemmat osat, jotta käyttöohje on hyödyllinen jo pidemmän ajan työkalua käyttäneille. Koska Katakrista julkistaan aika ajoin uusia versiota, haluttiin käyttöohje pitää myös helposti päivitettävänä, uusien versioiden julkaisujen myötä.

2 Työn lähtökohdat

Tämän opinnäytetyön toimeksiantaja oli KPMG, jossa opinnäytetyön tekijä oli juuri aloittanut työskentelyn. KPMG:n neuvontapalveluiden työssään käyttämän työkalun Katakrin viimeisintä versiota oltiin ottamassa käyttöön, ja tämän version tarkempi käyttöohje uupui. Uusien työntekijöiden perehdyttämisen helpottamiseksi, sekä työkalun käytön yhtenäistämisen vuoksi, käyttöohje koettiin tarpeelliseksi. Tästä syntyi luonnollinen ja hyödyllinen opinnäytetyön aihe, josta hyötyi sekä toimeksiantaja että opinnäytetyön tekijä.

2.1 Kehittämiskohteen kuvaus

Tietoturvaan ja kyberturvaan liittyviä standardeja, sertifiointeja, säädöksiä ja niin edelleen, löytyy useampia, niin kansallisia kuin kansainvälisiä. Yksi tärkeä työkalu varsinkin viranomaisten näkökulmasta, on Katakri. Katakri on auditointityökalu, johon on koottu erilaisiin säädöksiin ja velvoitteisiin perustuvia vähimmäisvaatimuksia. Katakrin neljäs versio, Katakri 2020, on ollut Suomen ulkoministeriön kansallisen turvallisuusviranomaisen perustaman alatyöryhmän vastuulla, jossa on ollut edustettuna sekä viranomaisia, että yrityksiä. Katakri 2020 osa-alue I, jonka ympärille kehittämistyön käyttöohje rakentuu, kattaa teknisen tietoturvallisuuden.

Katakri auditointityökalua käytetään muun muassa toimeksiantajan neuvontapalveluissa. Jotta KPMG työnantajana voi varmistua siitä, että heidän asiakkaansa saavat tasalaatuista, luotettavaa, sekä ammattimaista palvelua, riippumatta neuvonantajasta, käyttöohje koettiin tarpeelliseksi.

2.1.1 KPMG

KPMG International Limited, tuttavallisemmin ja jatkossa käytettävä KPMG, on kansainvälinen yritys, joka tuottaa erinäisiä palveluita. KPMG on yksi ”The Big Four” – yrityksistä, eli yksi maailman isoimmista tilintarkastustoimistoista. Muut kolme ovat Deloiette, PwC sekä Ernst & Young. Globaalisti KPMG:llä on yli 236 000 työntekijää, ja pelkästään Suomessa ja Virossa yli 1 500 työntekijää. Yritys toimii 145 maassa, Suomessa 21 paikkakunnalla, Virossa kahdessa (KPMG 2022).

KPMG:n tärkein palvelu asiakkailleen on tilintarkastuspalvelut, sekä vero- ja lakipalvelut. Näiden lisäksi yritys tuottaa erinäisiä neuvontapalveluita, kuten yritysjärjestelyitä, liikkeenjohdon konsultointia, digitalisointia sekä tietoturvapalveluita, mihin tässä kehitystyössä keskitytään (KPMG 2022).

On tärkeää huomata, että sertifiointi- ja tarkastuslaitoksena toimii KPMG IT Sertifiointi Oy, joka on riippumaton ja puolueeton (KPMG IT Sertifiointi Oy Palvelukuvaus 2021, 4). Sertifiointilaitos käyttää kuitenkin arvioinneissaan KPMG Oy Ab:n asiantuntijoita, erityisesti teknisinä asiantuntijoina (KPMG IT Sertifiointi Oy Palvelukuvaus 2021, 8). Tämän vuoksi tässä työssä käytetään KPMG Oy Ab:lle ja KPMG IT Sertifiointi Oy:lle yhteistä nimitystä, KPMG.

2.1.2 Tietoturvallisuuden arviointilaitokset

Liikenne ja viestintävirasto hyväksyy tietoturvallisuuden arviointilaitokset. Jotta arviointilaitos voi saada hyväksynnän, tulee se täyttää seuraavat ehdot (Laki tietoturvallisuuden arviointilaitoksista 1405/2011):

1) Arviointilaitos on riippumaton arvioinnin kohteesta
2) Arviointilaitoksen henkilökunta omaa tarpeellisen koulutuksen, sekä riittävän kokemuksen
3) Arviointilaitoksella on käytössään tarpeelliset laitteet, välineet ja järjestelmät
4) Arviointilaitoksen vastuuhenkilöt ovat luotettavia, ja arviointilaitoksella on käytössää luotettava ja valvottu menetelmä, millä varmistetaan tilojen sekä tietojenkäsittelyn turvallisuus
5) Arviointilaitoksella on ohjeet toimintaa ja seurantaa varten

Tätä opinnäytetyötä kirjoittaessa, KPMG:n sertifiointilaitoksella on pätevyys suorittaa arvioinnit Katakri 2015 – versiota vasten. Ainoa arviointilaitos, jolla on Katakri 2020:n pätevyys, on Nixu Certification Oy. (Kyberturvallisuuskeskus 2022.) Kuvioon 1 on koottu arviointilaitokset, jotka ovat hyväksytty arvioimaan Katakri 2015 ja Katakri 2020 vasten. Kuviossa on hyvä huomioida, että aikaisemmin on turvallisuusluokan (TL) tilasta käytetty sanaa suojaustasoa (ST).

Päätös annettu	Arviointilaitos	Pätevyysalue
8.7.2021	Nixu Certification Oy	Katakri 2020, TL IV ja III
25.6.2019	Nixu Certification Oy	VAHTI, ST IV KATAKRI 2015, ST IV ja III ISO/IEC 27001:2013, ST IV
28.8.2017	KPMG IT Sertifiointi Oy	VAHTI, ST IV KATAKRI II, ST IV KATAKRI 2015, ST IV ja III ISO/IEC 27001:2013, ST IV

Kuvio 1: Katakri 2015 & 2020 hyväksytyt arviointilaitokset (tiedot: Kyberturvallisuuskeskus 2022)

2.2 Kehittämistavoitteet

Työn tavoitteena oli tuottaa laadukas ja toimiva käyttöohje Katakri 2020 – arviointityökalun käyttämisestä. Käyttöohjetta voidaan käyttää niin asiakasyritysten neuvontapalveluissa kuin uusien työntekijöiden perehdyttämisessä. Käyttöohje perustuu pitkälti Kansallisen turvallisuusviranomaisen julkaisemaan materiaaliin ja itse työkaluun, mutta myös toimeksiantajan nykyisiin Katakrin aikaisempien versioiden toimintaohjeistuksiin, muihin materiaaleihin, sekä henkilökunnan haastatteluihin.

Uudella työntekijällä on organisaatiosta riippumatta paljon opittavaa. Kaikki voi olla uutta, niin työympäristö, työkaverit, kuin työtehtävä. Työnantajalla on jo työsuojelulainsäädännön puolesta vastuu perehdyttämisen järjestämiseksi (Perehdyttäminen ja työnopastus – Ennakoivaa työsuojelua 2013), ja on tietenkin luonnollista, että hyvällä perehdyttämisellä, hyötyy sekä työnantaja että työntekijä. Tämän kehitystyön yhtenä tavoitteena on varmistaa uusien työntekijöiden Katakri 2020 – työkalun oikeaoppinen käyttö. Käyttöohjeen avulla uusi työntekijä voi epäröidessään tarkistaa oikean menettelytavan.

Uusien työntekijöiden lisäksi tuotettavan käyttöohjeen on tarkoitus hyödyntää myös vanhoja työntekijöitä. Käyttöohje yhtenäistää toimintatapoja, joka varmistaa, että asiakasyritys saa laadukasta palvelua ja neuvontaa riippumatta työntekijästä.

Kehittämistyössä tärkeä huomioonotettava asia oli se, että sen tulee palvella eritasoisia ammattilaisia. Käyttöohjeen tulee olla tarpeeksi laaja, jotta se kattaa kaikki tarpeelliset näkökulmat ja kaikki työkalun sisältämät osuudet, unohtamatta helppolukuisuutta ja ymmärtäväisyyttä, jotta myös uudet työntekijät hyötyvät siitä. Koska vanhat työntekijät kuitenkin osaavat hyödyntää työkalua, oli tärkein kohderyhmä kuitenkin uudet työntekijät.

2.3 Aihealueen rajaus

Kansallinen turvallisuusauditointikriteeristö on laajempi kuin kehittämistyöhön otettu osuus. Kriteeristö on jaettu kolmeen osa-alueeseen, T, F ja I. Osa-alue T:n avulla varmistetaan, että kohdeyrityksellä on toimiva tietoturvallisuuden hallintajärjestelmä, sekä että menetelmät tietojen suojaamiseen ovat kunnossa. Osa-alue F kattaa fyysistä turvallisuutta, eli tietojen toimintaympäristöä.

Tässä kehittämistehtävässä keskitytään osa-alue I:hin. Kyseinen osa-alue kattaa kohdeyrityksen teknistä tietoturvallisuutta, sisältäen omat osuudet tietoliikennettä, tietojärjestelmiä, sekä käyttöturvallisuutta varten. Osa-alue I on sen verran laaja itsessään, että rajoitus pidettiin luontevana ja järkevänä.

2.4 Keskeiset käsitteet

Arviointi	Vaatimuksenmukaisuuden arviointi
Katakri	Kansallinen turvallisuusauditointikriteeristö
KPMG	Toimeksiantaja, yksi maailman isoimmista tilintarkastustoimistoista
NSA	Suomen Ulkoministeriön Kansallinen turvallisuusviranomainen
Sertifiointi	Arviointiin perustuvan todistuksen myöntämistä
SL	Suojaustaso (I, II, III, IV)
TL	Turvallisuusluokka (I, II, III, IV)
Traficom	Liikenne- ja viestintävirasto, Katakri osa-alue I:n toimivaltainen viranomainen

3 Katakri

Katakri, eli kansallinen turvallisuusauditointikriteeristö, on työkalu, jolla viranomainen voi varmistaa, että organisaatio suojaa turvallisuusluokiteltua materiaalia vaatimusten mukaisesti. Katakriin on koottu vaatimuksia, jotka perustuvat kansallisiin ja kansainvälisiin säädöksiin, velvoitteisiin sekä lakiin. Katakri itsessään ei siis aseta minkäänlaista vaatimusta, vaan kyseessä on kokoelma ja työkalu. Tärkeimpinä kansallisina lähteinä mainittakoon laki koskien julkisen hallinnon tiedonhallintaa, sekä Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa. Kansainvälisistä lähteistä on käytetty lähinnä Euroopan Unionin turvallisuussääntöjä. (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020. 2–6.) Katakri on rakenteeltaan kyselylomakkeen näköinen, luotu jotta yrityksen suojaustaso on helposti todennettavissa (Nykänen & Kärkkäinen 2014, 47).

Katakrin alkuperäinen tarkoitus oli yhtenäistää turvamenettelyjä, mahdollistaa omavalvontaa, sekä parantaa auditointeja. Viranomaisia ja yrityksiä haluttiin tukea kansainvälisissä toiminnoissa, tuoden yhtenäisemmän ja läpinäkyvämmän tietoturvakriteeristön. Ennen Katakrin käyttöönottoa, valittu tietoturvakriteeristö riippui viranomaisesta ja yrityksestä. (Experiences from development of security audit criteria 2017. 209.)

Ensimmäinen versio Katakrista valmistui 2009 osana hallituksen turvallisuusohjelmaa puolustusministeriön johdolla. Tämän jälkeen vastuu ylläpidosta ja kehityksestä siirrettiin sisäministeriölle, jonka johdolla Katakrin toinen versio valmistui vuonna 2011. Vuonna 2014 sisäministeriön työryhmä päätti, että päävastuu työkalusta siirtyy ulkoministeriössä toimivale Kansalliselle turvallisuusviranomaiselle, eli NSA:lle. NSA julkaisi kolmannen version 2015. (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020. 2–6.)

Katakrin neljäs versio, eli 2020, on ollut Suomen ulkoministeriön alaisen kansallisen turvallisuusviranomaisen perustaman alatyöryhmän vastuulla, jossa on ollut edustettuna useamman viranomaisen lisäksi myös yrityksiä (Kakakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020. 2). Vuoden 2015 versio Katakrista sisältää tietyiltä osin vanhaa tietoa, ja kaipasi täten päivitystä (Holopainen 2021). Uusimmassa versiossa onkin keskitytty vuoden 2020 alussa uudistuneeseen kansalliseen lainsäädäntöön, ja samalla huomioitu digitaalisen tietojenkäsittelyn kehitystä (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020. 2–6). Työkalun sisältöä ja käyttöä on myös pyritty selkeyttämään eri tavoin, kuten terminologiaa ja rakennetta (Holopainen 2021).

Katakri on jaettu kolmeen osa-alueeseen, jossa jokainen osa-alue keskittyy eri alueeseen, ja sisältää eri tarkistuskohteita. Osa-alue T kattaa turvallisuusjohtamista, osa-alue F kattaa Fyysistä turvallisuutta, ja osa-alue I kattaa teknistä tietoturvallisuutta. (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020. 5.)

3.1 Osa-alue T: Turvallisuusjohtaminen

Turvallisuusjohtamista koskevassa osa-alueessa toimivaltaisena viranomaisena ja NSA:n asiantuntijoina toimii Suojelupoliisi tai Pääesikunta. Kyseisessä osa-alueessa katsotaan miten turvallisuutta ja sen hallintaa käsitellään ja esitellään henkilöstölle kohdeyrityksessä, kattaen sekä hallinnollisen tietotuvan että henkilöstöturvallisuuden. Tavoitteena on, että kohdeyrityksellä on toimiva hallintajärjestelmä, ja pystyy varmistamaan, että henkilöstö käsittelee tietoja vaatimusten mukaisesti. (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020.)

3.2 Osa-alue F: Fyysinen turvallisuus

Fyysistä turvallisuutta koskevalla osa-alueella on samat toimivaltaiset viranomaiset sekä asiantuntijat kuin turvallisuusjohtamisessa, eli Suojelupoliisi tai Pääesikunta. Osa-alueessa tarkistetaan sekä fyysisiä että teknisiä turvatoimia, millä kohdeyritys pyrkii estämään luvattoman pääsyt tietoihin. Tämä sisältää myös sen, että tietoja on käsiteltävä ja säilytettävä paikassa, jossa tietojen luottamuksellisuus, eheys sekä saatavuus on varmistettu. (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020.)

3.3 Osa-alue I: Tekninen tietoturvallisuus

Kahdesta muusta osa-alueesta poiketen, teknistä tietoturvallisuutta koskevassa osa-alueessa toimivaltaisena viranomaisena toimii Liikenne- ja viestintävirasto, Traficom. Osa-alue on edelleen jaettu kolmeen osioon, tietoliikenne-, tietojärjestelmä-, sekä käyttöturvallisuuden osioihin. Osa-alueen sisältämillä vaatimuksilla on tarkoitus varmistaa sähköisen tiedon turvallisuusjärjestelyjen riittävyys. (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020.)

Teknistä tietoturvallisuutta ylläpitämisessä täytyy muistaa, että muutokset tai lisäykset tietojenkäsittely-ympäristössä myös vaikuttavat turvallisuuteen. Täten onkin välttämätöntä, että muutosten myötä, myös käytänteet ja asetukset varmistetaan, jotta varmistutaan että kokonaisuus on kunnossa (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. 63–64). Tommi Viitanen osaltaan muistuttaa Kauppalehden Digian tuottamassa kumppanisisällössä, että yrityksen tietoturva ei tule koskaan olemaan valmis, vaan järjestelmät ja uhat muuttuvat. Kuten moni muu asia yritystoiminnassa, vaatii myös tietoturva jatkuvaa huomiota. (Digia 2021.)

Teknisen tietoturvallisuuden sisältämä osiot ovat jaoteltu tarkastuskohteittain. Työkalun jokainen tarkastuskohde sisältää kyseiselle kohteelle asetetut vaatimukset, sekä lisätiedot. Lisätietojen alta löytyy yleistä tietoa tarkastuskohteesta, kuten vaatimuksen tarkoitus, odotukset, sekä toteutusesimerkkejä eri turvallisuusluokille. (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020.) Seuraavasti esitetään työkalua suppeammin työkalun teknisen tietoturvallisuusosion sisältämät vaatimukset, työkalun otsikot ja vaatimukset ovat esitetty liitteessä 1.

3.3.1 Tietoliikenneturvallisuus

Tietoliikenne on langallista tai langatonta tiedonvälitystä, jossa osapuolina voi olla sekä ihmisiä tai laitteita (Elisa 2022). Tietoliikenneturvallisuutta koskevassa osiossa tarkistetaan, että tiedonvälitykseen liittyvät asiat ovat vaatimusten mukaiset. Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille – dokumentin (2020, 65–74) mukaisesti tarkastuskohteina ovat:

- Tietoliikenneverkon rakenne. Turvallisuusluokitellun tiedon täytyy olla eristetty muista ympäristöistä.
- Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt. Tietoliikenneverkon tulisi olla segmentoitu, esimerkiksi palvelimet omaan vyöhykkeeseen ja työasemat omaansa, ja jossa liikenne näiden välissä suodatetaan ja rajoitetaan tarpeellisuuden mukaan.

- Suodatus- ja valvontajärjestelmien ylläpito. Asetukset ja dokumentaatio tulee ylläpitää koko elinkaaren ajan.
- Hallintayhteydet. Hallintayhteyksien suojauksista tulee huolehtia, esim. rajaamalla yhteydet turvallisuusluokittain.
- Langaton tiedonsiirto. Langaton tiedonsiirto tulee salata viranomaisen hyväksymällä menetelmällä.

3.3.2 Tietojärjestelmäturvallisuus

Tietojärjestelmä on eri osista, kuten ihmisistä, laitteistosta ja ohjelmistoista, koostuva järjestelmä, eli kokonaisuus (Peda.net 2022). Luonnollisesti, tämä osio kattaa näitä kaikkia osia, tarkastuskohteina ollessa (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020, 75–93):

- Pääsyoikeudet. Pääsyoikeuksia hallinnoidaan jatkuvasti, ja oikeudet myönnetään tarpeen mukaan.
- Ympäristöön liitettyjen osapuolten tunnistaminen. Kaikki liitetyt ja ympäristöä käyttävät osapuolet tulee tunnistaa luotettavasti.
- Järjestelmäkovennus. Varmistetaan että vain oleelliset palvelut ja toiminnot ovat päällä, samalla huolehditaan salasanoista ja päivityksistä.
- Haittaohjelmasuojaus. Huolehditaan että ympäristössä on asianmukainen haittaohjelmamenettely.
- Tapahtumien jäljitettävyys. Tietojen muutoksista ja käytöstä on kerättävä tarpeelliset lokitiedot.
- Poikkeamien havainnointi. Varmistetaan että mahdolliset hyökkäykset huomataan, ja rajoitetaan niiden vaikutukset.
- Salaus. Salausratkaisut tulee olla viranomaisen hyväksymiä.
- Ohjelmistojen suojaus. Varmistettava että käytettävät ohjelmistot ovat turvalliset, niin toteutus, integrointi muihin järjestelmiin ja tietoihin, kuin konfigurointi.
- Hajasäteily ja elektroninen tiedustelu. Ympäristö on suojattava tahattomia sähkömagneettisia vuotoja vasten, sekä pienennettävä elektronisen tiedustelun riskejä.

3.3.3 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan nimen mukaisesti tietojen turvallista käyttöä. Osiossa käydään läpi seuraavat kohteet (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020, 94–106):

- Tietojen sähköinen välitys. Jos turvallisuusluokiteltua tietoa siirretään suojatun turvallisuusalueen ulkopuolelle, tulee ensinnäkin varmistua salauksesta, sekä toisekseen varmistua, että vastaanottaja tunnistetaan ennen kuin taho pääsee käsiksi tietoihin.

- Muutoshallinta. Tietojenkäsittelyn turvallisuutta ylläpidetään koko elinkaaren ajan, tarkoittaen arviointeja ja tarkastuksia, sekä turvallisuusasiakirjojen päivitystä.
- Fyysinen turvallisuus. Varmistetaan missä ja miten turvallisuusluokiteltua tietoa käsitellään.
- Etäkäyttö ja etähallinta. Tarkistetaan miten tietoja ja järjestelmiä voidaan käyttää etänä.
- Ohjelmistohaavoittuvuuksien hallinta. Ohjelmistohaavoittuvuuksia hallitaan koko ympäristön elinkaaren ajan.
- Varmuuskopiointi. Varmuuskopiot tulee suojata alkuperäisten tietojen vastaavalla suojausmenetelmällä.
- Sähköisten turvallisuusluokiteltujen tietojen tuhoaminen. Tiedot tulee tuhota luotettavasti, ja tarvittaessa todistettavasti.

4 Katakri arvioinnin ja hyväksynnän vaiheet

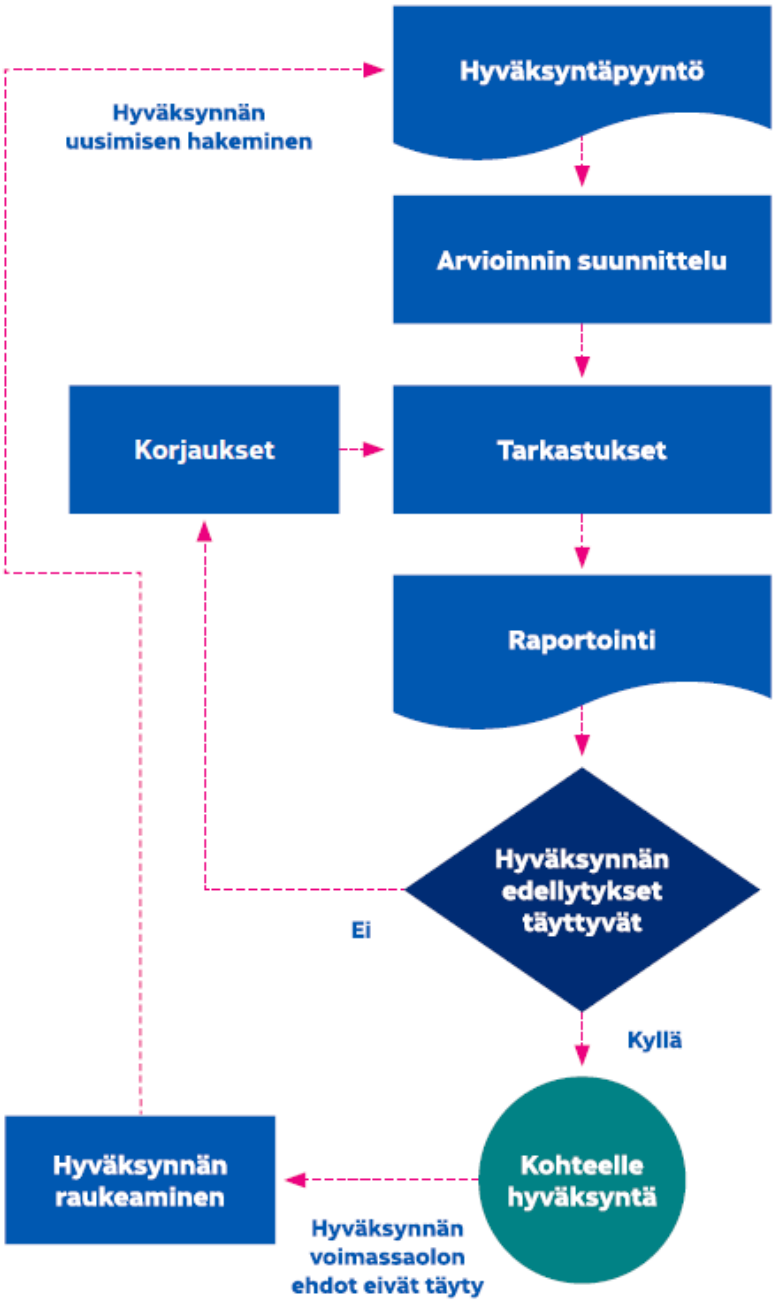
Tietoturvallisuuden arvioinnit arviointilaitoksissa aloitetaan aina ensin toimeksiannolla. Arviointilaitos laatii kirjallisen sopimuksen toimeksiantajan kanssa, johon kirjataan ainakin arvioinnin kohde, mahdolliset rajaukset, arviointiperuste sekä käytettävä kriteeristö, turvallisuusluokka, laajuus sekä kesto, raportti sekä muu aineisto, ja maksu. Toimeksiannon jälkeen arviointi aloitetaan havainnoimalla yleistilannetta, ja katselmoidessa saatavilla olevia asiakirjoja.

Arviointi jatkuu asiakkaan toimitilassa tehtävällä teknisellä tarkastuksella. Tehdyistä arvioinneista ja tarkastuksista laaditaan ISO/OEC 17021 ja ISO/IEC 27006 standardeiden mukainen arviointiraportti, jonka liitteeksi tulee Katakrin vaatimustaulukko tuloksineen sekä perusteluineen. Arviointilaitokset käyttävät raporteissaan pohjana Liikenne- ja Viestintäviraston toimittamaa raporttipohjaa. Jos arvioinnin kohteena olleen toimitila ja toiminta täyttää asetettuja vaatimuskriteerit, annetaan kohteelle arvioinnista todistus. Jos arvioinnissa havaitaan puute, todistusta ei anneta. (Ohje tietoturvallisuuden arviointilaitoksille 210/2016 O 2020.)

Arviointiprosessi Liikenne- ja Viestintäviraston tekemissä arvioinneissa on pitkälti sama, kuin arviointilaitoksien tekemissä arvioinneissa. Arviointilaitoksien arvioinnit rajautuvat turvallisuusluokkiin IV ja III, tätä korkeammat turvallisuusluokat vaativat Liikenne- ja Viestintäviraston tekemää arviointia. Ennen Liikenne- ja Viestintäviraston antamaa todistusta arviointilaitoksen tekemästä arvioinnista, on Liikenne- ja Viestintävirastolla oikeus ja mahdollisuus, suorittaa tarkentavaa arviointia kohdeyritykseen. (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020, 111–113). Kuviossa 2 nähdään arviointilaitoksien arviointiprosessi, ja kuviossa 3 Liikenne- ja Viestintäviraston hyväksyntäprosessi. Kuten mainittu, ovat prosessit melko samanlaiset.

Kuvio 2: Arviointilaitoksen arviointiprosessi (Ohje tietoturvallisuuden arviointilaitoksille 210/2016 O 2020, 16)

Jos asiakasyrityksellä on Liikenne- ja Viestintäviraston tai arviointilaitoksen aikaisemmin tehdystä arvioinnista raportti, jonka mukaan Katakrissa esitetyt vaatimukset täyttyvät, uutta arviointia ei välttämättä tarvita, ja todistus voidaan myöntää. Todistuksen yhteydessä asiakasyrityksen tulee sitoutua säilyttämään tietoturvallisuustason. (Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit – Tilaajaorganisaatio näkökulma. 2021).



Kuvio 3: Viranomaisen hyväksyntäprosessi (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020, 112)

5 Turvallisuusluokittelu

Kansallisen turvallisuusviranomaisen NSA:n tuottamassa Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohjeessa kuvataan turvallisuusluokitellun tiedon käsittelyä (2020, 4). Kansainvälisellä turvallisuusluokitellulla tiedolla tarkoitetaan aineistoa, jota on kansainvälisen sopimuksen tai EU:n turvallisuussääntöjen mukaan suojattava. Velvoitteet koskevat viranomaisia sekä yrityksiä, jotka käsittelevät turvallisuusluokiteltua tietoa. Nämä kansainväliset vaatimukset ovat myös huomioitu Katakrissa. (Kansainvälisen turvallisuusluokittelun tietoaineiston käsittelyohje 2020, 5–6).

Turvallisuusluokiteltua tietoa käsiteltäessä tiedolle on myös asetettu turvallisuusluokka. Turvallisuusluokkia on yhteensä neljä, ja niiden nimet riippuvat käyttöpaikasta. Suomessa käytetään yksinkertaista nimeämiskäytäntöä, eli turvallisuusluokka lisättynä numerolla yhdestä neljään, numero yhden ollessa tiukin turvallisuusluokka. (Kansainvälisen turvallisuusluokittelun tietoaineiston käsittelyohje 2020). Kuviossa 4 esitetään Suomen turvallisuusluokittelun Euroopan unionin sekä Naton vastaavat luokat. Muiden kansainvälisten tahojen kanssa tietoja vaihtaessa tehdään sopimus, jossa määritetään muun muassa tietotuvallisuusluokkien vastaavuudet (Kansainvälisen turvallisuusluokittelun tietoaineiston käsittelyohje 2020, 23).

Suomen turvallisuusluoka	**Euroopan unionin vastaava**	**Naton vastaava**
Erittäin salainen (TL I)	EU Top Secret	Cosmic Top Secret
Salainen (TL II)	EU Secret	Nato Secret
Luottamuksellinen (TL III)	EU Confidential	Nato Confidential
Käyttö rajattu (TL IV)	EU Restricted	Nato Restricted

Kuvio 4: Turvallisuusluokitus (tiedot: Kansainvälisen turvallisuusluokittelun tietoaineiston käsittelyohje 2020)

Euroopan unionin aineiston käsittelyn yleisten periaatteiden mukaan tiedot tulee suojata koko tiedon elinkaaren ajan. Mitä korkeampi turvallisuusluokka, sitä tiukemmat turvatoimet vaaditaan. Turvatoimet vaikuttavat muun muassa tietojen tuottamiseen, kopioimiseen, kuljettamiseen, säilyttämiseen ja tuhoamiseen. (Kansainvälisen turvallisuusluokittelun tietoaineiston käsittelyohje 2020, 7.)

Katakrin sisältämillä vaatimuksilla on tarkoitus varmistaa riittävät turvallisuusjärjestelyt turvallisuusluokitellun aineiston käytössä. Katakrin tarkastuskohteiden vaatimuksissa mainitaan hyväksytty toteutustapa turvallisuusluokittain. (Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille 2020, 63–64).

6 Ohjeen kirjoittaminen

Kotimaisten kielten keskuksen mukaan onnistunut ohje seuraa kolme asiaa. Kirjoittaessa tulisi käyttää käskymuotoa, tunnistaa olennaisimmat tiedot, sekä esittää ohjeet ymmärrettävässä muodossa. (Kotimaisten kielten keskus 2022).

Jane Campanizzi kirjoittaa Effective Writing for the Quality Professional kirjassaan (2005, 93), että hyvin kirjoitetut ohjeet vähentävät virheet ja hukatun ajan. Ohjeita kirjoittaessa tarkoituksena on tuottaa selkeät kuvaukset, jotta ohjeiden lukija osaa suorittaa tehtävän itsenäisesti. Prosessi aloitetaan suunnittelemalla, esimerkiksi suorittamalla tehtävä itse, seuraamalla muita tekemässä tehtävää, tai haastattelemalla. Samalla voidaan myös tarkastaa tehtävään liittyviä aikaisempia materiaaleja, kuten käytäntöjä. Suunnitteluvaiheessa tulee myös huomioida kohderyhmä ja heidän asiantuntijuutensa asiassa. (Campanizzi 2005, 93–94).

Ohjeet rakentuvat useimmiten kolmesta osasta, johdannosta, sisällöstä, ja johtopäätöksistä. Tärkeää on myös kirjoittamisen jälkeen arvioida ohjeita, mieluiten testaamalla. Jos se ei ole mahdollista, pyytämällä jonkun lukemaan ohjeita, ja antamaan palautetta. (Campanizzi 2005, 94–103).

7 Kehittämismenetelmät

Opinnäytetyö toteutettiin kehittämistyönä, käyttäen laadullisia, eli kvalitatiivisia menetelmiä. Laadullisissa menetelmissä on tarkoitus hankkia vähäisistä lähteistä mahdollisimman paljon tietoa, ja tällä tavalla ymmärtää asiaa paremmin (Ojasalo, Moilanen & Ritalahti 2015, 105). Koska julkista ja ajantasaista materiaalia aiheesta on melko rajallisesti, pidettiin kvalitatiivista lähestymistapaa parhaimpana. Teoria perustuukin lähinnä Suomen Ulkoministeriön sekä Liikenne- ja viestintäviraston tuottamaan materiaaliin sekä itse työkaluun. Edellä mainittujen lähteiden lisäksi kehitystyössä hyödynnettiin KPMG:n aikaisempia ohjeita sekä materiaaleja, sekä nykyisten työntekijöiden tiedot sekä taidot. Samalla mainittakoon, että opinnäytetyön tekijä oli uusi työntekijä alalla sekä yrityksessä, jota pystyttiin hyödyntämään, ajatellen uuden työntekijän perehtymistä.

7.1 Kirjallinen materiaali

Koska kehittämistyön lopputuotteen oli työkalun käyttöohje, käytettiin luonnollisesti itse työkalua pohjana. Muita kirjallisia materiaaleja, eli dokumentteja, analysoitiin dokumenttianalyysia hyödyntäen. Ojasalon, Moilasen ja Ritalahden (2015, 136) mukaan dokumenttianalyysin tavoitteena on luoda selkeä kuvaus kehitettävästä asiasta. Dokumenttianalyysia käytettäessä, saatiin käyttöohjeeseen viranomaisten niin kutsuttujen virallisten materiaalien lisäksi myös KPMG:n jo olemassa olevia ohjeita sisällettyä. KPMG:n tuottamasta materiaalista

pyrittiin etsiä ja tunnistaa olennaiset kohdat, sisällön analyysilla (Ojasalo, Moilanen & Ritalahti 2015, 137).

7.2 Havainnointi

Ojasalo, Moilanen ja Ritalahti (2015, 114) sanoo että havainnointi on hyvä tapa saada tieto siitä mitä tapahtuu luonnollisessa toimintaympäristössä, ja että havainnointia voidaan käyttää haastattelun tukena. Osallistuvassa havainnoinnissa tutkija pyrkii osallistumaan toimintaan, tutkittavien ehdoilla (Hirsijärvi, Remes, Sajavaara 2010, 216).

Havainnointi suoritettiin omaan työtehtävään perehdyttäessä. Työtehtävä oli uusi, mitä voitaisiin mieltää hankaloittavaksi ja hidastavaksi asiaksi, mutta koska opinnäyteyön tekijä oli ennestään perehtynyt Katakri – työkaluun, onnistui havainnointi suunnitellusti. Osallistuva havainnointi olikin kirjallisten lähteiden lisäksi tärkein ja hyödyllisin käytetty kehittämismenetelmä.

7.3 Haastattelut

Dokumenttianalyysin ja osallistuvan havainnoinnin lisäksi hyödynnettiin haastatteluita. Haastatteluiden odotettiin tuovan lisäarvoa, varsinkin parhaiden menetelmien löytämisessä. Haastattelut päätettiin suorittaa osallistuvan havainnoinnin yhteydessä, menetelmänä teemahaastattelu.

Hirsijärven, Remeksen ja Sajavaaran (2010, 205) mukaan haastattelu menetelmänä valitaan usein esimerkiksi sen takia, että aihe tuottaa monitahoisia vastauksia, halutaan selventää vastauksia, tai halutaan syventää saatavia tietoja esimerkiksi kysymällä lisätietoja. Koska tarkoitus oli löytää työntekijöiden parhaimmat menetelmät sekä saada mahdollisimman paljon tietoa työkalun käytöstä, haastattelut olivat luonteva menetelmä.

Teemahaastattelu valikoitui haastattelumenetelmäksi sen välimuodon vuoksi. Teemahaastatteluissa on tyypillistä, että haastatteluaiheet ovat selvät ennen haastattelua, mutta muoto ja järjestys voi vaihdella. Koska haastatteluista toivottiin syventäviä vastauksia, lomakehaastattelu ei pidetty soveltuvana, lomakkeen ollessa täysin ennalta määrätty. Avoin haastattelu puolestaan vaatii paljon asiantuntemusta haastattelijalta, mitä ei voida odottaa uudelta työntekijältä alalla. (Hirsijärvi, Remes & Sajavaara 2010, 208–209). Haastatteluita varten pohja sekä runko haluttiin valmistaa ennen haastattelua, jotta tärkeimmät tulee läpikäytyä. Haastattelut kuitenkin käytiin avoimesti ja keskustellen, jolloin teemahaastattelu pidettiin parhaiten sopivana.

7.4 Reliabiliteetti ja validiteetti

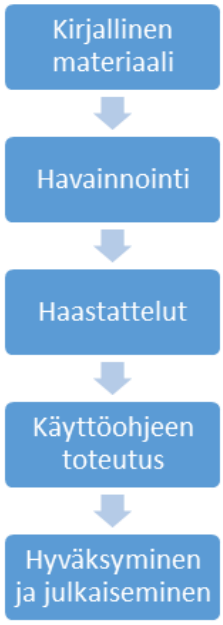
Tutkimuksen reliabiliteettia, eli luotettavuutta, voidaan todeta eri tavoin. Jos esimerkiksi kaksi tai useampi tutkimus päättyy samaan lopputulokseen, voidaan tutkimus pitää luotettavana. Reliabiliteetilla tarkoitetaankin toistettavuutta. (Hirsijärvi, Remes & Sajavaara 2010, 231).

Validiteetti, eli pätevyys, tarkoittaa sitä, että valitut tutkimusmenetelmät mittaavat sitä mitä tutkijan on tarkoitus mitata. Jos esimerkiksi haastateltava ymmärtää esitetyt kysymykset eri tavoin kuin tutkija on tarkoittanut, ja tutkija kuitenkin analysoi saamiaan vastauksia alkuperäisen suunnitelman mukaisesti, ei tutkimus välttämättä ole pätevä. (Hirsijärvi, Remes & Sajavaara 2010, 231–232).

Kvalitatiivisissa tutkimuksissa luotettavuutta ja pätevyyttä on tulkittu eri tavoin. Luotettavuutta kuitenkin parantaa tarkka ja selvä selostus tutkimuksen toteuttamisesta. Pätevyyttä voidaan niin kvantitatiivisissa kuin kvalitatiivissa tutkimuksissa parantaa käyttämällä tutkimuksissaan useampaa tutkimusmenetelmiä. Tärkeää kuitenkin on, että kaikkien tutkimusten luotettavuutta ja pätevyyttä pitää jollain tapaa pystyä arvioimaan. (Hirsijärvi, Remes & Sajavaara 2010, 232–233).

8 Kehittämistyön toteutus

Kehittämistyön tavoitteena oli tuottaa käyttöohje, joka yhtenäistää toimintaa, sekä helpottaa uusien työntekijöiden aloittamista työtehtävissään. Kehittämistyö toteutettiin viidessä vaiheessa. Ensimmäisessä vaiheessa tutustuttiin kirjalliseen materiaaliin, toisessa vaiheessa havainnoitiin, kolmannessa vaiheessa haastateltiin asiantuntijoita, neljännessä vaiheessa toteutettiin käyttöohje, ja lopuksi hyväksytettiin käyttöohje esimiehillä ja työkalua käyttävillä, ennen julkaisua. Kuviossa 5 on kuvattu kehittämistyön prosessi.



Kuvio 5: Suunniteltu prosessi kehitystyölle

8.1 Kirjallinen materiaali

Kuten sanottua, ensimmäisessä vaiheessa tutustuttiin kirjalliseen materiaaliin. Tässä vaiheessa käytettiin hyödyksi uuden työntekijän näkökulma, jotta se saatiin vahvasti mukaan lopulliseen käyttöohjeeseen. Kirjallinen materiaali sisälsi julkisesti saatavilla oleva materiaali, kuten työkalu itse, sekä Suomen Ulkoministeriön ja Liikenne- ja Viestintäviraston julkaisemat materiaalit. Varsinkin työkaluun tutustuttiin tarkoin, jotta työkalusta saatiin mahdollisimman kattavan kuvan heti alusta lähtien.

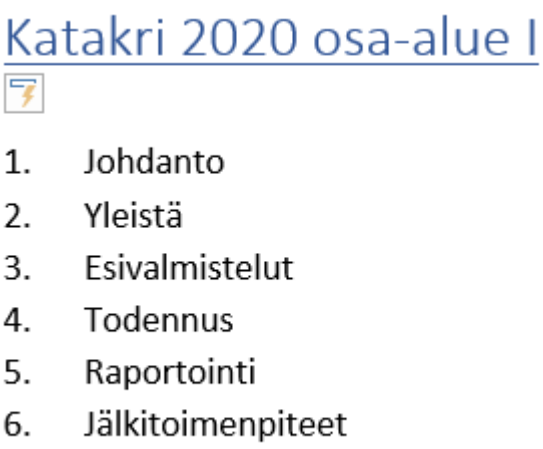
Näiden lisäksi, tutustuttiin myös KPMG:n sisäisiin materiaaleihin, sekä arviointilaitoksille ja arviointeja tekeville asetettuihin vaatimuksiin. KPMG:n sisäiset materiaalit käsittelivät lähinnä Katakri 2015 – versiota, johtuen luonnollisesti siitä, että kyseinen versio oli kirjoittamishetkellä käytössä oleva versio KPMG:llä. Katakri 2020 on kuitenkin pitkälti samansisältöinen kuin versio 2015, muutama poikkeus lukuun ottamatta. Uusimmassa versiossa muutama kohta osa-alue I:stä on siirretty osa-alue F:ään. Vaatimuksia edellä mainituille asettaa Suomen laki, toimeenpaneva viranomainen Liikenne- ja Viestintävirasto, sekä luonnollisesti KPMG itse.

8.2 Havainnointi

Toinen vaihe kehittämistyöstä käsitti havainnointia. Havainnointi suoritettiin suunnitelman mukaisesti, perehtymällä työkalun käyttöön asiantuntijan johdolla.

Perehtyminen aloitettiin käymällä läpi yleistä tietoa, miten KPMG:llä toimitaan, ja miten laki määrää, että arviointikohteet todennetaan. Tämä jälkeen siirryttiin työkalun käyttöön. Työkalun käyttöä harjoiteltiin osa osalta, käyden järjestelmällisesti läpi mitkä kaikki vaiheet todentamiseen kuuluu, ja miten vaatimusten täyttyminen todetaan.

Toisen vaiheen jälkeen tehtiin ensimmäinen luonnos käyttöohjeen sisältöluettelosta, ennen siirtymistä haastatteluihin. Luonnos toimitettiin myös tässä vaiheessa esimiehelle kommentointia varten. Esimies piti luonnosta hyvänä, joten sillä lähdettiin etenemään prosessissa. Sisältöluettelon ensimmäinen luonnos nähdään kuviossa 6.

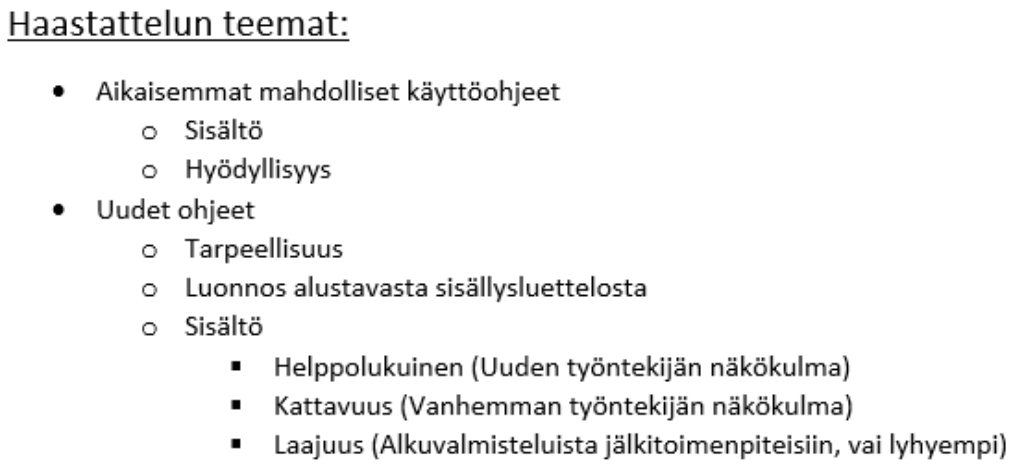


Kuvio 6: Ensimmäinen luonnos sisältöluettelosta

8.3 Haastattelut

Kirjallisten materiaalien ja havainnoinnin jälkeen siirryttiin haastatteluihin. Haastatteluiden toivottiin tuovan tarkennusta ja yleistä selvennystä työkalun käytöstä, sekä asiantuntijoiden näkemykset käyttöohjeen tarpeesta ja sen mahdollisesta sisällöstä.

Haastatteluihin valittiin rajallisesta määrästä asiantuntijoita kaksi, hieman eripituisilla Katakri – työkokemuksilla. Palvelusvuosia KPMG:llä toisella oli vähän yli vuoden, ja toisella lähes kuusi vuotta. Haastateltavien valinnassa pyrittiin saavuttamaan eri pituisten työkokemusten tuoman asiantuntijuustason. Kuviossa 7 nähdään haastatteluihin suunnitellut teemat.



Kuvio 7: Haastattelun teemat

Haastatteluista sovittiin hyvissä ajoin. Haastateltaville toimitettiin ennen haastatteluita luonnos käyttöohjeen sisällysluettelosta, sekä haastattelun teemat. Haastattelut aloitettiin käymällä läpi asiantuntijoiden nykyistä prosessia, sekä käyttämiään työkaluja. Tämän jälkeen keskusteltiin nykyisistä ohjeista, nykyisten ohjeiden puutteista, ja tarpeesta. Asiantuntijat olivat samaa mieltä siitä, että kirjallinen kattava ohje olisi hyödyllinen.

9 Kehittämiskohteen tulos

Kehitystyön prosessin aikana pyrittiin huomioimaan Jane Campanizzin kirjoitus ohjeen kirjoittamisesta. Vaikka kehitystyö rakentui viidestä osasta, sisälsi ne Campanizzin esiin nostetut asiat, eli suunnittelun, muiden seuraamisen suorittamassa tehtävää, haastattelut, ja tutustuminen aikaisempiin aiheeseen liittyviin materiaaleihin. Käyttöohjetta suunniteltiin lukemalla olemassa olevia materiaaleja, haastateltiin asiantuntijoita, ja käytettiin itse myös työkalua. Käyttöohjeen valmistuttua käyttöohje luetetaan asiantuntijoilla, ennen virallista julkaisua.

Kuten alla olevasta lopullisesta sisällysluettelosta näkyy (kuvio 8), muuttui rakenne hieman luonnoksesta. Alustavassa käyttöohjesuunnitelmassa ajatuksena oli jaotella käyttöohjeen otsikko 4. Todennus alaotsikoihin jokainen tarkistuskohde erikseen. Haastatteluissa asiantuntijoiden antamien näkemysten perusteella päätettiin kuitenkin, että luonnollisempi otsikointi ja jaottelu olisi työvaiheittain ja työkaluittain. Työkaluja käytettäessä ei luonnollisesti tarkisteta yhtä tarkistuskohdetta kerrallaan, vaan tietty skannaus tai testi voi vastata useampaan tarkistuskohteeseen yhdellä kertaa. Lopullinen sisällysluettelo pidettiin hyvänä ja järkevänä. Sisällysluettelon valmistuttua, oli helppo kirjoittaa myös sisältö.

Katakri 2020 osa-alue I

1. Johdanto
2. Esivalmistelut
3. Asiakasyrityksen haastattelu
4. Tekninen todennus
    a. Nessus
        i. Haavoittuvuudet
        ii. Compliance
    b. Porttiskannaukset (ARP & Nmap)
    c. Omat skriptit
    d. Tcpdump
    e. Sovellustestaus
        i. Burp suite
        ii. Selaintyökalut
        iii. OWASP ZAP
5. Raportointi

Kuvio 8: Lopullinen sisällysluettelo

10 Yhteenveto ja jatkokehitysehdotukset

Opinnäytetyön tarkoituksena oli luoda käyttöohje uusille ja vanhoille KPMG:n työntekijöille ketkä työskentelevät Katakri – työkalun kanssa arvioimassa asiakasyritysten teknistä tietoturvallisuutta. Käyttöohjeesta haluttiin selkeä ja sopivan teknistä, unohtamatta päivitettävyyttä. Valitut kehittämismenetelmät sopivat tällaiseen kehitystyöhön hyvin. Teoria lisättynä käytännön työllä ja haastatteluilla, antaa hyvän ja kattavan kuvan työkalun oikeaoppisesta käytöstä. Näillä perusteilla oli hyvä lähteä toteuttamaan käyttöohje.

Kehittämistyötä ja opinnäytetyötä tehtiin vuoden 2022 kevään aikana. Teoriaan tutustuminen aloitettiin noin kuukausi ennen uudessa työtehtävässä aloittamista, jonka jälkeen kehitystyö jatkui työn ohessa. Katakri kuuluu isona osana uuteen työtehtävään, joten teoriaan tutustuminen ennen aloitusta, helpotti myös omaa perehtymistä työtehtävään.

Hyvän alun jälkeen törmättiin muutamaan hidasteeseen. Turvallisuusluokiteltua materiaalia käsiteltävälle työntekijälle tulee suorittaa Suojelupoliisin tekemä turvallisuusselvittely. Turvallisuusselvityksissä saattaa vierähtää aikaa, riippuen Suojelupoliisin aikataulusta. Toinen hi-

dastava tekijä oli Katakri – toimeksiantojen aikataulut. Katakri – toimeksiannoista keskustellessa puhutaan enemmänkin kuukausista kestävistä projekteista, kuin päivistä. Tämä luonnollisesti tekee sen, että uusia projekteja ei aloiteta hirveänkään usein.

Käyttöohjeen laatiminen osoittautui muutoinkin pitkäksi prosessiksi. Hidasteiden jälkeen työkalun sisäistäminen, ja laadukkaan käyttöohjeen tuottaminen vei aikaa. Työn tavoitteena oli kuitenkin alusta lähtien laadukas käyttöohje, josta hyötyisi niin työntekijät kuin toimeksiantaja, ja tästä tavoitteesta ei haluttu luopua. Tämän takia, tätä kirjoittaessa, käyttöohje ei sisällöltään ole täysin valmis, ja jatkokehitysehdotuksena esitetäänkin käyttöohjeen viimeistelyä.

Opinnäytetyössä on pyritty kertomaan selkeästi kehitystyön eri askeleista tuoden opinnäytetyölle luotettavuutta. Samalla pätevyyttä on haettu käyttämällä useampaa kehittämismenetelmää, teorian lisäksi havainnointia ja haastatteluita. Uskon, että näillä toimenpiteillä kehitystyöstä toivotut reliabiliteetti ja validiteetti täyttyvät.

Kehitystyö oli kaiken kaikkiaan kiinnostava ja ajankohtainen. Tietoturva on ajankohtaisempi ja tärkeämpi kuin koskaan, eikä vähiten turvallisuusluokiteltu materiaali. Kehitystyö antoi ja opetti tekijälleen paljon, ja uskon, että käyttöohjeesta hyötyy tulevaisuudessa moni.

Lähteet

Painetut

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2010. Tutki ja kirjoita. 15–16. painos. Hämeenlinna: Kariston Kirjapaino Oy.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät – Uudenlaista osaamista liiketoimintaan. 3–4. painos. Helsinki: Sanoma Pro Oy.

Sähköiset

Campanizzi, J. 2005. Effective Writing for the Quality Professional – Creating Useful Letters, Reports, and Procedures. E-kirja. Milwaukee: Quality Press.

Digia. 2021. Tietoturvassa on kaksi keskeistä ongelmaa – Organisaation tietoturvan saa hallintaan yllättävän helposti ja ketterästi. Viitattu 18.4.2022. https://www.kauppalehti.fi/kumppanisisallot/digia/tietoturvassa-on-kaksi-keskeista-ongelmaa-organisaation-tietoturvan-saa-hallintaan-yllattavan-helposti-ja-ketterasti/

Elisa 2022. Viitattu 25.3.2022. https://yrityksille.elisa.fi/tietoverkot

Holopainen, R. 2021. Katakri-auditointityökalu sai päivityksen. Viitattu 18.4.2022. https://www-tivi-fi.nelli.laurea.fi/uutiset/katakri-auditointityokalu-sai-paivityksen/c4ad6dfb-6759-49b6-be20-f3fc43e8db34

Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje. 2020. Kansallinen turvallisuusviranomainen. Viitattu 25.3.2022. https://um.fi/documents/35732/0/KV-TIEDON+K%C3%84SITTELYOHJE+NSA+%28SUOMI%29_CLEAN.pdf/888aeb84-3e23-df3b-1774-a936f29a3fd9?t=1604931832075

Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. 2020. Ulkoministeriö. Viitattu 7.3.2022. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Katakri 2020 –arviointityökalu. 2020. Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. Viitattu 7.3.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Katakri-2020-arviointityokalu.xlsx

Kelo, T. & Eronen, J. 2017. Experiences from Development of Security Audit Criteria. Teoksessa European Conference on Cyber Warfare and Security. Reading: Academic Conferences International Limited. 208–215.

Kotimaisten kielten keskus 2022. Viitattu 11.4.2022. https://www.kotus.fi/ohjeet/hyvan_virkakielen_ohjeita/millaisia_ovat_toimivat_ohjeet_ja_kysymykset/ohjeita_ohjeiden_tekijoille

KPMG IT Sertifiointi Oy Palvelukuvaus. 2021. KPMG IT Sertifiointi Oy. Viitattu 6.4.2022. https://assets.kpmg/content/dam/kpmg/fi/pdf/2021/08/fi-kpmg-it-sertifiointi-oy-palvelukuvaus_2021.pdf

KPMG 2022. Viitattu 24.3.2022. https://home.kpmg/fi/fi/home/tietoa-kpmgsta/kpmg-yrityksena/organisaatio.html

KPMG 2022. Viitattu 24.3.2022. https://home.kpmg/fi/fi/home/palvelut/neuvontapalvelut.html

Kyberturvallisuuskeskus 2022. Viitattu 6.4.2022. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset

Laki tietoturvallisuuden arviointilaitoksista 1405/2011.Viitattu 5.4.2022. www.finlex.fi/fi/laki/alkup/2011/20111405

Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit – Tilaajaorganisaatio näkökulma. 2021. Liikenne- ja viestintävirasto. Viitattu 9.4.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf

Luottamuksen lähteillä Näkökulmia tietoturvan standardointiin ja sertifiointiin. 2019. Liikenne- ja viestintävirasto. Viitattu 22.3.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

Nykänen, R. & Kärkkäinen, T. 2014. Aligning Two Specifications for Controlling Information Security. International Journal of Cyber Warfare and Terrorism, 4(2), 46–62. Viitattu 13.4.2022. https://doi.org/10.4018/ijcwt.2014040104

Ohje tietoturvallisuuden arviointilaitoksille 210/2016 O. 2020. Liikenne- ja viestintävirasto. Viitattu 5.4.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Arviointilaitosohje_v_8_2.PDF

Peda.net 2022. Viitattu 25.3.2022. https://peda.net/ksao/oppimisymp%C3%A4rist%C3%B6/yto-aineet/arkisto/vtp/2m/tjvv/tietoj%C3%A4rjestelm%C3%A4t/tl

Perehdyttäminen ja työnopastus – Ennakoivaa työsuojelua. 2013. Työturvallisuuskeskus. Viitattu 22.3.2022. https://ttk.fi/oppaat_ja_ohjeet/digijulkaisut/perehdyttaminen_ja_tyonopastus_-_ennakoivaa_tyosuojelua

Kuviot

Liitteet

Liite 1: Katakri 2020 osa-alue I:n sisältö

Tietoliikenneturvallisuus

I-01 Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen – Verkon rakenteellinen turvallisuus

Turvallisuusluokka IV

1. Tietojenkäsittely-ympäristö on erotettu muista ympäristöistä.
2. Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää vähintään palomuurin käyttöä.
3. Hallitun fyysisen turva-alueen ulkopuolelle menevä liikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä salausratkaisulla (vrt. I-12 ja I-15).

Turvallisuusluokat III-II (Kohtien 1 ja 3 lisäksi)

4. Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymän yhdyskäytävän käyttöä.

I-02 Vähimpien oikeuksien periaate – tietoliikenne-verkon vyöhykkeistäminen ja suodatussäännöstöt ko. turvallisuusluokan sisällä

Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti.

I-03 Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan – suodatus- ja valvontajärjestelmien hallinnointi

Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan.

Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen, poistaminen ja valvonta (vrt. I-16) on vastuutettu ja organisoitu.

Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.

Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.

I-04 Tietojenkäsittely-ympäristöjen suojattu yhteen liittäminen – hallintayhteydet

Hallintayhteydet on rajattu turvallisuusluokittain, ellei käytössä ole toimivaltaisen viranomaisen ko. turvallisuusluokille hyväksymää yhdyskäytäväratkaisua.

Hallintaliikenteen sisältäessä turvallisuusluokiteltua tietoa ja kulkiessa matalamman turvallisuusluokan ympäristön kautta, turvallisuusluokitellut tiedot on salattu toimivaltaisen viranomaisen hyväksymällä salaustuotteella.

Hallintaliikenteen kulkiessa ko. turvallisuusluokan sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskienhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen.

Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaiseesti.

I-05 Suojattavien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella – langaton tiedonsiirto

Langattomassa tiedonsiirrossa tietoliikenne salataan toimivaltaisen viranomaisen ko. tuvallisuusluokalle hyväksymällä salausratkaisulla (vrt. I-12).

Tietojärjestelmäturvallisuus

I-06 Vähimpien oikeuksien periaate – pääsyoikeuksien hallinnointi

Tietojärjestelmien käyttöoikeudet on määritelty.

Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käsittelyoikeuksien (vrt. T-13) on varmistuttu.

Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä.

Käyttöoikeudet on pidettävä ajantasaisina.

I-07 Monitasoinen suojaaminen – Tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä

Tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti.

I-08 Vähimmäistoimintojen ja vähimpien oikeuksien periaate – Järjestelmäkovennus

Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut.

Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennetut asennus.

Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.

Kovennusten voimassaolosta ja vaikuttavuudesta huolehditaan koko tietojärjestelmän elinkaaren ajan.

I-09 Monitasoinen suojaaminen – Haittaohjelmasuojaus

Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.

I-10 Monitasoinen suojaaminen – Turvallisuuteen liittyvien tapahtumien jäljitettävyys

Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen.

Tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmien käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olvien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.

Turvallisuusluokan II-III tiedon käsittely on rekisteröitävä sähköiseen lokiin, tietojärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi).

I-11 Monitasoinen suojaaminen – Poikkeamien havainnointikyky ja toipuminen

Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan, rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai tietojenkäsittely-ympäristön resursseja ja estämään muut vahingot, sekä palauttamaan tietojenkäsittely-ympäristön suojattu tilanne viipymättä.

I-12 Tietoturvallisuustuotteiden arviointi ja hyväksyntä – Salausratkaisut

Toimivaltainen viranomainen on hyväksynyt käytetyt salausratkaisut (ja –tuotteet) ko. turvallisuusluokalle ko. käyttöympäristössä turvallisuusluokiteltujen tietojen luvattoman paljastumisen ja muuntelun estämiseksi.

I-13 Monitasoinen suojaaminen koko elinkaaren ajan – Ohjelmistojen suojaaminen verkkohyökkäyksiltä

Tietojenkäsittely-ympäristön turvallisuus, myös niiden tekniset ja muut kuin tekniset turvatoimen, testataan hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan, ja sen tarkistamiseksi, että ne on moitteettomasti toteutettu, integroitu ja konfiguroitu.

Tietoturvallisuutta vaaratavia verkkohyökkäyksiä vastaan suojaudutaan ja suojauksista sekä niiden toiminnasta huolehditaan tietojenkäsittely-ympäristön elinkaaren ajaksi.

I-14 Monitasoinen suojaaminen – Hajasäteily (TEMPTEST) ja elektroninen tiedustelu

Turvatoimia toteutetaan turvallisuusluokiteltuihin tietoihin liittyvässä tietojenkäsittely-ympäristössä toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymillä menetelmillä niin, että tahattomat sähkömagneettiset vuodot eivät vaaranna tietoja (TEMPTEST-turvatoimet).

Käsiteltäessä turvallisuusluokan III tai II tietoja sähköisesti, on pidettävä huolta, että elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi.

Nämä turvatoimet on suhteutettava tiedon hyväksikäytön riskiin ja turvallisuusluokkaan.

Käyttöturvallisuus

I-15 Turvallisuusluokiteltujen tietojen välitys fyysisesti suojattujen alueiden välillä – Tiedon sähköinen välitys

Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden ulkopuolella, tieto/tietoliikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä menetelmällä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä turvallisuusluokiteltuja tietoja.

Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden sisäpuolella, aiemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskienhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen.

I-16 Turvallisuusluokitellun tiedon käsittelyyn liittyvien tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Muutoshallintamenettelyt

Turvallisuuden varmistamista pidetään vaatimuksena koko tietojenkäsittely-ympäristön elinkaaren ajan sen alullepanosta käytöstä poistamiseen.

Tietoturvallisuutta koskevat arvioinnit, tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.

Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten- ja asetustenhallintaprosessia.

I-17 Turvallisuusluokiteltujen sähköisessä muodossa olevien tietojen käsittely fyysisesti suojattujen alueiden sisällä – Fyysinen turvallisuus

Turvallisuusluokka IV

Turvallisuusluokiteltujen tietoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta (vrt. F-04 ja I-18).

Tietojen käsittely on mahdollista toimivaltaisen viranomaisen hyväksymillä turvallisuusalueilla /vrt. F-04) ja toimivaltaisen viranomaisen hyväksymillä menettelyillä turvallisuusalueiden ulkopuolella (vrt. I18).

Tietojen säilytys on mahdollista toimivaltaisen viranomaisen hyväksymillä turvallisuusalueilla (vrt. F-04) ja toimivaltaisen viranomaisen hyväksymillä menettelyillä turvallisuusalueiden ulkopuolella (vrt. I-18).

Turvallisuusluokan IV tietoja sisältävät tietovarannot ja näiden tietojen käsittelyyn käytetty tietojärjestelmä on sijoitettava toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle (vrt. F-04).

Turvallisuusluokka III-II (Kohtien 1 ja 2 lisäksi)

Tietojen säilytys on mahdollista toimivaltaisen viranomaisen hyväksymillä turva-alueilla (vrt. F-04). Vrt. vain kansallisia tietoja koskeva poikkeus kohdassa 6 sekä etäkäyttö kohdassa I-18.

Vain kansallisten turvallisuusluokan III sähköisten tietojen säilytys on mahdollista kyseisen turvallisuusluokan mukaisessa päätelaitteessa turva-alueen ulkopuolella edellyttäen, että a) tiedot on suojattu ko. turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla (Vrt. I-12), ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle riittävästä luottamuksellisuudesta ja eheydestä on huolehdittu toimivaltaisen viranomaisten hyväksymällä menetelmällä (vrt. F-04). Vrt. etäkäyttö kohdassa I-18.

I-18 Turvallisuusluokiteltujen tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä – Etäkäyttö ja etähallinta

Turvallisuusluokka IV

Käyttäjät ja päätelaitteet tunnistetaan riittävän luotettavasti. Tietojen välitys ja käsittely turvallisuusalueiden (vrt. F-04) välillä on mahdollista vain toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymien korvaavien menettelyjen mukaisesti.

Turvallisuusluokiteltuja tietoja on turvallisuusalueiden ulkopuolalla käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta. Henkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan.

Elleivät turvallisuusalueiden ulkopuolelle viedyt turvallisuusluokiteltua tietoa sisältävät tietovälineen (kiintolevyt, USB-muistit ja vastaavat) ole salattu toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä menetelmällä, tietovälineitä ei jätetä valvomatta.

Järjestelmienetäkäyttö ja –hallinta edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokan tietojen suojaamiseen hyväksymää liikenteen salausta.

Päätelaitteessa olevat tiedot tulee olla suojattu kyseiselle turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla, ja päätelaitteen ko. turvallisuusluokalle riittävästä eheydestä tulee huolehtia.

Turvallisuusluokka III-II (Kohtien 1–5 lisäksi)

Turvallisuusluokiteltuja tietoja ei avata matkalla eikä lueta julkisilla paikoilla.

Järjestelmien etäkäyttö ja –hallinta rajataan toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle (vrt. F-04). Vrt. vain kansallisia tietoja koskeva poikkeus kohdassa 8.

Vain kansallisten turvallisuusluokan III sähköisten tietojen etäkäyttö (käsittely) ja säilytys on mahdollista kyseisen turvallisuusluokan mukaisessa päätelaitteessa turva-alueiden ulkopuolella edellyttäen, että a) tiedot on suojattu ko. turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla, ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle riittävästä luottamuksellisuudesta ja eheydestä on huolehdittu toimivaltaisen viranomaisen hyväksymällä menetelmällä.

I-19 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – ohjelmistohaavoittuvuuksien hallinta

Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.

I-20 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Varmuuskopiointi

Turvallisuusluokiteltua tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto on suojattu

I-21 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen

Turvallisuusluokka IV

Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen on järjestetty luotettavasti. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. Ei-sähköisten tietojen osalta ks. F-08.4.

Turvallisuusluokka III (Kohdan 1 lisäksi)

Kansainvälisten turvallisuusluokan III (CONFIDENTIAL) tietojen osalta, kirjaajan on allekirjoitettava tuhoamistodistus, joka tallennetaan kirjaamoon/rekisteröintipisteeseen. Kirjaustiedot on päivitettävä vastaavasti. Kirjaamon/rekisteröintipisteen on säilytettävä tuhoamistodistuksen vähintään viiden vuoden ajan. (vrt. F-08.3).

Turvallisuusluokka II (Kohtien 1–2 lisäksi)

Jos tiedon on laatinut toinen viranomaien, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle.

Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen version voi tuhota ne laatinut henkilö.

Kansainvälisten turvallisuusluokan II (SECRET) tietojen tuhoaminen on suoritettava todistajan läsnä ollessa. Todistajalla on oltava vähintään tuhottavan tiedon turvallisuusluokkaa vastaava turvallisuusselvitys.