LAUREA AMMATTIKORKEAKOULU Uuden edellä

Kansallinen turvallisuusauditointikriteeristö Case: Elisa Oyj, Tietoturvallisuusosion käyttöönotto

Tiinus, Harri

2011 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Kansallinen turvallisuusauditointikriteeristö
Case: Elisa Oyj, Tietoturvallisuusosion käyttöönotto

Harri Tiinus
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Toukokuu, 2011

Sisällys

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Harri Tiinus

Kansallinen turvallisuusauditointikriteeristö
Case: Elisa Oyj, Tietoturvallisuusosion käyttöönotto

Vuosi 2011 Sivumäärä 45

Opinnäytetyössä kuvattiin ja pyrittiin selvittämään kansallisen turvallisuusauditointikriteeristön (KATAKRI) sovellettavuutta ja käyttöönottoa Elisa Oyj:lle. Tutkimuksen tavoitteena oli toteuttaa helppokäyttöinen työväline, joka voidaan ottaa käyttöön osaksi kohdeorganisaation operatiivista työtä arvioitaessa kriteeristöä.

Tutkimuksen teoreettisena viitekehyksenä oli KATAKRI ja sen tietoturvallisuusosio sekä kohdeorganisaation määrittämä kohde, joihin tutkimus rajattiin. Tutkimuksen painopisteenä oli kehittää kohdeorganisaation tietoturvatyön käyttöön työväline, jonka käyttöönoton perusteella oli mahdollista tutkia kansallisen turvallisuusauditointikriteeristön käytön helppoutta sekä sen toimivuutta osana kohdeorganisaation operatiivista tietoturvatoimintaa.

Opinnäytetyön tutkimukseen pyrittiin löytämään tietoturvallisuuteen liittyvää lähdekirjallisuutta. Empiiriseen osioon sisältyy kansallisen turvallisuusauditointikriteeristön työstämiseen osallistuneiden asiantuntijoiden haastattelut sekä yritys- että valtionhallinnonorganisaatioista. Haastatteluilla selvitettiin KATAKRI:n työstämisprosessia sekä taustoja ja kartoitettiin asiantuntijaorganisaatioiden suhtautumista valmistuneeseen kriteeristön. Haastatteluaineistoa analysoimalla oli mahdollista selvittää KATAKRI:n tulevaisuuden tilannetta. Tutkimuksen otos muodostettiin toimeksiantajalta saadusta kirjallisesta materiaalista, asiantuntijoiden haastatteluista ja tutkijan omasta näkemyksestä.

Tutkimuksen tulos antaa viitteitä siihen, että työvälineen käyttöönoton tai koekäytön avulla voidaan saada selville kohdeorganisaation valitseman kohteen tietoturvataso suhteessa kriteeristöön. Tutkimuksen mukaan kohdeorganisaatio pystyi työvälineen avulla tarkastelemaan omaa päivittäistä tietoturvallisuustyötä ja sen käytön yhteydessä voitiin saada selville organisaation operatiivisen tietoturvallisuustoimintaan liittyviä kehityskohteita.

Johtopäätöksenä voidaan todeta, että kohdeorganisaation käyttökokemus KATAKRI:sta tulevien kilpailutusten varalle lisääntyi, jos sen vaatimuksena on tämä kriteeristö. Tutkimuksen mukaan voidaan todeta, että työväline mahdollistaa organisaation tarkastelemaan kriteeristön muiden osioiden suhdetta organisaation oman toiminnan turvallisuuteen.

Työvälineen käyttöönotossa on huomioitava helppokäyttöisyys ja tekninen toimintavarmuus. Käyttäjille tulee antaa työvälineen käyttöön riittävä koulutus.

Asiasanat Kansallinen turvallisuusauditointikriteeristö, Tietoturvallisuus

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Programme in Security Management

Harri Tiinus

The national security audit criteria
Case: Elisa Oyj, introducing the information security section of the criteria

Year 2011 Pages 45

This thesis described and attempted to ascertain the applicability and the introduction of the national security audit criteria (KATAKRI) in Elisa Oyj. The purpose of the thesis was to implement an easy-to-use tool that can be used in the target organization's operational work when assessing the security criteria.

The context of the theoretical section of the thesis was the KATAKRI and its information security part as well as an area defined by the target organization. They gave the framework to the research. The key focus of the research was to develop a tool for the target organization's security work. With this tool it is possible to examine the usability of the national security audit criteria and their functionality as part of the target organization's operational security work.

For the thesis research the objective was to find information security-related literature. The methodological section contains interviews with experts who participated in the national security audit criteria work. They represent both corporate and government organizations. In the interviews the focus was on the KATAKRI's working process, backgrounds and also experts' attitudes to the completed criteria. By analyzing the interview data it was possible to determine the future situation of the KATAKRI. The sample of this survey is built on the written material from the organization, interviews with experts and the researcher's own views.

The results of this research provide evidence that by taking the tool in use or on trial the target organization can identify the security level of a selected function in relation to the criteria. According to this study in the target organization it was possible to analyze their daily information security work and by using the tool it was possible to identify development areas in the operational security functions.

In conclusion, it can be stated that the target organization's user experience with KATAKRI increased for potential coming competitive biddings, provided that the set of criteria is a requirement. According to this study the tool enables an organization to examine the relationship between the set of criteria in other sections of the organization's operational safety.

Lastly, when taking this type of tool in use in an organization it is important to take into account tool user friendliness and technical reliability. Moreover, users must receive adequate training in order to be able to use the tool efficiently.

Keywords National security audit criteria, Information security

1 Johdanto

Tieto- ja viestintäalan yritysten liiketoiminnan taustalla oleellisena osana on toimiva ja riittävän turvallinen tietotekninen ympäristö ja sen tuottamat palvelut yrityksen asiakkaille. Liiketoiminnan muutokset ovat jatkuvia sekä nopeita ja niiden vaikutukset tulee huomioida yrityksen käytössä oleviin tietojärjestelmiin nopeasti. Elisa Oyj:ssä muutoksiin voidaan varautua sekä yrityksen strategian mukaisesti ja lisäksi käyttämällä turvallisuusauditoinnin työvälinettä tarkentamaan operatiivisen tietoturvatyön sisältöä ja toteuttamista. Tässä opinnäytetyössä on pyritty vastaamaan sen toteuttamiseen entistä tarkemmalla tasolla ja toteutettu turvallisuusauditointikriteeristöön pohjautuva operatiivinen työväline Elisan käyttöön. Opinnäytetyössä on kehitetty työväline Elisan tietoturvatyön päivittäiseen toimintaan, joka sisältää KATAKRI -kansallisen turvallisuusauditointikriteeristön.

KATAKRI eli Kansallinen turvallisuusauditointikriteeristö (myöh. KATAKRI) on viranomaisille ja yrityksille luotu yhteinen turvallisuuskriteeristö yhteisöturvallisuusmenettelyn yhtenäistämiseksi ja omavalvonnan ja auditoinnin parantamiseksi (KATAKRI 2009, 4). KATAKRI julkaistiin virallisesti Puolustusministeriön toimesta marraskuussa 2009 ja sen pilottikäyttö oli mahdollista hieman aiemmin. Kriteeristön käyttöönotto porrastetusti luo haasteita niin yrityksille kuin muillekin instansseille. KATAKRI:lle luodut odotukset ovat olleet kunnianhimoiset ja niiden toteutuessa yritykset joutuvat tarkastelemaan omaa toimintaansa sekä varautumaan viranomaisten suorittamia auditointeja varten.

Tässä opinnäytetyössä haetaan tutkimustuloksia siitä, miten työvälineen käyttöönotto ja mahdollisesti organisaation uudet toimintatavat toimivat, tarvitsevatko ne kehittämistä tai lisäkoulutuksen toteuttamista Elisan organisaatiossa. Tekijän intressinä on antaa näkemyksensä tämän työvälineen kehittämiseen ja sen luomiseen. Tekijä työskentelee eri tehtävissä Elisa Oyj:ssä ja opinnäytetyön tekijä toimii tässä kehittämistehtävässä suunnittelijana, kehittäjänä ja työvälineen toteuttajana tavoitteena lisätä KATAKRI:öön pohjautuva työväline osaksi Elisan päivittäistä toimintaa.

KATAKRI:n julkaisun jälkeen koettiin tarpeelliseksi tutkia kriteeristön soveltamista suhteessa Elisan tietoturvatoimintaan. Toimeksianto tutkimukselle sisälsi kysymyksen niistä toiminnoista, joita yrityksen tarvitsee muuttaa tai tarvitseeko muuttaa, jotta se täyttää KATAKRI-vaatimukset. (Kansallinen turvallisuusauditointikriteeristö 2009.)

1.1 Kehittämistyön ja tutkimuksen tausta

Opinnäytetyössä kehitetään ja arvioidaan kansallisen turvallisuusauditointikriteeristön tietoturvallisuusosiota, sen käyttöä ja käytettävyyttä organisaatiossa. Tutkimuksessa luodaan koh-

deorganisaatiolle työväline, jonka avulla yritys pystyy tarkastelemaan omaa toimintaansa suhteessa kriteeristöön sekä löytämään mahdolliset kehityskohteet. Toimintamalli ja sitä tukeva työväline mahdollistaa KATAKRI:n vaatimusten mukaisen toiminnan Elisan organisaatiossa.

Opinnäytetyön kehittämistehtävä on suunniteltu ja luotu Elisan turvallisuusyksikössä osana KATAKRI-projektia vuoden 2010 aikana siten, että keväällä 2010 toteutettiin empiiriseen osaan liittyvät haastattelut, kesällä 2010 toteutettiin työvälineen käyttöönoton ensimmäinen vaihe, joka samalla toteutti työvälineen kokeilukäytön ja käyttöönoton. Työvälineen käyttöönotto jatkui Elisan organisaatiossa syksyllä 2010. Tavoitteena oli toteuttaa toimintamallia tukeva käytännön sovellus eli työväline Elisan käyttöön. Tutkimusaiheen valintaan ja sen rajaukseen on vaikuttanut tietoturvallisuusaiheen ajankohtaisuus ja tutkijan oma ammatillinen osaaminen asiaa kohtaan.

1.2 Tutkimuksen tavoite, tutkimusongelma ja rajaukset

Tutkimuksen tavoitteena on sisällyttää Elisa Oy:n tietoturvatyön toimintamalliksi työväline, joka pohjautuu KATAKRIn eli kansalliseen turvallisuusauditointikriteeristön tietoturvallisuusosioon. Kehittämistehtävän tehtävänä on luoda uusi toimintatapa ja – malli Elisa Oyj:lle tietoturvallisuusosion operatiiviseen käyttöön ja tuottaa KATAKRIn mukaista palvelua organisaation sisäisille ja ulkoisille asiakkaille. Tavoitteena oli luoda työväline, jonka avulla kohdeyritys pystyy tarkastelemaan omaa toimintaansa vaivattomasti sekä löytämään mahdollisesti kehitettävät kohteet.

Tavoitteena on tutkia tietoturvakriteeristöä kriittisesti, pyrkiä löytämään sen hyvät ja huonot ominaisuudet sekä tutkia käytettävyyttä. Tekijän tavoitteena on oppia tietoturvallisuudesta ja sen johtamisesta sekä kehittyä auditoinnin että itse kriteeristön asiantuntijaksi. Toimeksiantajan osalta tavoitteena on ollut ensinnäkin, luoda yritykselle työväline, jonka avulla yrityksen vastuuhenkilö voi seurata Elisan tietoturvan tilaa suhteessa KATAKRI-kriteeristöön. Toisaalta, tavoitteena oli määrittää Elisan tietoturvan taso, jolla kohdeyritys toimii tällä hetkellä sekä mahdolliset kehityskohteet, jotta vaadittava taso saavutetaan.

Tutkimusongelma voidaan muotoilla tutkimuskysymyksenä seuraavasti:

Millainen on tietoturvakriteeristöä palveleva toimintamalli toimeksiantajaorganisaatiolle?

Tähän tutkimusongelmaan haetaan ratkaisua alakysymysten pohjalta:

Millainen työväline palvelee parhaiten uutta toimintamallia, jotta kriteeristön käyttöönotto on organisaatiossa toiminnallisesti helppoa ja tehokasta?

Kansallinen turvallisuusauditointikriteeristö on tutkimusnäkökulmasta mielenkiintoinen, ajankohtainen ja haastava asiakokonaisuus. Tutkimus on rajattu yhdessä toimeksiantajan kanssa tietoturvallisuusosaan, koska se kohdistuu oleellisesti Elisan liiketoimintaan. Kehittämistyön tutkimuksessa ei oteta kantaa yksittäisiin kriteereihin, niiden oikeellisuuteen, vaatimusten sisältöön tai vaatimustasojen luokitteluun. Yleisesti voidaan todeta tietoturvallisuusosion olevan kriteeristön haastavin ja tulevaisuuteen eniten vaikuttava aihealue. Tutkimustyöhön ei sisälly tutkimustulosten ja mahdollisesti ehdotettujen uusien toimintojen käyttöönottoa. Kriteeristön ja yksittäisten vaatimusten hyvyys ja huonous tullaan tässä opinnäytetyössä arvioimaan sen käytettävyyden osalta ja nimenomaan kohdeyrityksen näkökulmasta.

1.3 Työskentelymenetelmät ja tutkimusraportin rakenne

Opinnäytetyö on toiminnallinen ja työelämälähtöinen kehittämistehtävä, joka rakentuu teoria- ja empiirisestä osasta. Teoreettiseen osaan on haettu tietoa ajankohtaisesta kirjallisuudesta, Elisan tietoturvayksikön toimintaohjeistuksesta ja standardeista, joita on käytetty tietoturvakriteeristön luonnissa. Teoreettisen tiedon avulla pyritään luomaan kuva yksittäiseen kriteeriin kohdistuvista mahdollisista vaatimuksista ja perusteista. Tarkoituksena ei ole kuitenkaan syventyä teoriaan sinänsä, vaan käyttää sitä apumateriaalina työn luonnissa (Hakala 2004, 22–26).

Empiirisessä osassa selostetaan Elisa Oyj:n tietoturvatyötä ja toimintamallia. Empiriaosaan sisältyy tutkimuksessa tehdyt haastattelut, jossa haetaan sellaista tietoa, että se mahdollistaisi syventämään ja analysoimaan olemassa olevaa tietoa kriteeristöstä sekä sen luonnissa käytetyistä menetelmistä. Haastatteluilla pyritään selvittämään mahdollista työvälinetarvetta, voisiko esimerkiksi taulukkolaskenta-sovelluksen avulla tehostaa ja pitää ajan tasalla organisaation tietoturvatyötä suhteessa KATAKRIn sisältöön. Haastattelujen avulla pyritään saamaan kattava kuva kriteeristön luonnista, tavoitteista sekä käyttömahdollisuuksista. Asiantuntijoiden haastattelut olivat tiedonhankinnan osa-alue, johon haastateltiin kansallisen turvallisuusauditointikriteeristön valmisteluun osallistuneita henkilöitä valtionhallinnosta ja yrityselämästä sekä Elisa Oyj:n henkilökuntaa.

Opinnäytetyön tutkimusraportti on toimintatutkimus, jossa toimintamalli otettiin käyttöön osaksi Elisa Oyj:n tietoturvayksikön toimintaa, analysoitiin tutkimusaineistoa ja arvioitiin siitä saatavia tutkimustuloksia. Tämä kehittämistehtävä on tehty toimintatutkimukselle tyypillisissä vaiheissa. Johdanto -luku kuvaa opinnäytetyön taustaa ja esittelee tutkimusraportin rakenteen. Johdannon jälkeen kuvataan tutkimuksen tausta ja sen tavoitteet sekä määritellään tutkimusongelma, tutkimuksen rajaukset sekä viitekehys KATAKRI työvälineelle. Luku 2 käsittelee tutkimusaiheeseen liittyvän teorian eli kansallisen turvallisuusauditointikriteeristön

taustaa, tavoitteita sekä osa-alueita. Tämän jälkeen luku 3 sisältää toimintamallin rakentamisen ja siihen liittyvän operatiivisen toiminnan pilotointikäytön eli toimintatutkimuksen syklin. Tässä luvussa teoria konkretisoituu empiriaan, kun kehittämistehtävän tutkimusaineistoa analysoidaan ja arvioidaan osana opinnäytetyön tutkimusta. Luvussa 4 kuvataan kohdeorganisaatiossa tehdyn työvälineen koekäyttö sekä sen tulokset. Luvussa 5 esitetään tutkijan omaa pohdintaa sekä luvussa 6 tutkimuksen johtopäätökset. Tutkimusraportti sisältää lopuksi lähdeluettelon ja liitteet.

1.4 Elisa Oyj

Elisa Oyj (myöh. Elisa) on Pohjoismaiden johtava viestintäpalvelujen tuottaja ja yritys on julkisesti noteerattu NASDAQ OMX Helsinki Suuret Yhtiöt –listalla. Yritys toimii Pohjoismaiden lisäksi Baltian maissa ja Venäjällä ja palvelee alueellisesti noin kahta miljoonaa kuluttaja-asiakasta ja kansainvälisesti noin 150 000 yritys- ja yrittäjäasiakasta tarjoamalla laajan valikoiman erilaisia liittymiä palveluineen. Yrityksen liiketoiminta, strategiansa mukaisesti, pyrkii välittämään liiketoimintaympäristöönsä elämyksiä ja parantamaan organisaatioiden tuottavuutta verkossa sekä kehittämään kuluttajille ja yritysasiakkaille erilaisia informaatio- ja kommunikaatiopalveluja. Yrityksen liikevaihto oli vuonna 2009 1,43 miljardia euroa ja sen henkilöstön määrä on noin 3 200. Elisan liiketoiminta on kansainvälistä ja se toimii globaalisti yhteistyössä Vodafonen ja Telenorin kanssa. (Elisa Oyj 2010).

Elisa on suomalainen merkittävä tietoliikennetoimittaja ja sen toiminta-ajatuksena on tuottaa palveluita niin yksityis- kuin yritysmarkkinoille. Elisan palveluiden turvallisuuden on oltava korkealla tasolla, jotta luottamus palveluihin säilyy. Yrityksen asiakkaina on myös viranomaistahoja sekä valtionhallinnon yksiköitä, joiden oletetaan ensimmäisten joukossa ottavan Kansallinen turvallisuusauditointikriteeristön käyttöön. Tämä on yksi peruste sille, minkä takia yrityksessä on jo etupainotteisesti varauduttava mahdollisiin muutoksiin kilpailutusten vaatimuksissa. Elisan palvelukentästä johtuen, tietoturvallisuuden osiolla on suurin painoarvo kriteeristöön nähden.

1.5 Kehittämistehtävän tutkimus- ja liiketoimintaympäristö

Kehittämistehtävän tutkimus- ja liiketoimintaympäristönä toimii Elisa Oyj:n turvallisuusyksikkö, joka tuottaa tukipalveluita koko Elisa-konsernille. Turvallisuusyksikön päivittäinen operatiivinen työ sisältää yhteistyön myös viranomaisten kanssa. Tutkimuksen kehitystyö oli mahdollista toteuttaa samanaikaisesti sekä kehitys- että liiketoimintaympäristössä. Tutkimustyön toimeksiantajan edustajana toimi Elisan turvallisuusjohtaja.

2 KATAKRI – Kansallinen turvallisuusauditointikriteeristö

Tässä luvussa kuvataan KATAKRI-kriteeristön sisältö työvälineenä ja asiakokonaisuudet teorianäkökulmasta, jotta myöhemmin tutkimusraportissa voidaan esittää sen soveltaminen empiirisessä osassa tämän tutkimuksen tavoitteiden saavuttamiseksi. KATAKRI, Kansallinen turvallisuusauditointikriteeristö, on työväline yritysten ja viranomaisten yhteiskäyttöön. Se on luotu osana Suomen sisäisen turvallisuuden ohjelman toista vaihetta, jonka Suomen hallitus vahvisti ja kohdisti Puolustusministeriön johtovastuulle ja erillisen johtoryhmän alaisuuteen syyskuussa 2008. KATAKRI-työ julkaistiin 20.11.2009 ja työryhmän tarkoituksena oli luoda viranomaisille ja yrityksille yhteinen turvallisuuskriteeristö, joka yhtenäistää Suomen turvallisuustasojen määrittelyä sekä parantaa sen omavalvontaa sekä auditointia. Kriteeristön laadinnassa on käytetty laajalti maamme turvallisuusasiantuntijoita niin viranomais-, yhteisökuin yritysmaailmastakin, mahdollisimman kattavan ja käyttökelpoisen tuloksen takaamiseksi. (Kansallinen turvallisuusauditointikriteeristö 2009.)

2.1 Kansallisen turvallisuusauditointikriteeristön tausta

Kansallisen turvallisuusauditointikriteeristön työstäminen on lähtenyt liikkeelle vuonna 2008, jolloin Elinkeinoelämän keskusliitto ja viranomaiset kävivät keskusteluita kilpailukyvyn säilyttämisestä turvallisuustason nostamisen merkeissä. Näissä keskusteluissa nousi esille yhtenäisen, kansalliset ja kansainväliset säädökset kattavan toimintamallin rakentaminen, jonka avulla voitaisiin säilyttää suomalaisen elinkeinoelämä kilpailukyky turvallisuuden osa-alueella. (Tiihonen 2010.)

Elinkeinoelämän keskusliiton yritysturvallisuusyksikön päällikkö Kalevi Tiihosen mukaan elinkeinoelämän rakennemuutokset, kansainvälistyminen, toimenpiteiden ulkoistaminen ovat johtaneet muun muassa viranomaisten ja elinkeinoelämän lisääntyneeseen yhteistyöhön, jonka johdosta on huomattu tarve toteuttaa yhtenäinen KATAKRI-kriteeristö (Haastattelu K. Tiihonen 15.4.2010). Viranomaisilla on jo aiemmin ollut käytössä erilaisia standardeihin, vallitseviin käytäntöihin, kansainvälisiin sopimuksiin sekä kansallisiin lakeihin pohjautuvia turvallisuustason määrityksiä, mutta näiden vaatimusten vaateita ei ole tunnettu yritysmaailmassa, mikä on vaikeuttanut molempien osapuolten yhteistoimintaa. Myös eri yritykset ovat asettaneet turvallisuusvaateita yhteistyökumppaneilleen ja palveluntarjoajille, jotka ovat aikaisemmin voineet olla ristiriidassa viranomaisten vaateiden kanssa. Tiihosen mukaan tavoitteeksi Elinkeinoelämän Keskusliiton ja viranomaisten välisissä keskusteluissa oli luoda toimintamalli yritysturvallisuuden osa-alueiden kattamiseksi, jolla turvallisuustasoa voitaisiin luotet-

tavasti ja yhtenevästi auditoida sekä yritysten turvallisuuden omavalvontaa kehittää. (Kesäläinen 2010; Tiihonen 2010)

2.2 Kansallisen turvallisuusauditointikriteeristön tavoitteet

Kansallisen turvallisuusauditointikriteeristön ensisijaisen tavoite on yhtenäistää viranomaisten suorittamia turvallisuustason tarkastuksia yrityksiin, ennen kuin yrityksille luovutetaan viranomaisten salaiseksi luokittelemaa tietoa. KATAKRI-kriteeristön valmistuttua voidaan turvallisuusauditointi suorittaa toistuvasti samansisältöisenä, luotettavasti ja yhtenäisesti. Koska kriteeristö on viranomaisten yhteisesti hyväksymä, voidaan sen avulla välttää jatkuvia turvallisuusauditointeja myöntämällä yritykselle kriteeristön hyväksytystä tarkastuksesta sertifikaatin. (Kansallinen turvallisuusauditointikriteeristö 2009; Puolustusministeriö 2010.)

KATAKRIn toisena tavoitteena on ollut luoda yrityksille kansallinen ja yhtenäinen työväline, jonka avulla yritykset voivat tarkastella oman toiminnan tasoa jo ennen mahdollisia auditointeja. Rauno Hammarbergin mukaan kriteeristö on loistava työväline pienille ja keskisuurille yrityksille tarkastella ja kehittää yrityksen turvallisuustasoa (Hammarberg 2009). Motiivina voi olla pelkästään oman toiminnan jatkuvuuden turvaaminen, ei edes osallistua valtionhallinnon kilpailutuksiin. Yritys hyötyy kriteeristöstä, koska sitä tarkastelemalla organisaatio on pakotettu rakentamaan kokonaisvaltainen turvallisuusstrategia. Kriteeristön kokonaisvaltaisuus auttaa ei-turvallisuusasiantuntijaa hahmottamaan turvallisuuden eri osa-alueet sekä ottamaan turvallisuustyön osaksi päivittäistä operatiivista toimintaa (Hammarberg 2009; Kesäläinen 2010; Puolustusministeriö 2010).

Elinkeinoelämän Keskusliiton Kalevi Tiihosen mukaan kansallisen kilpailukyvyn parantaminen kansallisen turvallisuusauditointikriteeristön avulla on tärkeää ja oleellista. Kriteeristön avulla voidaan parantaa yritysten turvallisuutta, luoda yhtenäinen ja kaikille tasapuolinen toimintamalli. Tiihosen mukaan on tärkeää pyrkiä luomaan edistyksellinen malli yhteiseksi kriteeristöksi, jolloin auditoinnin läpäisseet yritykset voivat saada siitä kilpailuetua niin kotimaassa kuin kansainvälisilläkin markkinoilla. Suojelupoliisin lausuntotoimiston päällikkö Lotta Lampela toteaa TURVALLISUUS 5/2010 – lehden haastattelussa, että ”KATAKRIn vaatimukset täyttämällä yritys saa turvallisuutensa tason hyvälle tasolle”. Jos yritys on halukas osallistumaan kansainvälisiin tarjouskilpailuihin, jotka vaativat kansallisen NSAn suorittamaa yhteisöturvallisuusselvitystä, on KATAKRIn vaatimukset täyttämällä, Lampelan mukaan, hyvät mahdollisuudet läpäistä yhteisöturvallisuusselvitys. National Security Authority (lyh. NSA) eli kansallinen turvallisuusviranomainen on Suomessa on ulkoasianministeriö, jonka pyynnöstä Suojelupoliisi on auditoinnin suorittava taho (Tiihonen 2010; Lampela 2010).

2.3 KATAKRIN määritelmät, osa-alueet ja arviointi

Kansallinen turvallisuusauditointikriteeristö muodostuu eri yritysturvallisuuden osa-alueisiin liittyviin kysymyssarjoihin. Kriteeristön kysymykset on laadittu ulkopuolisen tahon suorittamaa auditointia varten, mutta niitä voidaan samalla tavalla käyttää yrityksen omassa turvallisuustyössä. (Kreus 2010.)

Kansallinen turvallisuusauditointikriteeristö on jaettu neljään toisiaan täydentävään osioon. Jokainen osio on jaettu kapeampiin osa-alueisiin, 3-9 osiosta riippuen. Jakamalla osio osa-alueisiin on pyritty saamaan kriteeristöön selkeyttä sekä helppokäyttöisyyttä. Jaon avulla on myös selkeämpää jakaa vastuita yrityksen tai yhteisön sisällä. Yksittäinen osa-alue sisältää eri määrän kyseiseen aiheeseen liittyviä kriteerejä. Tutkimuksen kannalta oleellista on sisällyttää kaikki osa-alueet yrityksen tietoturvan auditoinnin sisältöön. Hallinnollinen turvallisuus ja turvallisuusjohtaminen pitävät sisällään organisaation turvallisuusjohtamisen arvioinnin. Kysymykset liittyvät organisaation turvallisuuspolitiikkaan, periaatteisiin ja ohjeistukseen. Henkilöstöturvallisuus-osio sisältää organisaation kykyä suojata omaa toimintaansa sekä salaisten tietojen saatavuutta sekä sisältää arviointia rekrytoinnista, toiminnasta työsuhteen aikana ja sen loppuessa. Fyysinen turvallisuus-osio on toimitilaturvallisuus painotteinen, pitäen sisällään lähinnä kuorisuojaukseen pohjautuvaa toimintamallia. Tietoturvallisuusosio on kriteeristön laajin osio, joka pitää sisällään tietoturvallisuuden vaatimuksia turvallisuuspolitiikasta teknisiin vaatimuksiin. (Kansallinen turvallisuusauditointikriteeristö 2009.)

Kriteeristö on ositettu siten, että kirjain kuvaa päätasoa, joita ovat siis neljä edellä mainittua osa-aluetta, ensimmäinen numero kuvaa alatasoa ja seuraavat kyseessä olevan tason kysymystä. Esimerkiksi tietoturvallisuuden osio on jaettu 7 alatasoon I100:sta I700:taan ja jokaisessa alatasossa on vaihteleva määrä kysymyksiä eli kriteerejä. Itse kriteeri muodostuu pääkysymyksestä, joissain kriteereissä myös lisäkysymys, sekä tasovaatimuksista. Vaatimukset on jaettu neljään tasoon: lähtötaso, perustaso, korotettu taso sekä korkea taso. Lähtötaso on ainoastaan suositus yrityksen turvallisuustasosta, muut tasot ovat vaatimuksia, jotka on täytettävä. Vaatimukset myös periytyvät alemmalta ylöspäin, eli alemman tason vaatimus myös aina täytettävä. Vaatimuksissa voidaan viitata ylemmillä tasoilla lähtötasoon, tällöin lähtötasokin on itsenäinen vaatimus. (Kansallinen turvallisuusauditointikriteeristö 2009; Kreus 2010.)

Seuraavassa kuvassa (Kuva 1) on esitetty KATAKRI-dokumentin rakennetta ja siihen liittyviä tasovaatimuksia yleisesti.

Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, osa-alue A100					
Kysymys	**Lähtötason suositukset**	**Perustason (IV) vaatimukset**	**Korotetun tason (III) vaatimukset**	**Korkean tason (II) vaatimukset**	**Lähde/viite**
A 101.0 **Onko organisaation johto määrittänyt ja hyväksynyt turvallisuuspolitiikan. Onko politiikka tarkistettu määräajoin?** Kysymyksellä arvioidaan: Organisaation turvallisuusjohtamisen kypsyystasoa	Organisaatiolla on kirjattuna turvallisuutta koskevat perusasiat erillisenä dokumenttina tai osana yleisten tavoitteita	Organisaatiolla on kirjattuna turvallisuutta koskevat perusasiat erillisenä dokumenttina tai osana yleisten tavoitteita	Organisaatiolla on kirjattuna ylimmän johdon hyväksymä turvallisuuspolitiikka tai vastaava turvallisuustoimintaa ohjaava hyväksytty määrittely.	Organisaatiolla on voimassa oleva, julkaistu ja koulutettu turvallisuuspolitiikan nimellä dokumentoitu turvallisuustoiminnan ylätason asiakirja, joka on ylimmän johdon hyväksymä. Turvallisuuspolitiikka tarkistetaan vähintään vuosittain ja tarkistukset dokumentoidaan sekä hyväksytetään ylimmällä johdolla. Organisaation turvallisuuspolitiikka ohjaa seuraavia kokonaisuuksia: turvallisuuden vuotuinen toimintaohjelma, turvallisuustyön tavoitteet, riskien tunnistamisen arviointi ja kontrollit, turvallisuusorganisaatio ja vastuut, onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennaltaehkäisevät toimenpiteet, turvallisuusdokumentaatio ja sen hallinta, koulutuksen ja tietoisuuden lisääminen sekä osaamisen, raportoinnin ja johdon katselmukset.	

Kuva 1: Esimerkki KATAKRI:stä ja sen tasovaatimuksista.

KATAKRI:n arviointi tehdään pääsääntöisesti aina yrityksen näkökulmasta ja huomioidaan se, kuinka kriteeristö soveltuu käytettäväksi kyseessä olevassa organisaatiossa. Kohdeyrityksen toimialasta johtuen arvioitavaksi osioksi valikoitui tietoturvallisuusosio. Kirjallisuuden sekä haastatteluiden perusteella kriteeristöä ei ole sovellettu yritysten kilpailutuksissa koko laajuudessa. Koska tutkimuksen tarkoituksena on tehdä kansallisen turvallisuusauditointikriteeristön tarkastelua ja käyttöönottoa kohdeyrityksen näkökulmasta, on oleellista tarkastella tutkimusalueen kohtia arviointikriteereiden pohjalta.

Kun arvioidaan yksittäistä kriteeriä ja sen käyttöä, on huomioitava kriteerin kirjoitusasu ja sen luoma mielikuva kriteeristä, sen vaatimuksen sisällöstä sekä työvälineen käytön oletettu helppous. Oleellista on tehdä kriteeristön arvioinnin operatiivinen työ yrityksen näkökulmasta eli yksittäisen kriteerin vaatimuksen täyttäminen, joka edellyttää vahvaa yrityksen toimialan asiantuntemusta ja ammatillista osaamista, jotta arvioinnin vaikeus ei tule liian suureksi. Arviointityössä arvioidaan kansallisen turvallisuusauditointikriteeristön käyttö ja käytön mahdollisuuksia kohdeyrityksessä, ei itse kriteeristöä. Yksittäisen vaatimuksen tai koko kriteeristön tietoturvallisuusosion arviointi hyvyyden tai huonouden kannalta on hieman epärelevanttia tästä näkökulmasta kriteeristöä tarkasteltuna. Yksittäisen kriteerin hyvyyteen tai huonouteen

voi ottaa kantaa vain kohdeyrityksen kannalta, ei yleisestä näkökulmasta. Arviointityön haasteena on yksittäisen vaatimuksen sovellettavuus tiettyyn toimialaan tai toimitettuun palveluun, johon kriteeristöä mahdollisesti käytettäisiin.

2.4 KATAKRIN Tietoturvallisuusosa-alueet

Kansallisen tietoturvallisuusauditointikriteeristön tietoturvallisuusosion on tehnyt suomalainen asiantuntijaryhmä. Tietoturvallisuusryhmän puheenjohtajana oli Viestintäviraston Timo Lehtimäki ja ryhmän edustajat olivat sekä viranomaispuolelta että yritysmaailmasta. Viestintävirasto kuuluu Suomen kansalliseen turvallisuusviranomaisorganisaatioon, joka vastaa kansainvälisten sopimusten mukaisista turvallisuusauditointien suorittamisesta. Viestintäviraston vastuuna on myös ylläpitää tietoturvan tilannekuvaa sekä tiedottaa mahdollisista tietoturvauhkista, Verkot ja turvallisuustulosalue on Viestintäviraston kyseinen yksikkö. (Lehtimäki 2010.)

Kansallisen turvallisuusauditointikriteeristön tietoturvallisuuden osiossa esitetään suojattaville tiedoille vähimmäisvaatimukset. Tällaisia suojattavia tietoja voivat olla turvaluokitellut ja viranomaisten suojattavat tiedot, joita suojataan tietoturvallisuuden kolmen perinteisen ulottuvuuden, eheyden, luottamuksellisuuden ja käytettävyyden kautta. Tietoaineiston turvaaineisto on kuvattu tarkemmin liitteessä kaksi (Liite 2). (Kansallinen turvallisuusauditointikriteeristö 2009; Laakso 2010.)

Tietoturvallisuuden osio on kansallisessa turvallisuusauditointikriteeristössä jaettu seitsemään (7) osa-alueeseen, joista jokainen sisältää otsikkoon liittyviä kriteereitä. Vaatimukset on jaettu neljään tasoon, lähtötasosta korkeaan tasoon. Tietoturvallisuuden osiossa lähtötason suositukset ovat kohdistettu koko organisaatiolle, eli koko yrityksen tietoturvallisuuden on toimittava tason suositusten edellyttämällä tavalla. Ylempien tasojen vaatimukset koskevat vain yrityksen suojattavaa kohdetta tai tietoa, joka voi siis olla yksittäinen järjestelmä, prosessi tai sen osa. (Kansallinen turvallisuusauditointikriteeristö 2009). Opinnäytetyön tutkimustavoitteiden osalta seuraavissa kappaleissa on lyhyesti avattu oleelliset kohdat tietoturvallisuusosion osa-alueista.

2.4.1 Hallinnollinen tietoturvallisuus, osa-alue I100

Hallinnollisen tietoturvallisuuden osiossa käsitellään yleisiä tietoturvakäytänteitä sekä riskien arviointia. Osa-alue I100 kattaa organisaation tietoturvan periaatteet, toiminnan suuntaviivat

sekä yleiset tietoturva-ohjeistukset organisaatiossa. Kyseisessä osa-alueessa ei vielä pureuduta kovinkaan syvällisesti yksityiskohtiin tai teknisiin määritelmiin, vaan pyritään löytämään organisaation linjaukset ja ohjeistukset. Kriteeristö antaa mahdollisuuden organisaatiolle monessakin kohtaa suorittaa vaaditut asiat haluamallaan tavalla, vaatimuksissa ei siis ole määritetty toteuttamistapaa, ainoastaan lopputulos.

2.4.2 Henkilöstöturvallisuus osana tietoturvallisuutta, osa-alue I200

Henkilöstöturvallisuuden osa-alueessa käsitellään käyttöoikeuksiin, tietoturvallisuusohjeisiin, tietoturvallisuuden koulutukseen sekä salassapitoasioihin liittyviä tietoturvavaateita. Henkilöstö on organisaation voimavara, mutta useimmiten suurin uhka organisaation tietoturvalle on oma henkilökunta. Henkilökunta on kuitenkin se tekijä, joka käsittelee, muokkaa, tallentaa ja välittää tietoa, myös luottamuksellista. Henkilöstöturvallisuudella tässä aihepiirissä tarkoitetaan omasta henkilöstöstä aiheutuvien riskien hallintaa, ei siis henkilöturvallisuutta, josta puhuttaessa tarkoitetaan henkilöstöön kohdistuvien uhkien torjumista.

2.4.3 Fyysinen turvallisuus osana tietoturvallisuutta, osa-alue I300

Fyysisen turvallisuuden osa-alueessa keskitytään tietoa sisältävien tilojen fyysiseen suojaukseen. Kuten työn aiemmassa vaiheessa kerrottiin, kriteeristö on tehty yhtenäiseksi kokonaisuudeksi. Tietoturvallisuuden fyysisen turvallisuuden osuudessa viitataan myös kriteeristön toiseen osa-alueeseen eli fyysiseen turvallisuuteen. Myös hajasäteilyn riskiin on uudessa kriteeristössä kiinnitetty huomiota, vaikka siihen ei ole juurikaan kiinnitetty huomiota viimeisten vuosien aikana suomalaisessa yritysmaailmassa. Matti Kesäläinen kantaa asiasta huolta uusimmassa Turvallisuus-lehden numerossa 2/2010, jossa hän toteaa, että kontrolloimattoman elektromagneettisen säteilyn estämiseen pitäisi kiinnittää enemmän huomiota korkeimpien turvallisuusluokkien tiloissa. (Kesäläinen 2010.)

2.4.4 Tietoliikenneturvallisuus, osa-alue I400

Tietoliikenneturvallisuus osa-alue sisältää tietoliikenneverkkoon, palomuureihin, tietoliikenteen suodatukseen, langattomien verkkojen sekä niiden valvontaan liittyviä vaateita. Kysymyksessä I 402.0 vaaditaan palomuureilta ja muilta vastaavilta liikennettä suodattavilta laitteilta yksityiskohtaisia sääntöjä suodattamisesta.

2.4.5 Tietojärjestelmäturvallisuus, osa-alue I500

Tietojärjestelmäturvallisuus on Katakrin tietoturvallisuuden osa-alueista yksityiskohtaisin vaatimusten toteuttamisen osalta. Osa-alue sisältää kriteereitä, joissa edellytetään tietynlaista toteuttamistapaa organisaatiolta. Tietojärjestelmäturvallisuuden osa-alue sisältää tunnistautumiseen, uusien järjestelmien asennukseen sekä lokien keräämiseen ja säilyttämiseen liittyviä kriteereitä.

2.4.6 Tietoaineistoturvallisuus, osa-alue I600

Tietoaineistoturvallisuus osa-alue pitää sisällään kriteereitä muun muassa tietoaineiston säilyttämisestä, käsittelystä ja hävittämisestä. Osa-alueen kaikki kriteerit käsittelevät vain salassa pidettävään tietoon liittyviä toimenpiteitä organisaatiossa. Ensimmäinen kriteeri on tiedon luokitteluun liittyvä vaatimus. Tietoaineiston turvaluokitukset eri organisaatioiden turvaluokilla löytyvät liitteestä 2.

2.4.7 Käyttöturvallisuus, osa-alue I700

Käyttöturvallisuus osa-alue sisältää tietoaineiston käyttöön, suojaukseen ja sekä hallintaan liittyviä kriteereitä. Muutamassa kriteerissä viitataan myös aiemmin valmistuneeseen, Valtiovarainministeriön julkaisemaan valtionhallinnon ICT-varautumiseen, Jatkuvuuden hallinta ja tiedon turvaaminen – dokumenttiin. JHTT on ICT-varautumisen perusvaatimukset valtionhallinnon yksiköille sekä palveluntarjoajille, jotka tuottavat kyseisille yksiköille ICT-palveluita. (Valtiovarainministeriö 2009)

3 KATAKRI – Toimintamalli ja työvälineen kehittäminen

Tässä luvussa kuvataan työvälineen toimintamallin prosessia, millä tavoin työvälineen kehitys on tapahtunut sekä millä tavoin työväline kehitettiin toimeksiantajalle. Luvussa kuvataan myös työvälineen periaatteet sekä käytön periaatteet, joita on sovellettu kohdeyritykseen. Sovellettu osuus on kuvattu tarkemmin luvussa neljä (4).

3.1 KATAKRI -työvälineen toimintamalli

Tietoturvallisuusosion yhtenä suurena haasteena on toimintojen turvallisuustason ylläpitäminen ja hahmottaminen. Vastaavasti esimerkiksi fyysisen turvallisuuden puolella muutokset tapahtuvat hallitummin ja pidemmällä aikavälillä, tietoturvallisuuden alueella järjestelmien

ja prosessien päivitykset ja muutokset voivat vaikuttaa turvallisuuden tasoon jatkuvasti. Tietojen haavoittuvuuksien ja mahdollisten hyökkäysten havainnointi, torjunta ja selvittelyt ovat haastavampaa ja vaatii selkeää ja johdonmukaista etenemistapaa.

Tietoturvallisuuden ongelmana on suhteessa muihin turvallisuuden osa-alueisiin päivitysten ja muutosten reaaliaikaisuus. Muutokset, päivitykset tai hyökkäykset eivät odota. Kaikki edellä mainitut asiat tapahtuvat huomattavasti nopeammassa syklissä kuin muilla kriteeristön osioilla, joten myös kriteeristön olisi seurattava niitä. Nämä vaatimukset on tärkeitä lähtökohtia huomioitavaksi uuden työvälineen kehittämisessä, jotta työväline olisi helposti ja nopeasti päivitettävissä kulloistakin tilannetta vastaavaksi. Toisaalta uuden työvälineen tulisi vastata toimialan ja kohdeyrityksen haasteeseen ja mahdollistaa auditoinnin tekeminen.

Elisa Oyj:n organisaation käyttöön oli tarve luoda yksinkertainen ja helposti ajantasaisena pidettävä työväline kansallisen turvallisuusauditointikriteeristön tietoturvallisuusosion arviointiin. Sen toiminnallisuuksiksi asetettiin vaatimuksia, joiden tulisi olla tietoturvallisuuden tasoiset suhteessa kriteeristöön ja sen eri tasoihin. Kehittämistyön alkuvaiheessa selvisi, että KATAKRI:n vaatimukset eri tasoineen oli helposti siirrettävissä taulukkolaskentaohjelmaan, joka sovellusohjelmana oli organisaation työntekijöille tuttu ja helppokäyttöinen työväline. Sen taulukkomuotoinen esitystapa sopi hyvin rakenteellisesti kuvaamaan KATAKRI-kriteeristön esittämisen asiakohtia ja tarvittaessa taulukkolaskentaohjelmaan oli mahdollista räätälöidä kriteeristölle kohdistuvia ja tarvittavia lisätoiminnallisuuksia ja siten luoda Elisalle oma räätälöity taulukkolaskentasovellus.

KATAKRI:n mukainen operatiivinen ja helppokäyttöinen työväline voidaan toteuttaa Elisalle käytännössä seuraavien osa-alueiden kautta:

1. Soveltaa KATAKRI:ä kohta kohdalta taulukkolaskentaohjelmaan
2. Sisällyttää organisaation erityisvaatimukset taulukkolaskentaohjelmaan
3. Työvälineen koekäyttö organisaatiossa

Kansallisen tietoturvallisuusauditointikriteeristön sisältölaajuus tai sisällön laajuus on hallittavissa, kun käytettävä työväline sisältää valmiiksi kaikki tarvittavat kriteerit, jotka on käytävä läpi ja arvioitava päivittäisessä operatiivisessa tietoturvatyössä. Taulukkolaskentasovelluksen kriteeristösisällön ymmärtäminen ja auditointi organisaatiossa yleensä vaatii käyttäjiltään ammatillista ja ajantasaista käytännön osaamista, ajattelutapaa ja toimialakohtaista tietoperustan vahvaa hallintaa.

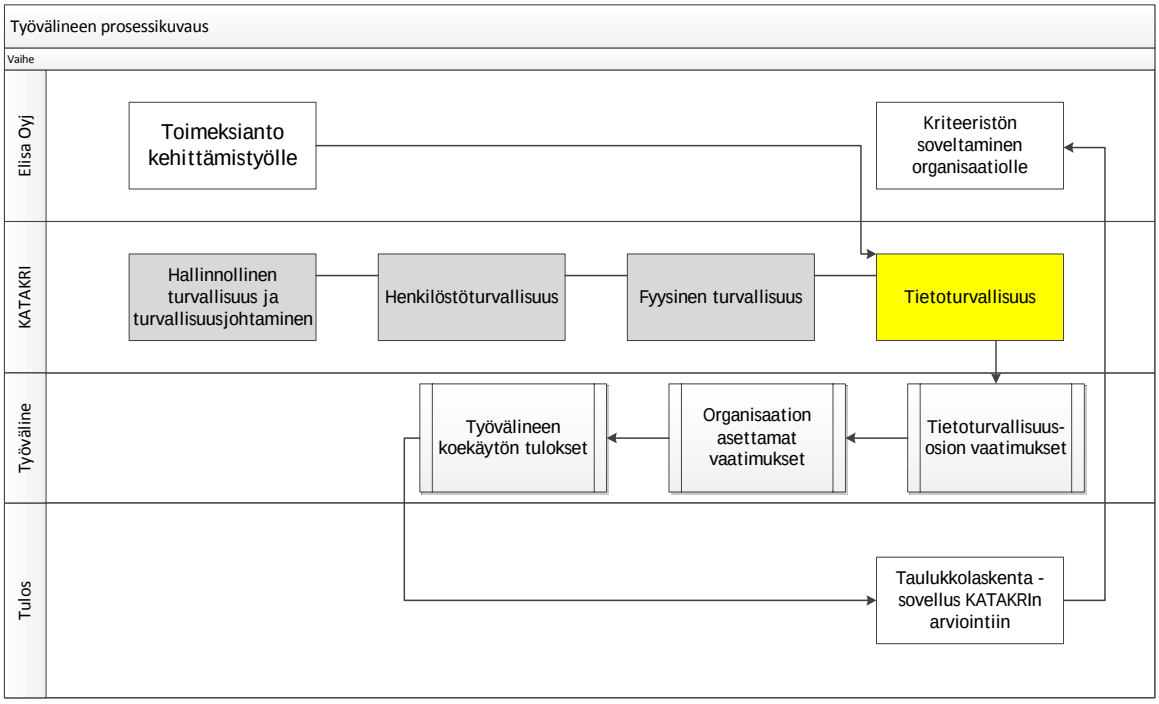
Oheisessa kuvassa (Kuva 2) näkyy pelkistetysti ne toimintamallin sisältämät asiakokonaisuudet peräkkäisinä toimintoina, jotka ovat yhteydessä toisiinsa, kun tietoturvallisuuden päivittäistyössä sovelletaan ja toteutetaan kansallista turvallisuusauditointikriteeristöä.

Kuva 2: Toimintamallin päävaiheet

3.2 KATAKRI-työvälineen kehittäminen (Elisa Oyj:lle)

Kansallisen turvallisuusauditointikriteeristön, joka on tämän kehittämistyön teoriapohja, käyttöönottoon pohjautuvan työvälineen kehittäminen on toteutettu tarvelähtökohdasta ja sen yhtenä tavoitteena on luoda yrityksen käyttöön työväline, jonka avulla kriteeristön käyttöönotto olisi mahdollisimman helppoa. Itse organisaatio luo edellytykset ja pohjat kyseisen työvälinen vaatimuksille ja tarpeille. Operatiivisen työvälineen tulee olla yksinkertainen, helposti käytettävä sekä helposti ajan tasalla pidettävä.

Toimintamallia on sovellettu Elisan organisaatiossa tässä kehittämistehtävässä ensimmäisessä vaiheessa (sykli 1) keväällä 2010 ja pilointikäyttöönoton jälkeen täydennetty kehitystyön toisessa vaiheessa (sykli 2) syksyllä 2010. Toimintamallin soveltamisen tuotoksena on luotu seuraavan prosessin mukaisesti (Kuva 3) kehittämistehtävän toimeksiantajalle operatiivinen työväline KATAKRI:n käyttöä varten. Kehitystyössä on ollut saatavilla ja käytössä Elisa Oyj:n ammatillinen osaaminen ja materiaalit tietoturvallisuudesta, jotka ovat osa kehittämistehtävän viitekehystä.



Kuva 3: Työvälineen kehityksen prosessikuvaus

3.3 Työväline operatiiviseen tietoturvatyöhön

Kehittämistehtävä on toteutettu toimintatutkimuksena ja sen käytännön toteutuksen pohjalta on luotu työväline (Kuva 4), jonka perustana on kriteeristön käyttöä tukeva toimintamalli.

KYSYMYS	Lähtötason suositukset	Pakollisuus	Status	Perustason (IV) vaatimukset	Pakollisuus	Status	Korotetun tason (III) vaatimukset	Pakollisuus	Status	Korkean tason (II) vaatimukset	Pakollisuus	Status
Hallinnollinen tietoturvallisuus, osa-alue I100												
I 101.0 Onko organisaation tietoturvallisuudella johdon tuki? Vaaditaan vähintään, että:	Tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.)	Ohjaava	Valmis	Tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.)	Ohjaava	Valmis	Tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.)	Ohjaava	Valmis	Tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.)	Ohjaava	Valmis
	organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet	Ohjaava	Valmis	organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet	Ohjaava	Valmis	organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet	Ohjaava	Valmis	organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet	Ohjaava	Valmis
	tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon	Ohjaava	Valmis	tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon	Ohjaava	Valmis	tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon	Ohjaava	Valmis	tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon	Ohjaava	Valmis
	tietoturvaperiaatteet ja -käytänteet katselmoidaan aina, kun merkittäviä muutoksia tapahtuu	Ohjaava	Valmis	tietoturvaperiaatteet ja -käytänteet katselmoidaan aina, kun merkittäviä muutoksia tapahtuu	Ohjaava	Valmis	tietoturvaperiaatteet ja -käytänteet katselmoidaan aina, kun merkittäviä muutoksia tapahtuu	Ohjaava	Valmis	tietoturvaperiaatteet ja -käytänteet katselmoidaan aina, kun merkittäviä muutoksia tapahtuu	Ohjaava	Valmis
	johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti	Ohjaava	Valmis	johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti	Ohjaava	Valmis	johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti	Ohjaava	Valmis	johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti	Ohjaava	Valmis
	tietoturvallisuudelle on varattu tarvittavat resurssit.	Ohjaava	Valmis	tietoturvallisuudelle on varattu tarvittavat resurssit.	Ohjaava	Valmis	tietoturvallisuudelle on varattu tarvittavat resurssit.	Ohjaava	Valmis	tietoturvallisuudelle on varattu tarvittavat resurssit.	Ohjaava	Valmis

Kuva 4: Esimerkki työvälineen näyttökuvasta.

Työväline on jaettu osioihin, jotta sen havainnointi, ylläpito ja täyttö ovat helpompaa ja siihen on kuvattu koko osa-alueen kriteeristö. Taulukkolaskentasovellukseen on siirretty KATAKRI:n vaatimukset ja toiminnallisuuksiin tarvittavat kaikki osat. Työvälineeksi valittiin taulukkolaskentaohjelmisto, koska se on Elisassa yksi perustietotekniikkavälineistä kunkin työntekijän tietokoneella. Tämän työvälineen luonti on toteutettu siten, että kriteeristön tietoturvallisuusosion osat siirrettiin yksitellen taulukkolaskennan sarakkeisiin siinä järjestyksessä, jossa niitä loogisesti tehdään operatiivisessa työssä ja jossa ne ovat itse kriteeristössä.

Tietoturvallisuuden osion eri osa-alueet luotiin omiksi osioiksi myös sen takia, että nykyajan työelämässä harva vastaa enää yksin koko kokonaisuudesta. Työvälineen jokaisella osa-alueella on oma välilehtensä, jolloin palvelun tai järjestelmän auditointia varten on helpompaa kierrättää samaa dokumenttia. Vastaavasti jokaiselle lähetetty oma dokumentti rasittaisi tietoturvasta vastaavan henkilön resursseja. Yhteen dokumenttiin keräämällä pystytään resurssien säästämisen lisäksi keräämään varmasti ajankohtainen ja autenttinen tieto kyseessä olevan järjestelmän tai palvelun tietoturvan tilasta.

Kehittämistyön soveltamisen tuloksena on luotu työväline, jonka jokainen tietoturvallisuus-osa-alueen osio on omalla välilehdellä. Kuvassa viisi (Kuva 5) on esitetty KATAKRI -työvälineen räätälöity näyttökuva. Tiedostomuotoinen dokumentti on työväline tietoturvayksiköiden toi-

minalle, josta arvioidaan kaikki näkyvissä olevat kriteeristön vaatimukset tasoluokittelun mukaisesti.

KYSYMYS	Lähtötason suositukset	Pakollisuus	Status	Perustason (IV) vaatimukset	Pakollisuus	Status	Korotetun tason (III) vaatimukset	Pakollisuus	Status	Korkean tason (II) vaatimukset	Pakollisuus	Status
Fyysinen turvallisuus osana tietoturvallisuutta, osa-alue I300												
I 301.0 Pääkysymys: Miten suojattavaa tietoa sisältävän tilan fyysisestä turvallisuudesta on huolehdittu?	Toimistojen, tilojen ja laitteistojen fyysinen turvallisuus on suunniteltu ja toteutettu riskiarvion mukaisilla menetelmillä. Suojattavat tiedot, niitä käsittelevät laitteistot, oheislaitteet ja tietovälineet on sijoitettu ja suojattu niin, että niihin ei ole pääsyä ulkopuolisilla.	Ohjaava	Valmis	Ks. fyysisen turvallisuuden auditointikriteeristö.	Ohjaava	Aloitettu, ei valmis	Ks. fyysisen turvallisuuden auditointikriteeristö.	Ohjaava	Ei aloitettu	Ks. fyysisen turvallisuuden auditointikriteeristö.	Ohjaava	Ei aloitettu
I 302.0 Tapahtuvatko laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet vain valvottuina?	Laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat riskienarvioinnin mukaisesti. Riskienarvioinnissa voidaan päätyä hyväksymään toimet esim. vain oman henkilöstön valvomana, sähköisellä tallentavalla kulunvalvonnalla (esim. sähköinen kulkuavain ja koodi) järjestettynä, ja/tai sopimuksin suojattuna.	Pakollinen	Valmis	Laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat vain turvatasolle hyväksytyn henkilön valvonnassa.	Pakollinen	Valmis	Perustason vaatimusten lisäksi seuraavat vaatimukset: Suojaustasoon III kuuluvan aineiston käsittely on huoltotöiden aikana kielletty ko. tilassa.	Sopimuksiin	Aloitettu, ei valmis	Perustason vaatimusten lisäksi seuraavat vaatimukset: Suojaustasoon II kuuluvan aineiston käsittely on huoltotöiden aikana kielletty ko. tilassa.	Ohjaava	Ei aloitettu
I303.0 Miten on varauduttu salakuunteluun, hajasäteilyyn ja vastaaviin uhkiin?	Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan salassa pidettävistä asioista.	Pakollinen	Valmis	Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan luokitelluista asioista.	Pakollinen	Aloitettu, ei valmis	Tilassa ei käytetä mitään sellaisia elektronisia laitteita (kannettavat tietokoneet, matkapuhelimet jne.) joiden käyttö on erikseen kielletty.	Ohjaava	Valmis	Tilaan ei saa viedä mitään sellaisia elektronisia laitteita (kannettavat tietokoneet, matkapuhelimet jne.) jotka eivät ole tilaan erikseen hyväksyttyjä.	Ohjaava	Valmis
	Henkilöstölle on muistutettava, että taukopaikoilla (tupakkakopit jne.) ei saa keskustella salassa pidettävistä asioista.	Ohjaava	Valmis	Huoneen ovet ja ikkunat on pidettävä kiinni keskusteltaessa em. asioista.	Ohjaava	Valmis	Tapauskohtaisesti arvioidaan tarve järjestelmien suojaamiseksi lähteviltä hajasäteilyltä (TEMPEST).	Ohjaava	Valmis	Tapauskohtaisesti arvioidaan tarve viranomaisen tekemälle tarkastukselle salakuuntelulaitteiden (ja vastaavien) varalta.	Ohjaava	Valmis
							Tilan äänieristys on sellainen, että tilasta ei suoranaisesti johdu ääntä ympäröiviin huonetiloihin esimerkiksi kaapelikourujen tai ilmastointikotelointien kautta.	Ohjaava	Valmis	Tapauskohtaisesti arvioidaan tarve TEMPEST- tai EMP/HMP-suojaukselle.	Ohjaava	Valmis

Kuva 5: Työvälineen räätälöity näyttökuva.

Jokaisen kriteerin kysymyksen ja vaatimusten lisäksi työvälineessä on jokaista yksittäistä vaatimusta kohden "Pakollisuus"-kenttä sekä "Status"-kenttä. Pakollisuus-kenttään voidaan kuvata, varsinkin korotetun ja korkean tason vaatimuksissa, yrityksen tai palvelun tarve täyttää kyseinen vaade. Status-kenttään merkitään yrityksen toiminnan tila toisin sanoen onko toiminta kriteerin vaatimalla tavalla, onko toiminnan toteutus aloitettu, onko toteutettu osittain vai kokonaan aloittamatta. Pakollisuus- ja status-kentän tilat on koodattu liikennevaloin, jolloin havainnointi ja yrityksen tilan tarkastelu on helpompaa. Kriteeristön tietoturvallisuuden osio on jaettu omiin välilehtiin ja näin ollen on saatu tilaa myös kohdeyrityksen omille ohjeille ja asetuksille. Työvälineen jokaiseen kriteeriin on myös liitetty tukimateriaali. Tukimateriaali löytyy jokaisen osion alareunasta ja siihen voidaan kerätä tietoa yrityksen ohjeistuksesta, periaatteista tai kyseessä olevan kilpailutuksen erityisvaateista. Uutta työvälinettä voidaan käyttää myös kriteeristön muiden osioiden käyttöön, jos KATAKRI-osiot lisätään räätälöidysti taulukkolaskenta-pohjaiseen työvälineeseen.

Työvälineen avulla voidaan arvioida tietoturvallisuustasot suhteessa kansalliseen turvallisuusauditointikriteeristöön. Jokaiseen vaatimukseen luotiin linkki taulukon alla olevaan lisämateriaali osioon, joka sisältää kyseistä vaatimusta vastaavan ohjeistuksen kohdeyrityksessä. Näin ollen yritys on jatkuvasti ajan tasalla oman ohjeistuksen kanssa suhteessa kriteeristöön. Sovelluskäytön perusteella voidaan todeta, että tämä on edellytys, jos ja kun tietoturvallisuuteen liittyviä asioita auditoidaan, ja siten olemassa olevan dokumentaation avulla pystytään todistamaan yrityksen menettelytapa kyseessä olevassa kohdassa.

Tämänkaltaisissa, kehittämistehtävän sisältävissä projekteissa, on hyvä huomioida yrityksen omaan toimintaan liittyvä uuden työvälineen käyttöönotto ja käytettävyys. Tämän lisäksi on huomioitava, voiko tämän toimintamallin ja työvälineen avulla suoriutua myös ulkopuolisesta auditoinnista. Työvälineessä on kriteeriin liitetyn tukimateriaalin avulla pyritty varmistamaan se, että jokaisesta auditoitavasta kohdasta on olemassa myös dokumentoitua materiaalia toimintatavoista. Yrityskulttuureissa toisinaan ilmenevä tapa – ”näin nämä asiat on aina hoidettu ja tullaan hoitamaan” - ei edistä varsinaisen työn tarkoitusta ja hyödyntämistä organisaatiossa. Organisaation olisi hyvä lisätä työvälineen jokaiseen kohtaan dokumentaatio kyseisestä tavasta toimia, jolloin lähes kuka tahansa yrityksessä voisi toteuttaa auditoinnin kestävän palvelun. Tämän avulla on mahdollista säästää tietoturvallisuudesta vastaavan henkilön resursseissa. Mahdollista on, että kriteeristön käyttöönotto voi aiheuttaa yrityksille henkilöstöresurssivajetta, jos se tulee osaksi normaalia kaupankäyntiä.

3.4 Työvälineen käytön periaatteet

KATAKRI työvälinettä voidaan käyttää koko organisaation tietoturvallisuuden tason määrittämisen lisäksi yksittäisen palvelun tai prosessin tietoturvallisuuden tason omatoimiseen tarkasteluun. Kriteeristön sisältämät muut vastaavanlaiset paperidokumentit poistettiin käytöstä ja tämän avulla pyrittiin tavoitteissa asetettuihin ehtoihin eli helppokäyttöisyyteen ja ajantasaisuuteen. Uuteen KATAKRI työvälineeseen tallennetaan organisaatiossa oleva turvallisuuteen liittyvä tieto ja siten voidaan todeta, että tietoturvallisuuden tasot tässä muodossa ja yhteisessä fyysisessä paikassa ovat päivitysten ja muutosten hallinnan kannalta huomattavasti helpommin ylläpidettävissä ja organisaation tietoturvayksikön hallittavissa.

KATAKRI työvälineen käytön periaatteena on toteuttaa organisaatiossa selkeästi niitä vaatimuksia, joita auditointikonteksti sisältää. Tämä voidaan organisaatiossa operatiivisesti toteuttaa yksinkertaisen ja helppokäyttöisen sovelluksen käyttöönoton kautta. Koska työvälineessä

tietoturvallisuusosion osa-alueet ovat omilla välilehdillä, on tällä tavoin helpompaa hahmottaa tietoturvallisuusauditointikokonaisuutta, eikä tiedostokoko kasva niin isoksi.

Jokainen kriteeri ja siihen liittyvät vaatimukset ovat sellaisenaan kuin ne on kriteeristöön kirjoitettu. Sen lisäksi jokaiselle vaatimukselle on tehty ”status” sekä ”pakollisuus” – kentät. Status -kenttään voidaan valita yksi kolmesta eri vaihtoehdosta, sen hetkistä vaatimuksen täytön tilaa kuvaava vaihtoehto. Vaihtoehdot on kuvattu liikennevalo värein sekä tekstein. ”Vihreä valmis” kuvaa, että organisaatio tai auditoitava palvelu täyttää kyseessä olevan vaateen. ”Keltainen Aloitettu, ei valmis” kertoo, että kyseinen vaatimus täytetään jo jollain tasolla ja toimenpiteet vaatimuksen täyttämiseksi ovat jo käynnissä. ”Punainen Ei aloitettu” tarkoittaa, että auditoitava kohde ei täytä vaatimusta, eikä sen täyttämiseksi ole aloitettu toimenpiteitä. Pakollisuus -kenttä on enemmänkin lisätieto, jolla voidaan merkitä, jos auditoitavalla kohteella ei ole tarvetta täyttää kyseessä olevaa vaatimusta tai vaatimuksen korotettua tasoa. Tämän avulla voidaan merkitä siis esimerkiksi se, että ei ole tarvetta kiinnittää huomiota vaikka korkean tason vaatimusten täyttämiseen. ”Vihreä ohjaava” tarkoittaa, että kyseistä vaatimusta ei ole pakollista täyttää, mutta kriteerin vaatimus ohjaa kohteen tietoturvaa. ”Keltainen sopimuksiin” voidaan merkitä silloin, jos kyseisen kriteerin vaatimuksia on laitettava esimerkiksi alihankkijan kanssa tehtävään sopimukseen. ”Punainen pakollinen” kertoo sen, että auditoitavan kohteen on täytettävä kyseiset vaatimukset.

Tämän luokittelun avulla pystytään kohdentamaan resursseja sekä löytämään helpommin kehitettävät kohteet. Taulukon alla on myös tilaa jokaisen kriteerin tukimateriaalille. Siihen voidaan merkitä esimerkiksi lisätietoja jonkun vaatimuksen täytöstä auditoitavassa kohteessa. Kehittämistehtävässä organisaatiosta kerättiin tukimateriaalia kyseistä kriteeriä varten sekä tehtiin työvälineen täyttöä kuvaava ohje tai dokumentti. Kyseessä on kirjallinen dokumentti tai sen osa, jossa kuvataan vaatimuksen täyttö. Tämän avulla voidaan selvittää dokumentaation taso ja olemassa olo, eli auditointi ei perustu vain suulliseen tietoon tai vallitsevaan käytäntöön, vaan vaatimuksen täytöstä on dokumentti.

4 Case: Elisa Oyj

Tässä luvussa on kuvattu esimerkinomaisesti yhden tietoturvallisuusosion osa-alueen arviointi kohdeorganisaatiossa. Kyseinen arviointi on suoritettu luodun toimintamallin mukaisesti kehitetyllä työvälineellä. Arvioinnista saadut tulokset on avattu sanalliseen muotoon, jotta tulokset on saatu työssä esitettävään muotoon.

4.1 Hallinnollisen tietoturvallisuusosa-alueen arviointi Elisassa

4.1.1 I 101.0 Onko organisaation tietoturvallisuudella johdon tuki?

Hallinnollisen tietoturvallisuuden ensimmäisessä kriteerissä käsitellään organisaation tietoturvallisuuden lähtökohtia. Kriteerissä vaaditaan tietoturvallisuuden perusteiden hallintaa, ohjeistuksen ajantasaisuutta ja tietoon saattamista. Kriteerin pohjana käytetään ISO/IEC 27002 standardia, joka käsittää tietoturvallisuuden hallintaa sekä PCI DSS -tietoturvastandardia, joka määrittää standardeja maksuliikenteelle. Kriteerin lähtötason suositukset, jossa vaaditaan tietoturvallisuuden vähimmäistasot, ovat samat kuin kriteerin korkean tason vaatimukset.

Elisa: Kohdeorganisaatiolla on olemassa oleva dokumentaatio, joissa määritellään tietoturvallisuuden vastuut, toimintaperiaatteet sekä käytänteet. Tämä dokumentti on koko henkilöstön saatavilla yrityksen sisäisessä verkossa. Yrityksellä on myös olemassa oleva käytäntö uusien henkilöiden kouluttamiseksi, jotta he osaavat toimia yrityksen tietoturvaperiaatteiden mukaisesti.

4.1.2 I 102.0 Onko organisaatiolla dokumentoitu ohjelma tietoturvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?

Kysymys I 102.0 määrittelee vaatimukset organisaation dokumentoidun tietoturvasuunnitelman vähimmäisvaatimuksista. Organisaation tietoturvasuunnitelman tulee käsittää kuvaukset eri sektoreiden, kuten fyysisen ja hallinnollisen turvallisuuden, tietoturvasta, joissa on otettu huomioon vallitseva lainsäädäntö. Ohjeiden tulee olla kyseessä olevaan organisaatioon sopivat ja kriteerin toteutus todennetaan tarkistamalla ohjeet.

Elisa: Organisaatiolla on ajantasainen dokumentti, jossa kuvataan kaikki kriteerissä vaadittavat asiat. Tosin on hieman haasteellista määritellä, mikä on vaatimuksessa mainittu riittävä taso suhteessa organisaation kokoon.

4.1.3 I 103.0 Onko toiminnalle tärkeät suojattavat kohteet (toiminnot, tiedot, järjestelmät) tunnistettu?

Kriteerin täyttäminen vaatii suojattavien kohteiden sekä uhkien tunnistamista ja niihin varautumista. Suojattaville kohteille on määritetty vastuuhenkilöt ja suojattavaan kohteeseen kohdistuvaan riskiin on osattu varautua riittävästi. Korkean tason vaatimukset ovat samat kuin

perustasolla. Uhkien tunnistaminen voidaan todentaa käyttämällä KATAKRIn liitteenä olevaa lomaketta.

Elisa: Organisaatiolla on käytössä järjestelmällinen menetelmä, jolla voidaan arvioida palveluita, prosesseja sekä niiden tarvitsemat suojaustoimenpiteet (vrt. I104.0). Menetelmän avulla pystytään todentamaan kohteeseen kohdistuvat uhat. Menetelmää on jatkossa kehitettävä, koska edellisessä Viestintäviraston tarkastuksessa pidettiin määrittelyä riittämättömänä. Organisaatiossa on määritetty että, jokaisella järjestelmällä, sovelluksella, tiedolla ja prosessilla on oltava nimetty omistaja, joka viime kädessä on vastuussa kohteen kaikista toimista. Omistajalle tulee nimetä myös varahenkilö.

4.1.4 I 104.0 Miten suojattaviin kohteisiin kohdistuvia riskejä arvioidaan?

Kysymyksessä 1 103.0 todettuihin suojattaviin kohteisiin kohdistuvat riskit arvioidaan säännöllisesti ja järjestelmällisesti. Tietoihin kohdistuvia riskejä on yrityksen pystyttävä hallitsemaan sekä vähentämään. Riskien arvioinnin ja -hallinnan on oltava jatkuvaa sekä kaikkiin toimintavaiheisiin vaikuttavaa. Kriteerin hyväksytty täyttäminen voidaan todentaa kuvaamalla käytössä oleva turvatoimet sekä niistä syntyvät raportit.

Elisa: Organisaatiolla on olemassa järjestelmällinen menetelmä, jolla arvioidaan järjestelmiin, sovelluksiin ja tietoon kohdistuvia riskejä. Tämä järjestelmä täyttää kriteerissä asetetut vaatimukset riskien arvioinnille. Organisaation tulisi kiinnittää huomiota arvioinnin säännöllisyyteen sekä säännöllisyyden dokumentoitiin. Organisaatiolla tulisi olla järjestelmä, jonka avulla voidaan todentaa, koska kyseessä oleva kohde on viimeksi arvioitu.

4.1.5 I 105.0 Miten organisaation tietoturvallisuutta arvioidaan?

Kysymyksen lähtötason suositus edellyttää säännöllistä tietoturvallisuuden tason seuraamista. Korotettujen tasojen vaatimuksissa edellytetään systemaattista tietoturvallisuuden seurantaa ja analysointia sekä mahdollisten puutteiden kehitettämistä.

Elisa: Kriteerin vaatimusten täyttäminen on suuntaa-antava, koska vaateissa ei esimerkiksi määritellä mikä on tietoturvallisuuden tason säännöllinen tarkastelu, vaanmikä on hyväksyttävä väli tarkastelulle. Tietoturvallisuuden jatkuva arviointi ja kehittäminen tulisi organisaatiossa saada automaattiseksi toiminnaksi, jotta kyseessä oleva vaatimus saadaan täytettyä, sekä riippumaton katselmus tietoturvallisuuden tasosta tulisi tehdä suunnitellusti ja aikataulutetusti.

4.1.6 I 106.0 Onko tietoturvallisuudesta huolehdittu alihankinta-, palveluhankinta- ja muissa vastaavissa yhteistyökuvioissa?

Organisaatioille suositellaan lähtötasolla, että ne liittävät erillisen turvallisuussopimuksen tai tietoturvavaatimukset tarjouspyyntöihin. Vaatimuksissa vaaditaan alihankintaketjun riskien kartoittamista ja tarvittavien toimenpiteiden suorittamista. Mahdollinen tarkastusoikeus palveluntarjoajan prosesseihin tulee liittää sopimuksiin. Ulkoistettujen palveluiden osalta määritetään myös palvelutaso sekä toimenpidemallit mahdollisten poikkeamien varalle.

Elisa: Organisaatiolla on ajantasainen ohjeistus toiminnasta yhteistyökuvioissa. Palveluja ulkoistettaessa, jolloin Elisa toimii asiakkaana, palvelun omistaja Elisassa vastaa palvelun tietoturvallisuudesta. Ulkoistettavasta palvelusta edellytetään alihankkijalta jo tarjousvaiheessa asianmukaista turvallisuuskuvausta sekä sopimusvaiheessa turvallisuussopimusta. Yhteistyössä käytetään vähintään näiden tietoturvallisuusperiaatteiden mukaisia tietosuoja- ja tietoturvallisuusjärjestelyjä. Elisa varaa oikeuden itse tarkastaa tai tarkistuttaa kolmannella osapuolella kaikkien Elisalle tuotettavien palveluiden komponentit ja kokonaisuudet.

4.1.7 I 107.0 Miten organisaatiossa toimitaan tietoturvapoikkeamatilanteissa?

Tietoturvapoikkeamien osalta lähtötason suositukset edellyttävät, että tietoturvapoikkeaman sattuessa organisaation toiminta on suunniteltua, toiminta on ohjeistettua ja viestintä on hoidettu asianmukaisella tavalla. Ylemmillä tasoilla organisaation toiminnan tulee lisäksi olla harjoiteltua sekä poikkeamat on dokumentoitu.

Elisa: Organisaatiossa on suunniteltu, ohjeistettu sekä varmistettu toiminta tietoturvapoikkeamatilanteissa. Organisaation tulee kiinnittää huomiota edellä mainitun toiminnan säännölliseen harjoitteluun ja sen dokumentointiin.

4.1.8 I 108.0 Onko toiminnan lakisääteiset vaatimukset huomioitu?

Organisaatio on tunnistanut toimintaa ohjaavat lakisääteiset vastuut ja velvoitteet ja ne on täytetty. Organisaatiossa käsitellään turvaluokiteltuja tietoja lakien ja säädösten edellyttämällä tavalla koko niiden elinkaaren ajan.

Elisa: Organisaation kaikessa toiminnassa noudatetaan kyseisen markkina-alueen vallitsevia lakeja ja se on myös dokumentoitu. Sähköisen viestinnän tietosuojalain tulkinta löytyy organisaation toimittamasta käsikirjasta. Luottamuksellisiksi ja salaisiksi luokiteltujen tietojen käsittelytapahtumista tulee tarvittaessa jäädä käsittelyloki. Erityisesti on huomioitu sähköisen viestinnän tietosuojalain (SVTsL) § 15 vaatimukset tunnistamistietojen käsittelyn tallentamisesta sekä Viestintäviraston 47C/2009.

4.1.9 I 109.0 Onko organisaatiossa menettely, jonka avulla varmistetaan, että merkittävät tietojenkäsittely-ympäristön muutokset tapahtuvat hallitusti?

Tämän kriteerin ainoa vaatimus on, että organisaatiolla on käytössä muutoshallintamenettely. Ennen tietojenkäsittelyyn liittyviä muutoksia, tulee uusia toimintatapoja tarkastella organisaation tietoturvapolitiikan kautta sekä muutokset tulee testata ja tarkastaa ennen käyttöönottoa.

Elisa: Organisaatiolla on olemassa oleva muutoksenhallintamenettely tietojenkäsittely-ympäristön muutoksille. Menettely pitää sisällään tarvittavat komponentit prosessille, kuten muutoksen tunnistamisen, muutoksen suunnittelun ja testauksen sekä mahdollisten turvallisuusvaikutusten arvioinnin.

4.2 Toimintamallista saavutettuja tuloksia ja niiden arviointia

Tässä kappaleessa arvioidaan tietoturvallisuuden tasojen analysoinnin tulokset KATAKRIn suhteen vain yleisellä tasolla. Tietoturvallisuusosa-alueen yksittäiset kriteerit, vaatimukset ja niiden täyttö on kuvattu lyhyesti edellä olevassa kappaleessa esimerkinomaisesti kohdeorganisaation osalta.

Kansallista turvallisuusauditointikriteeristöä työstettiin organisaatiossa kehittämäni työvälineen kautta. Työvälineeseen kerättiin jokaista kriteeriä vastaava dokumentti tai sen osa. Käytännössä se oli ohje, raportti tai vastaava. Vaatimusta ei ollut mahdollista täyttää hyväksytysti ilman dokumentaatiota eli ”näin tehdään” – tieto ei riittänyt. Dokumentaation keräämisen jälkeen dokumentaation yhteneväisyys suhteessa kriteeristön vaatimuksiin arvioitiin yhdessä organisaation tietoturvallisuudesta vastaavan henkilön kanssa. Tietoturvallisuudesta vastaavan henkilön kanssa merkittiin työvälineeseen organisaation toiminnan tasoa vastaava status aiemmin tässä työssä kuvatulla tavalla.

Tämän työstämisen ja tulosten analysoinnin avulla saimme kuvattua työvälineeseen organisaation tietoturvallisuuden taso suhteessa kansallisen turvallisuusauditointikriteeristön vaatimusten tasoon. Esimerkkinä olleen osa-alueen vaateet organisaatio täytti hyvin. Tietoturvallisuudesta vastaava henkilö sai myös tiedon, minkä vaateiden osalta organisaatiolla olisi mahdollisen auditoinnin tullessa parannettavaa. Parannettavaa voi olla itse toiminnassa tai toiminnan dokumentoinnissa, jonka merkitsemiseen ei vielä tässä työvälineen versiossa ole mahdollisuutta. Tulosten ja työvälinen ajantasaisuuden varmistamiseksi organisaatiossa olisi luotava toimintamalli, jonka avulla muutosten jälkeen tarkistettaisiin muuttunut taso suhteessa kriteeristöön. Tällöin työvälineestä saadaan suurin mahdollinen hyöty.

4.3 Kehitysehdotukset kohdeorganisaatiolle

Organisaation yleisen tason vertaaminen kansallisen turvallisuusauditointiktiteeristön vaatimuksiin antoi kuvan organisaation tietoturvallisuuden tasosta. Kriteeristön käyttöönotto työvälineen avulla antoi organisaation vastuuhenkilöille dokumentoidun tiedon senhetkisestä tasosta. Jotta käyttöönoton ja työvälineen kaikki hyöty saadaan irti, olisi organisaation nimettävä vastuuhenkilö päivittämään ja ylläpitämään tietoa. Organisaation tietoturvallisuuden taso on kriteeristön suhteen hyvällä tasolla. Suurimmat heikkoudet löytyvät sellaisista vaatimuksista, joissa vaaditaan säännöllisyyttä, ajantasaisuutta tai jatkuvuutta. Myös sellaisten vaatimusten täytössä oli puutteita, joissa vaadittiin kyseisen toiminnan harjoittelua. Näitä puutteita voidaan parantaa tietoturvallisuuden pitkäjänteisellä suunnittelulla, riittävillä resursseilla sekä ohjeiden päivittämisellä. Työvälineen ylläpidon avulla voidaan myös pitää yllä tietoa organisaation tietoturvan tasosta. Näin ollen voidaan parantaa ja helpottaa suunnittelua, sekä korjaavien toimenpiteiden suuntausta oikeisiin asioihin ja kohteisiin.

4.4 Työvälineen arviointi

KATAKRI -työvälineen avulla on mahdollista ylläpitää tietoturvallisuuden tason tilaa suhteessa kansalliseen turvallisuusauditointikriteeristöön. Samalla pohjalla voidaan toteuttaa myös muut KATAKRI:n osiot. Kriteeristön kattavuuden ja ajankohtaisuuden vuoksi työvälineellä saadaan myös hyvä kuva tietoturvallisuuden yleistilasta. Työväline vaatii työtä ajan tasalla pitämisen suhteen melko paljon. Periaatteessa jokaisen muutoksen jälkeen tulisi tarkistaa, onko se vaikuttanut jonkun kriteerin hyväksyttävään täyttöön. Tämän osalta työväline on hieman raskasta ylläpitää. Kriteeristön käyttöönottoon työväline soveltui mielestäni hyvin, koska sen avulla saatiin yksi dokumentti, josta löytyy tarvittava tieto Elisan osalta. Työvälineen avulla tietoturvallisuudesta vastaavan henkilön on helpompi lähteä miettimään kriteeristön soveltuvuutta sekä organisaation tietoturvallisuuden kehittämistä. Sen avulla on myös toivottavasti

organisaation helpompi ottaa osaa tulevaisuudessa sellaiseen tarjouskilpailuun, jossa vaaditaan kansallisen turvallisuusauditointikriteeristön täyttöä.

Jos työvälinettä kehittäisi, olisi hyvä luoda myös mahdollisuus raportin tai pienen muistion kirjoittamiselle kunkin vaatimuksen kohdalle. Näin ollen voitaisiin lisätä työvälineen antamaa informaatiota, esimerkiksi lisäämällä siihen seuraavan mahdollisesti muutoksia aiheuttavan päivityksen päivämäärän. Työvälineeseen olisi hyvä myös kehittää jonkinlainen raportointijärjestelmä, jos sen ottaa suuremmassa mittasuhteessa käyttöön. Järjestelmän avulla saataisiin ulos raportti, joka kertoisi hyväksyttävästi täytettyjen ja täyttämättömien vaatimusten määrän sekä statuksen.

5 Pohdintaa

Mielestäni kansallisen turvallisuusauditointikriteeristön työryhmä on onnistunut työssään hyvin. Kaikki kriteerit olivat relevantteja organisaation päivittäiselle tietoturvallisuustyölle. Vaatimukset täyttämällä tai niiden hyväksyttävää täyttöä kohti pyrkimällä, on mahdollisuus saada organisaation tietoturvallisuus todella hyvälle tasolle. Suurin osa kriteereistä sekä vaatimuksista oli kirjoitettu helposti ymmärrettävään muotoon ja väärinymmärryksen mahdollisuus oli pyritty minimoimaan. Kriteereiden ja vaatimusten tarkkuus on todella tärkeää, jotta mahdolliset väärinkäsitykset saadaan minimoitua. Sanojen paikan vaihtaminen saattaa muuttaa vaatimuksia tai niiden ymmärtämistä oleellisesti. Muutaman yksittäisen kriteerin tai vaatimuksen kohdalla oli luettava kriteeriä todella tarkasti ja mietittävä ideaa. Onneksi lisätieto -kohdassa oli usein avattu tai pyritty muuten helpottamaan kriteeriin asetettujen vaatimusten oikeanlaista ymmärtämistä.

Arviointityön haasteena ja mahdollisena ongelmana on yksittäisen vaatimuksen sovellettavuus tiettyyn toimialaan tai toimitettuun palveluun, johon kriteeristöä mahdollisesti käytettäisiin. Arviointityössä ei aina pystytä rajaamaan tarpeettomia tai turhia vaateita pois kuin tarkasteltavan näkökulman osalta, joka voi olla koko yrityksen toimintakenttä tai yksittäinen tarjottava palvelu. Tutkimukseni mukaan kansallinen turvallisuusauditointikriteeristöä ei voida toteuttaa alkuperäisen sisällön mukaisesti, jos sieltä rajataan tai jätetään pois yksittäisiä vaatimuksia tai kokonaisuuksia. Kriteeristön henki kun on ”kaikki tai ei mitään” – periaatteella. Esimerkiksi, jos kohdeyritys haluaa täyttää kriteeristön tai sen tietyn tason, on siihen pystyttävä koko kriteeristön osalta.

Työvälineen kehittämisen yhteydessä ongelmaksi ilmeni se, että läheskään kaikki toiminnot eivät ole sellaisia, joilla olisi tarvetta täyttää koko kriteeristö. Kehittämistyössä luotua työvä-

linettä voidaan muokata vastaamaan yrityksen kulloisenkin palvelun tai järjestelmän vaatimuksia, lähtökohtana ei ole pelkästään kriteeristö ja sen vaatimusten täyttö, vaan myös yrityksen oma auditointi ja sen kautta oman toiminnan kehittäminen. Työvälineen avulla pystytään tekemään kriteeristön auditointi niiltä osin kuin se on tarpeellista.

Kansallisen turvallisuusauditointikriteeristön, erityisesti tietoturvallisuusosa-alueen osalta, on tärkeää, että joku taho/organisaatio ottaa kriteeristön ylläpidon vastuulleen. Tietoturvallisuuden vaatimukset, tarpeet ja toteutustavat muuttuvat huimalla vauhdilla ja sen vuoksi myös kriteeristön tulisi pysyä ajantasaisena.

Kriteeristön markkinointi yrityksille olisi tärkeää, jotta ne ottaisivat sen käyttöön ja alkaisivat kehittää omaa turvallisuustyötään sen asettamien vaatimusten suuntaan. Tämä siksi, että kriteeristö on todella hyvä kokonaisuus turvallisuuden koko kentästä ja sen avulla on mahdollista tulevaisuudessa osallistua kansallisiin kilpailutuksiin.

Ajantasainen ylläpito ja markkinointi ovat mielestäni tällä hetkellä tärkeimmät kynnyskysymykset kriteeristön tulevaisuuden kannalta. Ilman markkinointia on mahdollista, että yritykset eivät ota oma-aloitteisesti kriteeristöä käyttöön. Ilman ylläpitoa käy siten, kuin on jo hieman käynyt. Viestintäviraston Timo Lehtimäki totesi haastattelussaan toukokuussa, että Viestintävirasto on jo useaan otteeseen päivittänyt itse kriteeristön tietoturvallisuusosa-aluetta, eikä tule sitä julkaistussa muodossa enää käyttämään. Tämä aiheuttaa ongelmia monella tavalla, koska Viestintävirasto olisi todennäköisesti se viranomainen, joka voisi kriteeristön tietoturvallisuus osa-alueen auditointeja tehdä. Koska he ovat jo päivittäneet kriteeristön paremmin omaan käyttöön sopivaksi, ei auditointien suorittaminen ole heidän intresseissään kovin korkealla. Myös kriteeristön idea, valtionhallinnon kilpailutusten vaatimuksina ei oikein toimi, jos valtionhallinnon yksikkö tulee mahdollisesti jotain muuta kilpailutuksessa vaatimaan. (Lehtimäki 2010.)

Tämän työn puutteet ovat rajauksesta johtuneen materiaalin suppeus niin teoreettisessa kuin tutkittavassakin aineistossa. Myös teoria-aineiston vähäistä käyttöä voidaan pitää työn puutteena.

Tässä työssä esitetyt tulokset sekä päätelmät eivät ole yleistettävissä vastaamaan yleistä tasoa tai yleistä käsitystä KATAKRI:sta. Tutkimuksen otannan rajaus ja suppeus vaikuttavat siihen, että tuloksia voidaan pitkällä aikavälillä verrata vain Elisa Oyj:n vastaaviin tutkimuksiin. Työssä kehitetty työväline on mahdollista ottaa käyttöön koko kohdeorganisaatiossa, mutta myös missä tahansa muussa organisaatiossa pienten muutosten avulla. Jatkotutkimuksena tällä työlle kohdeorganisaatiossa voidaan tutkia KATAKRI:n kaikkien osioiden käyttöönottoa organisaatiossa.

6 Johtopäätökset

Kansallinen turvallisuusauditointikriteeristö on toimiva kokonaisuus organisaation omaehtoiseen turvallisuustyöhön sekä käytettäväksi valtionhallinnon ja yritysten välisessä toiminnassa turvallisuuden tason mittaamiseen. Kansallisen turvallisuusauditointikriteeristön vaatimukset täyttämällä yrityksen turvallisuus on hyvällä tasolla. Kriteeristön käyttö kertoo myös yrityksen hyvästä turvallisuuskulttuurista. Tämä on todettu eri tahojen toimesta, niin yritys- kuin viranomaisorganisaatioissa.

Kansallisen turvallisuusauditointikriteeristön suurin uhka liittyy mielestäni sen ajantasaisuuteen ja ajantasaisena pidettävyyteen. KATAKRIn luonnissa vastuussa olleiden organisaatioiden tulisi mielestäni perustaa seuranta-/kehitystyöryhmä, jonka tehtävänä olisi pitää KATAKRI ajantasaisena ja tällä tavoin säilyttää kriteeristön merkitys suomalaisen turvallisuuskulttuurin luonnissa. Työryhmän tehtävinä olisi säännöllisin väliajoin, esimerkiksi vuosittain, tarkastella kriteereiden ja vaatimusten relevanttius. Lisäksi tulisi tarvittaessa päivittää kriteereitä ja/tai niiden vaatimuksia, jos esimerkiksi niiden toimimattomuus käytännön työssä havaitaan tai kriteeriin vaikuttanut asetus/laki on muuttunut. Työryhmän tulisi sisältää edustus niin viranomais- kuin yritysorganisaatioista, aivan kuten kriteeristön luonnissakin.

Työssä käsitellyn organisaation osalta suurimmat puutteet liittyvät vaatimuksiin, joissa vaaditaan säännöllistä tarkastelua tai harjoittelua. Jos KATAKRI otetaan organisaatiossa käyttöön, mielestäni organisaation tulee luoda seurantaryhmä, joka vastaa vaatimusten täyttämisestä. Seurantaryhmässä tulisi olla edustus tarvittavista yksiköistä, kuten tietoturvapäällikkö, turvallisuusjohtaja, fyysisestä turvallisuudesta vastaava henkilö sekä muita tarvittavia asiantuntijoita. Kuitenkin siten, että kriteeristön jokaisen osa-alueen turvallisuudesta vastaava henkilö olisi ryhmässä. Säännöllisten seurantakokousten avulla pidettäisiin organisaation turvallisuustaso vaaditulla ja halutulla tasolla.

Lähteet

Airaksinen, T & Vilkka, H. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Elisa Oyj 2010. Tietoa Elisasta. Viitattu 17.10.2010. http://www.elisa.fi/elisa-oyj/tietoa_elisasta/

Hakala, J. T. 2004. Opinnäytetyöopas ammattikorkeakouluille. Helsinki: Gaudeamus.

Kesäläinen, M. 2010. KATAKRI mittaa turvallisuuden tasoa. Turvallisuus 2/2010, 12–14.

Kreus, J. 2010. Johtamisen käsikirjat: Turvallisuuden hallinta. Helsinki: Kauppalehti

Kansallinen turvallisuusauditointikriteeristö 2009. Puolustusministeriö. Tulostettu 3.1.2010. http://www.defmin.fi/files/1525/Katakri.pdf

Lampela, L. 2010. Yhteisöturvallisuustodistus on merkki luotettavasta sopimuskumppanista. Turvallisuus 5/2010, 18–20.

Puolustusministeriö 2010. Kansallinen turvallisuusauditointikriteeristö. Viitattu 7.4.2010. http://www.defmin.fi/index.phtml?s=481

Valtiovarainministeriö 2009. Valtionhallinnon ICT-varautuminen, Jatkuvuuden hallinta ja tiedon turvaaminen. Viitattu 25.5.2010. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20090820Lausun/02_VARE_vaatimukset_ver_2_02_20_8_2009_.pdf

Valtiovarainministeriö 2008. Tietoaineistojen turvallinen käsittely. Viitattu 20.4.2010. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/TietoaineistojenTurvallinenKasittely_v14.pdf

Viestintävirasto 2010. Asiointi ja info. Viitattu 14.10.2010. http://www.viestintavirasto.fi/index/asiointi-info/viestintavirasto.html

Julkaisemattomat lähteet

Hammarberg, R. 2010. Turvallisuusjohtajan haastattelu 15.3.2010. Nokia Oyj. Espoo.

Laakso, P. 2010. Tietoturvapäällikön haastattelu 3.3.2010. Itella Oyj. Espoo.

Lehtimäki, T. 2010. Viestintävirasto, verkot ja turvallisuus tulosalueen johtaja. haastattelu 11.5.2010. Viestintävirasto. Helsinki

Tiihonen, K. 2010. Elinkeinoelämän keskusliiton EK:n Yritysturvallisuustoimiston päällikön haastattelu 15.4.2010. Elinkeinoelämän keskusliitto EK. Helsinki

Kuvat

Liitteet

Liite 1: Kansallinen turvallisuusauditointikriteeristö tietoturvallisuusosio

Hallinnollinen tietoturvallisuus, osa-alue I100

Hallinnollisen tietoturvallisuuden osiossa käsitellään yleisiä tietoturvakäytänteitä sekä riskienarviointia. Osa-alue I100 kattaa organisaation tietoturvan periaatteet, toiminnan suuntaviivat sekä yleiset tietoturva-ohjeistukset organisaatiossa. Kyseisessä osa-alueessa ei vielä pureuduta kovinkaan syvällisesti yksityiskohtiin tai teknisiin määritelmiin, vaan pyritään löytämään organisaation linjaukset ja ohjeistukset. Kriteeristö antaa mahdollisuuden organisaatiolle monessakin kohtaa suorittaa vaaditut asiat haluamallaan tavalla, vaatimuksissa ei siis ole määritetty toteuttamistapaa, ainoastaan lopputulos.

I 101.0 Onko organisaation tietoturvallisuudella johdon tuki?

Hallinnollisen tietoturvallisuuden ensimmäisessä kriteerissä käsitellään organisaation tietoturvallisuuden lähtökohtia. Kriteerissä vaaditaan tietoturvallisuuden perusteiden hallintaa, ohjeistuksen ajantasaisuutta ja tietoon saattamista. Kriteerin pohjana käytetään ISO/IEC 27002 standardia, joka käsittää tietoturvallisuuden hallintaa sekä PCI DSS -tietoturvastandardia, joka määrittää standardeja maksuliikenteelle. Kriteerin lähtötason suositukset, jossa vaaditaan tietoturvallisuuden vähimmäistasot, ovat samat kuin kriteerin korkean tason vaatimukset.

I 102.0 Onko organisaatiolla dokumentoitu ohjelma tietoturvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?

Kysymys I 102.0 määrittelee vaatimukset organisaation dokumentoidun tietoturvasuunnitelman vähimmäisvaatimuksista. Organisaation tietoturvasuunnitelman tulee käsittää kuvaukset eri sektoreiden, kuten fyysisen ja hallinnollisen turvallisuuden, tietoturvasta, joissa on otettu huomioon vallitseva lainsäädäntö. Ohjeiden tulee olla kyseessä olevaan organisaatioon sopivat ja kriteerin toteutus todennetaan tarkistamalla ohjeet.

I 103.0 Onko toiminnalle tärkeät suojattavat kohteet (toiminnot, tiedot, järjestelmät) tunnistettu?

Kriteerin täyttäminen vaatii suojattavien kohteiden sekä uhkien tunnistamista ja niihin varautumista. Suojattaville kohteille on määritetty vastuuhenkilöt ja suojattavaan kohteeseen kohdistuvaan riskiin on osattu varautua riittävästi. Korkean tason vaatimukset ovat samat kuin perustasolla. Uhkien tunnistaminen voidaan todentaa käyttämällä liitteenä olevaa lomaketta.

I 104.0 Miten suojattaviin kohteisiin kohdistuvia riskejä arvioidaan?

Kysymyksessä 1 103.0 todettuihin suojattaviin kohteisiin kohdistuvat riskit arvioidaan säännöllisesti ja järjestelmällisesti. Tietoihin kohdistuvia riskejä on yrityksen pystyttävä hallitsemaan sekä vähentämään. Riskien arvioinnin ja -hallinnan on oltava jatkuvaa sekä kaikkiin toimintavaiheisiin vaikuttavaa. Kriteerin hyväksytty täyttäminen voidaan todentaa kuvaamalla käytössä oleva turvatoimet sekä niistä syntyvät raportit

I 105.0 Miten organisaation tietoturvallisuutta arvioidaan?

Kysymyksen lähtötason suositus edellyttää säännöllistä tietoturvallisuuden tason seuraamista. Korotettujen tasojen vaatimuksissa edellytetään systemaattista tietoturvallisuuden seurantaa ja analysointi sekä mahdollisia puutteita kehitetään.

I 106.0 Onko tietoturvallisuudesta huolehdittu alihankinta-, palveluhankinta- ja muissa vastaavissa yhteistyökuvioissa?

Organisaatioille suositellaan lähtötasolla, että ne liittävät erillisen turvallisuussopimuksen tai tietoturvavaatimukset tarjouspyyntöihin. Vaatimuksissa vaaditaan alihankintaketjun riskien kartoittamista ja tarvittavien toimenpiteiden suorittamista sekä mahdollinen tarkastusoikeus palveluntarjoajan prosesseihin liitetään sopimuksiin. Ulkoistettujen palveluiden osalta määritetään myös palvelutaso sekä toimenpidemallit mahdollisten poikkeamien varalle.

I 107.0 Miten organisaatiossa toimitaan tietoturvapoikkeamatilanteissa?

Tietoturvapoikkeamien osalta organisaation on täytynyt tehdä jo lähtötason suositukset täyttääkseen, että tietoturvapoikkeaman sattuessa organisaation toiminta on suunniteltua, toiminta on ohjeistettua ja viestintä on hoidettu asianmukaisella tavalla. Ylemmillä tasoilla organisaation toiminnan tulee lisäksi olla harjoiteltua sekä poikkeamat on dokumentoitu.

I 108.0 Onko toiminnan lakisääteiset vaatimukset huomioitu?

Organisaatio on tunnistanut toimintaa ohjaavat lakisääteiset vastuut ja velvoitteet ja ne on täytetty. Organisaatiossa käsitellään turvaluokiteltuja tietoja lakien ja säädösten edellyttämällä tavalla koko niiden elinkaaren ajan.

I 109.0 Onko organisaatiossa menettely, jonka avulla varmistetaan, että merkittävät tietojenkäsittely-ympäristön muutokset tapahtuvat hallitusti?

Kriteerin ainut vaatimus on, että organisaatiolla on käytössä muutoshallintamenettely, jolloin ennen tietojenkäsittelyyn liittyviä muutoksia, tulee uusia toimintatapoja tarkastella organisaation tietoturvapolitiikan kautta sekä muutokset tulee testata ja tarkastaa ennen käyttöönottoa.

Henkilöstöturvallisuus osana tietoturvallisuutta, osa-alue I200

Henkilöstöturvallisuuden osa-alueessa käsitellään käyttöoikeuksiin, tietoturvallisuusohjeisiin, tietoturvallisuuden koulutukseen sekä salassapitoasioihin liittyviä tietoturvavaateita. Henkilöstö on organisaation voimavara, mutta useimmiten suurin uhka organisaation tietoturvalle kohdistuu omasta henkilökunnasta. Henkilökunta on kuitenkin se tekijä, joka käsittelee, muokkaa, tallentaa ja välittää tietoa, myös luottamuksellista. Henkilöstöturvallisuudella tässä aihepiirissä tarkoitetaan omasta henkilöstöstä aiheutuvien riskien hallintaa, ei siis henkilöturvallisuutta, josta puhuttaessa tarkoitetaan henkilöstöön kohdistuvien uhkien torjumista.

I 201.0 Hallitaanko kaikkien käyttäjien pääsy- ja käyttöoikeuksia hyvän tiedonhallintatavan mukaan?

Kriteerin täyttö edellyttää organisaatiolta suunniteltua käyttöoikeuksien myöntämisprosessia ja oikea menettelytapa on koko organisaation tiedossa. Prosessiin kuuluu selkeät ohjeet oikeuksien myöntämiseen, niin fyysiset kuin järjestelmät, myöntämisen edellytyksiin, oikeuksien hallintaan kuin oikeuksien poistamiseen. Järjestelmät sekä kulkuoikeudet on pystyttävä organisaatiossa rajaamaan siten, että oikeudet voidaan antaa vain niihin tiloihin ja järjestelmiin kuin on tarpeen.

I 202.0 Onko salassapito- tai vaitiolositoumukset laadittu ja otettu käyttöön siten, että ne vastaavat organisaation tietojen suojaamistarpeita?

Organisaatiolla tulee olla ohjeistus salassapitositoumusten laadinnasta, eli mitkä tiedot ovat sellaisia, joihin pääsyoikeuden saadakseen on kirjoitettava salassapitositoumus. Ohjeistuksen on koskettava oman henkilökunnan lisäksi kaikkia muitakin toimijoita tiedon luotettavuuden takaamiseksi.

I 203.0 Onko avainhenkilöt sekä organisaation riippuvuus heistä tunnistettu?

Vaatimusten täyttäminen edellyttää organisaatiolta avainhenkilöiden tunnistamisen lisäksi varahenkilöjärjestelmän luontia ja ylläpitoa. Ylemmillä tasoilla avainhenkilöt tulee kouluttaa häiriötilanteiden varalle ja toiminta kriisitilanteissa tulee harjoitella.

I 204.0 Onko organisaatiossa huolehdittu riittävästä ohjeistuksesta, koulutuksesta ja tiedotuksesta?

Organisaatio on luonut ohjeet, kuinka henkilö perehdytetään organisaation tietoturvaperiaatteisiin ja -ohjeisiin. Ohjeiden tulee sisältää normaalin käytön lisäksi myös esimerkiksi etäkäytön ja työmatkat. Ylempien tasojen vaatimukset vaativat erillisiä ohjeita salassa pidettävien tietojen käsittelylle, henkilötietojen käsittelylle sekä tietoturva uhkien tiedottamisen ajantasaisuudesta organisaatiossa.

I 205.0 Onko tietoon ja tietojenkäsittelypalveluihin määritetty hyväksyttävän käytön säännöt ja onko niistä tiedotettu henkilöstölle?

Kriteerin täyttö edellyttää, että henkilöstölle on selvästi informoitu sallitun henkilökohtaisen käytön rajat ja niissä on kerrottu, mikä on hyväksyttävän käytön rajat, esimerkiksi palveluiden, levytilan käytön sekä sähköpostin käytön suhteen.

I 206.0 Valvotaanko organisaatiossa tietoturvaohjeiden noudattamista ja onko tietoturvarikkomusten käsittely ja seuraukset määritelty?

Perusedellytys kysymykseen on, että ohjeiden noudattamista valvotaan ja se, että mahdollisiin rikkeisiin puututaan tarvittavin keinoin. Korkeampien tasojen vaatimusten saavuttamiseksi organisaation on määritettävä rikkomukset sekä niistä seuraavat rangaistukset ja niiden on oltava yhtenäiset koko organisaatiossa.

I 207.0 Millaisia menettelytapoja organisaatiolla on tunnistaa ulkopuoliset työntekijät sekä vierailijat?

Organisaatiolla tulee olla ohjeistus vierailijoiden isännöinnistä, jotta lähtötaso on saavutettu. Korotettujen tasojen vaatimusten täyttämiseksi organisaation on ohjeistettu valvomaan vierailijoita, käyttämään tunnisteita sekä puuttumaan ilman tunnisteita liikkuvien henkilöiden kulkuun.

Fyysinen turvallisuus osana tietoturvallisuutta, osa-alue I300

Fyysisen turvallisuuden osa-alueessa keskitytään tietoa sisältävien tilojen fyysiseen suojaukseen. Kuten työn aiemmassa vaiheessa kerrottiin, kriteeristö on tehty yhtenäiseksi kokonaisuudeksi. Tietoturvallisuuden fyysisen turvallisuuden osuudessa viitataan myös kriteeristön toiseen osa-alueeseen eli fyysiseen turvallisuuteen. Myös hajasäteilyn riskiin on uudessa kriteeristössä kiinnitetty huomiota, vaikka siihen ei ole juurikaan kiinnitetty huomiota viimeisten vuosien aikana suomalaisessa yritysmaailmassa. Matti Kesäläinen kantaa asiasta huolta uusimmassa Turvallisuus-lehden numerossa 2/2010, jossa hän toteaa, että kontrolloimattoman elektromagneettisen säteilyn estämiseen pitäisi kiinnittää enemmän huomiota korkeimpien turvallisuusluokkien tiloissa. (Kesäläinen 2010.)

I 301.0 Miten suojattavaa tietoa sisältävän tilan fyysisestä turvallisuudesta on huolehdittu?

Lähtötason suositusten mukaan yrityksen tulisi suojata toimitilat sekä tietoa sisältävät laitteistot suoritetun riskien arvioinnin mukaan. Suojattavat tiedot tulee sijoittaa siten, että ulkopuolisilla tai asiattomilla henkilöillä ei ole pääsyä tilaan. Ylemmän tason vaatimukset on määritetty fyysisen turvallisuuden osiossa.

I 302.0 Tapahtuvatko laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet vain valvottuna?

Kriteeristön vaatimusten täyttämiseksi tulee tilasta tehdä riskienarviointi ja sen pohjalta tehdä ohjeistus, jossa otetaan kantaa millä tavoin edellä mainitut toimenpiteet tulee tilassa suorittaa. Vaateiden täyttämiseksi voidaan edellyttää esimerkiksi henkilöstä tehtävää turvallisuusselvitystä.

I 303.0 Miten on varauduttu salakuunteluun, hajasäteilyyn ja vastaaviin uhkiin?

Lähtötason suositukset edellyttävät ohjeistuksen olemassa olo, henkilökuntaa tulee informoida siitä, että salassa pidettäviä tietoja ei jaeta sellaisessa ympäristössä, jossa ne voivat kulkeutua asiattomien saataville. Myös toimitilojen, kuten neuvotteluhuoneiden, riittävästä äänieristyksestä tulee huolehtia. Korotettujen tasojen vaatimuksissa tulee arvioida mahdollisen salakuuntelun sekä hajasäteilyn aiheuttaman tietovuodon mahdollisuus.

I 304.0 Onko LVIS-järjestelyt varmistettu niin, että ne vastaavat organisaation toimintavaatimuksia?

Kriittisten laitteistojen tunnistamisen ja tarvittavien varajärjestelmien luonti on toteutettu. Kriittisten laitteistojen liittämisestä häiriöttömän sähkönsyötön piiriin ja sen testaus korotetun ja korkean tason vaatimukset vaativissa kohteissa.

I 305.0 Ovatko näyttöpäätteet asetetut siten, ettei salassa pidettävää tietoa paljastu ohikulkijoille tai muille asiattomille?

Tietoliikenneturvallisuus, osa-alue I 401.0

Tietoliikenneturvallisuus osa-alue sisältää tietoliikenneverkkoon, palomuureihin, tietoliikenteen suodatukseen, langattomien verkkojen sekä niiden valvontaan liittyviä vaateita. Kysymyksessä I 402.0 vaaditaan palomuureilta ja muilta vastaavilta liikennettä suodattavilta laitteilta yksityiskohtaisia sääntöjä suodattamisesta.

I 401.0 Onko tietoliikenneverkon rakenne turvallinen?

Edellytetään, että organisaatiolla on käytössään perussuojausmenetelmät omaa verkkoaan suojaamaan, kuten palomuuriratkaisu. Vaaditaan vähintään, että organisaation oma verkko on erotettu palomuurilla Internetistä. Perustason vaatimuksissa edellytetään organisaation verkon jakoa vyöhykkeisiin sekä eri tietoturvatason järjestelmien sijoittamista eri vyöhykkeille.

I402.0 Ovatko palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöt hyvien tietoturvaperiaatteiden mukaisia?

Lähtötason suosituksissa suositetaan, että erikseen sallittu liikenne sallittu, kaikki muu kielletty sekä määrittelemättömän liikenteen eston. Perustason vaatimuksissa vaaditaan palomuuriratkaisun yksityiskohtaista konfiguroimista.

I 403.0 Miten varmistutaan siitä, että liikennettä suodattavat tai valvovat järjestelmät toimivat halutulla tavalla?

Organisaation palomuurit tulee olla oikein konfiguroidut, palomuurien ylläpito ja huolto vastuutettu sekä käytössä olevat suodatussäännöt tulee dokumentoitu. Korkeampien tasojen vaatimusten täyttö edellyttää halutun toiminnan seurantaa ja tarkastuksia.

I 404.0 Onko hallintayhteydet suojattu asianmukaisesti?

Palvelimet ja työasemat tulee olla suojattu sekä hallintaliikenne salattua.

I 405.0

Ovatko verkon aktiivilaitteet kovennettuja (konfiguroituja organisaation omilla parametreilla tehdasparametrien sijaan)?

Aktiivilaitteiden koventaminen vaatii vähintään oletus salasanojen vaihdon, tarpeellisten verkkopalveluiden päällä pidon sekä turvapäivitysten ajantasaisuuden. Korkeampien tasojen vaatimukset ovat samat kuin lähtötasojen suositukset.

I 406.0 Ovatko langattomien verkkojen perussuojaukset käytössä?

Langattomien verkkojen käyttö tulee salata ja se sallitaan vain tunnistetuille käyttäjille, myös mahdollisen vierasverkon käyttö tulisi suojata salasanalla. Myös langattomien verkkojen laitteiden sekä ratkaisujen tulee täyttää korotetun tietoturvatason vaatimukset, korotetuilla vaatimustasoilla.

I 407.0 Onko sisäverkon rakenteen näkyminen Internetiin estetty?

Sisäverkon rakenteen ja sen suojauksen tulee olla sellainen, ettei tietoliikenne paljasta organisaation verkon rakennetta.

I 408.0 Miten verkkoa, järjestelmiä ja niiden käyttöä valvotaan?

Organisaation tietoliikennettä valvovalla taholla on oltava tiedossa normaalin liikenteen tila sekä liikennemäärät. Korotetun ja korkean tason vaatimuksissa tulee olla varauduttu verkkohyökkäyksiin, normaalista poikkeavaan toimintaan sekä on oltava käytössä menettely havaita hyökkäykset ja väärinkäytökset.

Tietojärjestelmäturvallisuus, osa-alue I 500

Osa-alue I 500 on Katakrin tietoturvallisuuden osa-alueista yksityiskohtaisin vaatimusten toteuttamisen osalta. Osa-alue sisältää kriteereitä, joissa edellytetään tietynlaista toteuttamistapaa organisaatiolta. Tietojärjestelmäturvallisuuden osa-alue sisältää tunnistautumiseen, uusien järjestelmien asennukseen sekä lokien keräämiseen ja säilyttämiseen liittyviä kriteereitä.

I 501.0 Tunnistetaanko ja todennetaanko käyttäjät ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin?

Lähtötason suositus on, että käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista. Korkeamman tason vaatimuksissa vaaditaan yksilöllisiä tunnisteita, salasana suojausta sekä ylläpitotunnusten henkilökohtaisuutta, jotta muutosten tekeminen on hallittua.

I 502.0 Onko organisaatiossa menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, verkkotulostimet ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus?

Kriteerin vaatimukset sisältävät yksityiskohtaisia vaateita uusien järjestelmien asentamisesta ja niihin liittyvistä ohjelmistoista. Tarpeelliset turvapäivitykset tulee olla asennettu, järjestelmän tulee sisältää vain tarvittavat komponentit ja palvelu tulee olla rajattu vain välttämättömään. Korotettujen vaatimusten vaateissa edellytetään ohjelmistojen turvallista konfiguroimista sekä sähköpostiohjelmistojen perusasetusten muuttamista.

I 503.0 Miten on pienennetty haittaohjelmien aiheuttamia riskejä?

Haittaohjelmistojen torjuntaohjelmat tulee olla asennettuina kaikkiin laitteisiin ja järjestelmiin, jotka ovat yhteydessä organisaation verkkoon. Ohjelmistojen tulee lisäksi olla toiminnassa sekä asianmukaisesti päivittyvä sekä niiden tulee tuottaa lokitietoa.

I 504.0 Miten organisaation lokimenettely on toteutettu?

Lokia keräävien ohjelmien tulee tallentaa tietoa riittävän pitkältä ajalta, tärkeitä tallenteita 24kk. Tallentuvien lokitietojen tulee olla riittävän kattavat tietomurtojen todentamiseen ja lokitietoja tulee säilyttää suojattuna. Korotettujen vaatimusten vaateissa vaaditaan lokitietojen suojaamista luvattomalta pääsyltä ja väärentämiseltä, myös kriittisten lokitietojen tarkastelusta tulee syntyä loki. Järjestelmän ylläpitäjällä ei tulisi olla oikeuksia järjestelmän lokitietoon.

I 505.0 Miten salassa pidettävät tiedot säilytetään tietojärjestelmissä?

Salassa pidettävä tieto säilytetään salakirjoitettuna palvelimilla ja työasemissa, käytön yhteydessä syntyvät tiedot hävitetään säännöllisesti. Suojaustason 3 ja 2 tiedot pidetään erillään julkisesta tiedosta.

I 506.0 Kuinka varmistutaan siitä, että luottamuksellista tietoa sisältävät liikuteltavat kiintolevyt, muistit, mediat, älypuhelimet ja vastaavat ovat aina suojattuja luvatonta pääsyä vastaan?

Liikuteltavat muistit tulee olla suojattuna sen sisältämän tiedon luokituksen edellyttämällä tavalla. Myös älypuhelinten suojauksen tulee olla riittävällä tasolla sen sisältämään tietoon nähden.

I 507.0 Kuinka varmistutaan siitä, etteivät salassa pidettävät tiedot joudu kolmansille osapuolille huoltotoimenpiteiden tai käytöstä poiston yhteydessä?

Kaikki sensitiivistä ja luotettavaa tietoa sisältävät osat tulee tyhjentää ennen käytöstä poistoa tai huoltoon lähettämistä. Huoltoyhtiön kanssa on suositeltua tehdä turvallisuussopimus, jossa määritellään tiedon käsittelyn säännöt sekä mahdolliset seuraamusvaatimukset.

I 508.0 Miten varmistutaan, ettei organisaation verkossa ole luvattomia laitteita tai järjestelmiä?

Organisaation käytössä olevista laitteista tulee olla rekisteri, jossa näkyvät myös käytöstä poistetut laitteet. Myös käytettävistä ohjelmistoista ja niiden lisensseistä pitää olla rekisteri. Ylempien tasojen vaatimuksissa edellytetään esimerkiksi laitetilojen ajoittaista tarkistamista luvattomista laitteista, jos on kyse suojatun verkon tiloista, tarkastusten tulee olla säännöllisiä.

I 509.0 Miten varmistutaan siitä, että käytetyt salausratkaisut ovat riittävän turvallisia?

Organisaation käytössä tulee olla kansallisen tai kansainvälisen tietoturvaviranomaisen toimesta hyväksytty salausratkaisu.

I 510.0 Ovatko salaiset avaimet vain valtuutettujen käyttäjien ja prosessien käytössä?

Salaisten avainten tulee olla vain valtuutettujen henkilöiden ja prosessien käytössä. Perustasolla vaaditaan avainten turvallista säilytystä, jakelua sekä säännöllistä avainten vaihtoa.

I 511.0 Käytetäänkö istunnonhallinnassa tunnettua ja luotettavana pidettyä tekniikkaa?

Tunnettua tekniikka käyttämällä tai muulla vastaavalla tavalla on istunnon kaappaus tai kloonaus tehtävä huomattavan vaikeaksi.

I 512.0 Onko huolehdittu, että autentikaatiodataa ei säilytetä tietojärjestelmissä selväkielisenä?

Salasanoja ei tule säilyttää selväkielisenä tietojärjestelmissä, vaan ne tulee salata luotettavalla menetelmällä.

I 513.0 Miten varmistutaan ajettavan koodin turvallisuudesta?

Organisaatioon hankittavat ja asennettavat ohjelmistot on peräisin luotettavasta lähteestä ja niiden eheys tulee tarkastaa ennen käyttöönottoa.

Tietoaineistoturvallisuus, osa-alue I 600

Tietoaineistoturvallisuus osa-alue pitää sisällään kriteereitä muun muassa tietoaineiston säilyttämisestä, käsittelystä ja hävittämisestä. Osa-alueen kaikki kriteerit käsittelevät vain salassa pidettävään tietoon liittyviä toimenpiteitä organisaatiossa. Ensimmäinen kriteeri on tiedon luokitteluun liittyvä vaatimus. Tietoaineiston turvaluokitukset eri organisaatioiden turvaluokilla löytyvät liitteestä 2.

I 601.0 Millainen tiedon luokittelumenettely organisaatiolla on?

Organisaation tulee luokitella tieto lakisääteisten määräysten mukaan, jonka ohjeistus löytyy muun muassa Valtiovarainministeriön julkaisusta Tietoaineistojen turvallinen käsittely.

I 602.0 Onko huolehdittu siitä, että salassa pidettäviä tietoja sisältäviä aineistoja ja tietovälineitä säilytetään turvallisesti?

Luokiteltua tietoa on säilytettävä kyseisen tason vaatimalla tavalla, perusoletuksena että työ- ja säilytystilat lukitaan käytön jälkeen. Korotetun suojaustason tietoja tulee säilyttää kassakaapissa, on muistettava, että vaatimus koskee paperimuotoisten dokumenttien lisäksi myös esimerkiksi ulkoisia muistivälineitä.

I 603.0 Hävitetäänkö luottamuksellisia tietoja sisältävät aineistot luotettavasti?

Luottamuksellisia tietoja sisältävät dokumentit ja sähköiset tallenteet hävitetään järjestelmällisesti, tietojen tuhoaminen tapahtuu luotettavasti ja korkeamman suojaustason tietoja käsittelevien henkilöiden tulee olla tietoisia oikeasta menettelytavasta hävittää tieto.

I 604.0 Onko salassa pidettävän aineiston kopiointi ja tulostus järjestetty turvallisesti?

Kopioiden ja tulosteiden käsittelyn ja tulostuksen tulee olla riittävän turvallista ja hallittua, korotetun suojaustason asiakirjojen kopioita ja tulosteita luovutetaan eteenpäin aivan kuten alkuperäisiä, myös alkuperäisen asiakirjan luokituksen on säilyttävä.

I 605.0 Onko salassa pidettävän aineiston sähköinen välitys järjestetty turvallisesti?

Salassa pidettävän aineiston välittäminen sähköisessä muodossa on pystyttävä tekemään turvallisesti ja luotettavasti. Yhteyksien ja sähköpostin suojaukset tulee olla asianmukaisella tasolla ja oikein suojattuja. Jos salassa pidettävää tietoa kulkee julkisessa verkossa, on se aina salattava luotettavalla tavalla. Korotetun suojaustason tiedon siirtämisessä sähköisesti on huolehdittava tietoliikenteen suojauksen lisäksi riittävästä mobiililaitteiden suojauksesta.

I606.0 Onko salassa pidettävän aineiston välitys postilla ja/tai kuriirilla järjestetty turvallisesti?

Salassa pidettävän tiedon välitys hoidetaan tiedon luokituksen vaatimalla tavalla. Perustason ja korotettujen tasojen vaateissa vaaditaan kuorien sinetöimistä sekä kuriirien käyttöä sekä huomioidaan myös oman organisaation postituksen luotettavuus ja siitä huolehtiminen.

I 607.0 Pystytäänkö seuraamaan minne ja mistä salassa pidettävät aineistot on välitetty?

Vaatimuksia on vain korkeampien suojaustasojen tiedon välityksessä, organisaation ohjeistettava korotettujen suojaustasojen tietojen käsittely sekä tarvittaessa valvoa sähköisessä muodossa olevan tiedon latauksia.

Käyttöturvallisuus, osa-alue I 700

Osa-alue sisältää tietoaineiston käyttöön, suojaukseen ja sekä hallintaan liittyviä kriteereitä. Muutamassa kriteerissä viitataan myös aiemmin valmistuneeseen, Valtiovarainministeriön julkaisemaan valtionhallinnon ICT-varautumiseen, Jatkuvuuden hallinta ja tiedon turvaaminen – dokumenttiin. JHTT on ICT-varautumisen perusvaatimukset valtionhallinnon yksiköille sekä palveluntarjoajille, jotka tuottavat kyseisille yksiköille ICT-palveluita. (Valtiovarainministeriö 2009)

I 701.0 Onko huolehdittu, että organisaatiolla on toimintaansa nähden riittävät jatkuvuuden varmistavat suunnitelmat?

Organisaatiolla on oltava omaan toimintaansa nähden riittävät suunnitelmat kriisitilanteiden varalle. Edellytetään, että kriittiset toiminnot, jotka on todennettu riskienkartoituksen avulla, ovat suojattu, toipumissuunnitelmat kyseisille palveluille ovat olemassa ja ne on testattu.

I 702.0 Mahdollistaako organisaatiossa saatavilla oleva dokumentaatio vioista, toimintahäiriöistä, hyökkäyksistä ja vastaavista toipumisen?

Organisaation dokumentoinnin käytännöt ovat sellaiset, että järjestelmien ja vastaavien asetukset ja perustiedot on dokumentoitu ajantasaisesti. Dokumentaation avulla on voitava pystyä korjaamaan toimintahäiriöt, korotetun tason järjestelmien dokumentaation on oltava yhdenmukainen toteutuksen kanssa.

I 703.0 Onko organisaatiossa selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita?

Organisaation rajattava ohjelmistojen ja verkkojen asennus vain nimetyille tahoille, peruskäyttäjällä ei saa olla oikeuksia muokata tai asentaa ohjelmistoja tai asetuksia. Korotetun tason vaatimukset edellyttävät turvaluokitellun tiedon osalta viranomaishyväksyttyjä tiloja ja ohjelmia. Organisaation on myös varmistuttava asennettavien ohjelmistojen eheydestä.

I 704.0 Onko organisaatiossa otettu käyttöön periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan?

Periaatteet ja turvamekanismit on oltava olemassa, periaatteista ja turvamekanismeista on tiedotettu henkilökunnalle ja niiden mahdollinen käyttö opastettu. Perustason vaatimuksissa edellytetään turvallisen etä- ja matkatyön ohjetta, etäkäytössä oltava vahvat todennusmenetelmät käytössä ja vain todennettuja yhteyksiä käytetään.

I 705.0 Ovatko kehitys-/testaus ja tuotantojärjestelmät erilliset?

Järjestelmien on oltava erillisiä, mahdollisten käyttökatkosten estämiseksi. Ennen käyttöönottoa testauksesta aiheutunut data on tuhottava mukaan luettuna testitilit. Suojattavaa tietoa ei kopioida testausympäristöön, mikäli sen turvataso on tuotantoympäristöä alhaisempi.

I 706.0 Miten varmistetaan, että verkossa ja sen palveluissa ei ole tunnettuja haavoittuvuuksia?

Luotettavien tahojen, kuten viranomaisten ja ohjelmistovalmistajien, tiedotteita koskien tietoturvallisuutta seurataan ja mahdolliset toimenpiteet kuten päivitykset tehdään järjestelmällisesti. Verkko ja siihen kytketyt laitteet skannataan säännöllisesti.

I 707.0 Miten varmistutaan siitä, että työskentelytauoilla tai työskentelyn jälkeen laitteet eivät jää ilman riittävää suojaa?

Organisaation on ohjeistuksella ja tietoturvaperiaatteilla velvoitettava käyttäjät toimimaan siten, että tauoilla tai työskentelyn jälkeen ei ulkopuolisen ole mahdollista päästä tietoon käsiksi.

I 708.0 Onko käytössä ns. puhtaan pöydän politiikka? Koskeeko sama periaate myös näyttöjä?

Organisaation on ohjeistanut henkilökunnalle puhtaan pöydän politiikan.

I 709.0 Onko huolehdittu riittävästä työtehtävien eriyttämisestä niin, ettei synny ns. vaarallisia työyhdistelmiä?
Varsinkin kriittisten toimintojen osalta organisaation on kyettävä riittävissä määrin eriyttämään työtehtäviä ja vastuukokonaisuuksia, jotta väärinkäytöksen riskiä saadaan pienennettyä. Korotettujen tasojen vaatimuksissa edellytetään valvontamekanismeja, jos vaarallisia työyhdistelmiä syntyy sekä kriittisille toiminnoille ylipäänsä.

I 710.0 Onko riittävästä varmuuskopioinnista huolehdittu?

Varmuuskopioinnissa on otettava huomioon riittävä tiheys, palautusprosessin toimivuus sekä oikea säilytys ja pääsynvalvonta. Varmuuskopiot on muistettava säilyttää sisältävän tiedon suojausluokan edellyttämässä paikassa sekä oikeanlaisessa muodossa.

Liite 2: Tietoaineiston turvaluokitukset

Talletetulle tietoaineistolle pitää aina määrittä turvallisuusluokka, turvallisuusluokan määrittelyllä pyritään siihen, että tietoon pääsevät käsiksi vain ne kenelle se on tarkoitettu. Tietoa tulee suojata koko sen elinkaaren ajan ja se on myös tuhottava luotettavasti, näin luottamuksellista tietoa ei joudu vääriin käsiin. Tiedon suojaamiseen liittyy tiedon luotettavan käsittelyn lisäksi käsittelijän luotettavuus sekä erilaiset suojaustoimet, tahallisen tiedon varastamisen estämiseksi. Tieto voi levitä myös varomattoman tai huolimattoman käytön seurauksena. Kansallisen turvallisuusauditointikriteeristön tarkoituksena on estää tiedon tahaton tai tahallinen leviäminen, tietoturvallisuusosiossa keskitytään tiedon suojaamiseen sekä tunkeutujan tunnistamiseen sekä reagointiin ennen tiedon häviämistä.

Tieto luokitellaan eri kategorioihin sen sisältämän tiedon perusteella. Oheisessa kaaviossa on esitetty Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) turvallisuusluokitusta suhteessa kansallisen turvallisuusauditointikriteeristön vaatimuksiin. Kuten kansallisen turvallisuusauditointikriteeristön tietoturvallisuusosion johdannossa mainitaan:" Viranomaisten suojattavien tai turvaluokiteltujen tietojen käsittely edellyttää organisaatiolta vastaavan vaatimustason täyttämistä." (Kansallinen turvallisuusauditointikriteeristö 2009, 59.) Tällöin organisaatiolla on valmius käsitellä sen vaatimustason tietoja, mitkä organisaatio täyttää. (Kansallinen turvallisuusauditointikriteeristö 2009; Kreus 2010; Valtiovarainministeriö 2008.)

Turvallisuusluokka	**Suojaustaso (TLL)**	**Katakri**
Erittäin salainen	I	(ei luokiteltu)
Salainen	II	korkea taso
Luottamuksellinen	III	korotettu taso
Käyttö rajoitettu	IV	perustaso
Julkinen tieto	-	lähtötaso

Kuva 6: Tietoaineiston turvaluokitukset.