jamk.fi

Kyberturvallisuustason arviointi

Kyberturvallisuustason arviointi FINCSC-sertifioinneissa

Tuukka Laava

Opinnäytetyö
Toukokuu 2020
Tekniikan ala
Insinööri (AMK), tietotekniikan koulutusohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Laava, Tuukka	Opinnäytetyö, AMK	Toukokuu 2020
	Sivumäärä 44 + Liitteet 30 sivua	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Kyberturvallisuustason arviointi
Kyberturvallisuustason arviointi FINCSC-sertifioinneissa

Tutkinto-ohjelma
Insinööri (AMK), tietotekniikka

Työn ohjaaja(t)
Juha Piispanen; Jarmo Nevala

Toimeksiantaja(t)
JYVSECTEC – Jyväskylä Security Technology

Tiivistelmä

Toiminnallisen opinnäytetyön tarkoituksena oli jatkaa kansallisen kyberturvallisuusstrategian toiseen toimeenpano-ohjelmaan kuuluvan FINCSC-sertifiointijärjestelmän (Finnish Cyber Security Certificate) edelleen kehittämistä. Kehittämistehtävällä pyrittiin järkeistämään olemassa olevia sertifiointipalveluita tekemällä FINCSC ja FINCSC PLUS -sertifioinneissa noudatettavista arviointimenettelyistä nykyistä ymmärrettävämpiä. Arviointimenettelyitä oli tavoite täsmentää arviointilaitoksen palveluiden aikaisilta toimilta asiakkaan kyberturvallisuustason selvittämiseksi.

Kehittämistehtävää toteutettiin Jyväskylän ammattikorkeakoulun alaisuudessa toimivan kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus JYVSECTECin (Jyväskylä Security Technology) toimeksiannosta. Toimeksiannossa annettua kehittämistehtävää lähestyttiin vertaisoppimisen ja kehittämällä oppimisen keinoin hyödyntäen vertailukohteina sertifiointijärjestelmän taustalla aiemmin vaikuttaneita kansallisia ja kansainvälisiä tietoturvallisuuden arviointimalleja. Työssä kerättyä tietoaineistoa käsiteltiin laadullista sisällön analyysia mukaillen.

Kehittämistehtävän tuotoksena syntyi esitys auktorisoitujen arviointilaitosten käyttöön tarkoitetusta kyberturvallisuuden arviointiohjeistuksesta. Ohjeistuksessa tarjotaan tietoa sertifiointikriteerien täyttymisen todentamiseksi käytettävistä arviointimenetelmistä ja kyberturvallisuuden arviointitoimintaa ohjaavista yleisistä periaatteista. Ohjeistuksessa kyberturvallisuuden arviointitoimintaa lähestytään arvioinnin toteuttajan näkökulmasta huomioiden toimintaan liittyvät, sertifioinnin kohteelta edellytettävät arviointijärjestelyt

Avainsanat (asiasanat)
arviointi, auditointi, kyberturvallisuus, sertifiointi, todentaminen

Muut tiedot (Salassa pidettävät liitteet)
Liitteet 1, 2 ja 3 ovat salassa pidettäviä, ja ne on poistettu julkisesta työstä. Salassapidon perusteena on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:n kohta 17: julkisyhteisön liike-tai ammattisalaisuus. Salassapitoaika on viisi (5) vuotta. Salassapito päättyy 29.5.2025.

jamk.fi

Description

Author(s)	Type of publication	Date
Laava, Tuukka	Bachelor's thesis	May 2020
		Language of publication: Finnish
	Number of pages 44 + Annexes 30 pages	Permission for web publication: x

Title of publication

Cyber security level assessment

Assessing cyber security level in FINCSC certifications

Degree programme

Bachelor of Engineering, Information Technology

Supervisor(s)

Piispanen Juha; Nevala Jarmo

Assigned by

JYVSECTEC – Jyväskylä Security Technology

Abstract

The purpose of the functional thesis was to further develop the FINCSC certification mechanism (Finnish Cyber Security Certificate) included in the second implementation program of the Finnish national cyber security strategy. The goal of the development task was to rationalize the existing FINCSC and FINCSC PLUS certification services by making the assessment procedures more comprehensible. The work aimed to specify the assessment procedures from the activities of the assessment body in order to determine the customer's cyber security level.

The development task was carried out on behalf of the cyber security research, development and training center JYVSECTEC (Jyväskylä Security Technology) operating under the auspices of JAMK University of Applied Sciences. The development task was approached by the means of benchmarking and learning by developing, using the previously influenced national and international information security assessment models as a reference point. The data collected in the work was processed in accordance with the qualitative content analysis.

The output of the development task was a proposal for cyber security assessment guidelines for use by authorized assessment bodies. The guidelines provide information on the assessment methods used to verify compliance with the certification criteria and the general principles that guide cyber security assessment activities. The guidelines approach cyber security assessment activities from the perspective of the assessment body, taking into account the assessment arrangements required of the subject of certification.

Keywords/tags (subjects)

assessment, auditing, cyber security, certification, verification

Miscellaneous (Confidential information)

Annexes 1, 2 and 3 are confidential and have been removed from the public work. The basis for secrecy is section 24 (17) of the Act on the Openness of Government Activities (621/1999): business or professional secret of the public institution. The confidentiality period is five (5) years. The secrecy ends on May 29, 2025.

Sisältö

1 Johdanto

Digitalisaatio on koko suomalaista kansakuntaa läpileikkaava ilmiö, sen koskettaessa jokaista yhteiskunnan osa-aluetta ja tasoa. Digitalisaation muutosvoimat ulottuvat niin julkiseen, yksityiseen kuin kolmanteen sektoriin sekä yksittäisiin kansalaisiin.

Digitalisaatio uudistaa työn tekemisen ja kuluttamisen tapoja korostamalla teknologian käytön merkitystä. Digitaaliteknologioita ja niihin kuuluvia digitaalisia alustoja hyödynnetään enenevissä määrin erottamattomana osana työn ja arjen päivittäistoimintaa ja aktiviteetteja. Positiivisesta kasvusta viestii tietoliikenneyhteyksien saatavuuden ja teknologian käytön jatkuva lisääntyminen yritysten ja kotitalouksien keskuudessa. Teknologiaa hyödynnetään niin viranomaisasioinnissa, kaupankäynnissä kuin sosiaalisessa kanssakäymisessä.

> *74 % yritysten yhteenlasketusta henkilöstöstä käytti vuonna 2019 työssään Internet-yhteydellä olevaa tietokonetta, missä on 2 %-yks. nousua edeltävään vuoteen. (Internet yrityksissä 2018; Internet yrityksissä 2019)*

Digitaalinen muutos on omiaan muokkaamaan yksilöiden ja yhteisöjen elin- ja vaikutuspiiriä kohti kansainvälisesti verkottunutta sähköistä toimintaympäristöä. Maailmanlaajuisessa digitaalisessa toimintaympäristössä tietoliikenneyhteydet tuovat palvelunkäyttäjät ja –tarjoajat yhteisen kohtaamis- ja tiedonvälityspaikan ääreen valtioiden fyysiset rajat ylittävään kybertoimintaympäristöön. Viestintäverkoista ja tietojärjestelmistä koostuvassa kybertoimintaympäristössä tieto digitaalisena, aineettomana hyödykkeenä ja pääomana välittää sanomia ihmisten ja laitteiden välillä mahdollistaen monensuuntaisen vuorovaikutuksen.

Kybertoimintaympäristöllä on organisaatioiden toiminnan jatkuvuuden ja tietoyhteiskunnan toimivuuden kannalta arvoa, jota on tarve vaalia ja suojella, ja jonka saatavuudesta kannetaan huolta. Kybertoimintaympäristöä pyritään suojaamaan ajassa yhä monimutkaisemmiksi ja vaarallisemmiksi kehittyvien kyberuhkien aiheuttamilta, organisaatioiden ja tietojärjestelmien toimintaa

haittaavilta kyberhäiriötilanteilta. Kybertoimintaympäristön suojaamiseksi käytettävistä toimenpiteistä käytetään nimitystä tietoturvakontrollit.

Toteutettavat tietoturvakontrollit perustuvat riskien arvioinnin ja vallitsevan turvallisuustietämyksen kautta toiminnassa tunnistettaviin uhkakuviin ja riskitekijöihin. Tilannekuvaa ja –tietoisuutta kybertoimintaympäristön uhkista ja varautumiskeinoista rakennetaan monitoimijayhteistyössä kaikilla yhteiskunnan tasoilla. Varautumisen suunnittelussa ohjausta tarkoituksenmukaisten tietoturvakontrollien valintaan ja niiden riittävyyden arviointiin annetaan sekä yhteiskunnassa säädettävin oikeusnormein että tietyllä toimialalla tai toiminnassa noudatettavin kansallisin ja kansainvälisin standardein, ja erilaisin arviointimallein.

2 Tausta ja tavoitteet

2.1 Suomalaisen yhteiskunnan turvallisuusuhat

Suomen ensimmäinen kyberturvallisuusstrategia hyväksyttiin valtioneuvoston periaatepäätöksellä 24.päivänä tammikuuta vuonna 2013. Kyberturvallisuusstrategian valmistelu käynnistyi osana yhteiskunnan turvallisuusstrategian toimeenpanoa. Valmistelun alulle panosta vastasi tasavallan presidentti yhdessä valtioneuvoston ulko- ja turvallisuuspoliittisen ministerivaliokunnan kanssa. Valmistelun sai toteuttaakseen viranomaisista ja elinkeinoelämän edustajista koottu poikkihallinnollinen työryhmä, jonka työskentelyä johti Suomen itsenäisyyden juhlarahasto Sitran yliasiamies Mikko Kosonen. (Suomen kyberturvallisuusstrategia valmis 2013; Suomen kyberturvallisuusstrategia 2013, 1-2.)

Työryhmätyöskentelyn taustalla olleessa, vuosikymmenen vaihteessa hyväksytyssä yhteiskunnan turvallisuusstrategiassa arvioitiin yhteiskunnan turvallisuusympäristön kehitystä ja suomalaisen yhteiskunnan muutosta. Yhteiskunnan elintärkeiden toimintojen turvaamisen katsottiin yhteiskunnan lisääntyneen tietointensiivisyyden myötä

olevan yhä enemmän riippuvainen viestintäverkkojen ja tietojärjestelmien toiminnasta. Tästä seuraten elintärkeitä toimintoja vaarantavaksi uhkamalliksi kuvattiin kyberuhkien aiheuttamat tietoliikenteen ja –järjestelmien vakavat häiriötilanteet niin normaali- kuin poikkeusoloissa. (Yhteiskunnan turvallisuusstrategia 2010, 15-16 ja 67-69.)

Esimakua odotettavissa olevista kyberuhkien haittavaikutuksista tietoyhteiskunnan toimivuudelle oltiin saatu kokea jo entuudestaan tapahtuneiden haittaohjelmatartuntojen, ja viestintäverkkojen ja –palvelujen toimivuushäiriöiden kautta. Vuonna 2009 silloinen Viestintävirasto eli nykyinen Liikenne- ja viestintävirasto TRAFICOM oli rekisteröinyt kuluneen vuoden aikana tulleen kansallisesti tietoon 2515 haittaohjelma- ja tietoturvaloukkaushavaintoa. Samaisena ajanjaksona Poliisi kirjasi sille ilmoitetun 496 tietoverkkorikollisuuteen liittyvää tapausta. (Sisäisen turvallisuuden ohjelman toimeenpano 2010, 37.)

Yhteiskunnan tahtotilaa varautua aiemmin koettujen kaltaisiin ja lähivuosina yleistyväksi odotettaviin kyberuhkiin kuvattiin kyberturvallisuusstrategialla. Strategiassa esitetty visio kyberturvallisuuden tahtotilasta jakaantui kolmeen osaan. Ensimmäisenä tavoitteena oli kyetä suojaamaan Suomen elintärkeät toiminnot kaikissa tilanteissa kyberuhkaa vastaan. Toisena tavoitteena oli tarjota kansalaisille, viranomaisille ja yrityksille mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista. Kolmantena tavoitteena oli tehdä Suomesta *”-- maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa”*. (Suomen kyberturvallisuusstrategia 2013, 3.)

Edellytyksiä kyberturvallisuuden kansallisen tahtotilan toteutumiselle luotiin kyberturvallisuusstrategiassa määritellyllä kymmenellä strategisella linjauksella. Strategisissa linjauksissa korostettiin suomalaisen turvallisuusyhteistyön vahvuutena olevaa julkisen ja yksityisen sektorin yhteistoimintaa. Kyberturvallisuusstrategia lausuikin kyberturvallisuuden toimintamallin periaatteissa kyberturvallisuuden edellytyksenä olevan *”jokaisen kybertoimintaympäristössä toimivan toteuttamat tarkoituksenmukaiset ja riittävät tietojärjestelmien ja tietoverkkojen turvallisuusratkaisut”*. (Suomen kyberturvallisuusstrategia 2013, 5-11.)

2.2 Kyberuhkien kansalliset varautumistoimenpiteet

Suomalaisen yhteiskunnan käytännön toimia kyberturvallisuusstrategian tavoitteisiin pääsemiseksi ja toimintalinjauksiin vastaamiseksi esiteltiin kyberturvallisuusstrategian nojalla laadituissa toimeenpano-ohjelmissa. Toimeenpano-ohjelmat koostuivat eri toimijoiden ja hallinnonalojen esitysten pohjalta tuotetuista poikkihallinnollisista toimenpiteistä. Toimenpiteet kyberuhkiin varautumisesta ja niiden aiheuttamien häiriötilanteiden hallinnasta linkittyivät yhdeltä tai useammalta kohtaa kyberturvallisuusstrategiassa esiteltyyn kymmeneen strategiseen linjaukseen. (Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 2014, 18-22; Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, 7-10.)

Turvallisuuskomitea hyväksyi kyberturvallisuusstrategian ensimmäisen toimeenpano-ohjelman 11.päivänä maaliskuuta vuonna 2014. Ensimmäinen toimeenpano-ohjelma koostui 74 kyberturvallisuuden kansallisen tahtotilan edistämiseksi toteutettavasta toimenpiteestä. Toimenpiteiden toteutusvastuut jakaantuivat eri ministeriöille ja yksittäisille toimijoille. Keskeisinä kehittämiskohteina toimeenpano-ohjelman toimenpiteissä korostui viranomaisten kyberturvallisuuden toimintavalmiuksien ja tilannekuvan kehittäminen sekä Suomesta aiemmin puuttuneen ja sittemmin Sanastokeskuksen julkaiseman yhteisen kyberturvallisuuden käsitteistön määrittäminen. (Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 2014; Kyberturvallisuuden sanasto 2018.)

Turvallisuuskomitean sihteeristö selvitti ensimmäisen kyberturvallisuusstrategian toimeenpano-ohjelman toimenpiteiden toteutumista tammikuussa vuonna 2016 laatimassaan arviossa. Arviointiin kerättiin eri hallinnonaloilta, elinkeinoelämän edustajilta, akatemialta ja järjestöiltä näkemyksiä kyberturvallisuuden kansallisen tahtotilan kehityksestä ja toimeenpano-ohjelman toimenpiteiden vaikuttavuudesta. Arvioinnissa korostui kyberturvallisuuden johtamismallien kehittämisen tarve. Arvion perusteella Turvallisuuskomitea päätti toimeenpano-ohjelman päivittämisestä. (Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, 4-6; ks. Lehto, Limnéll, Innola, Pöyhönen, Rusi & Salminen 2017.)

Kyberturvallisuusstrategian nojalla annettu toinen, päivitetty toimeenpano-ohjelma julkaistiin 20. päivänä huhtikuuta vuonna 2017. Toiseen toimeenpano-ohjelmaan sisällytettiin kaikkinensa 22 toimenpidettä. Määritellyillä toimenpiteillä pyrittiin edistämään puutteelliseksi koettua kyberturvallisuuden johtamista sekä tukemaan turvallisen kybertoimintaympäristön ylläpitämistä ja sähköisten palvelujen tuottamista viranomaisissa, yrityksissä ja järjestöissä. Aiemmin toteutetusta poiketen toimenpiteiden vaikutusten keskiöön nostettiin kansalainen viestintäverkkojen ja –palvelujen käyttäjänä. (Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020.)

Elinkeinoelämän toimijoiden osaamista ja ymmärrystä kyberturvallisuudesta sekä sen toteuttamisesta ja johtamisesta liiketoiminnassa tuettiin erityisesti toisen toimeenpano-ohjelman toimenpiteellä kansallisesta kyberturvallisuuden arviointimallista. Arviointimallilla viitataan Jyväskylän ammattikorkeakoulussa kehitettyyn, ja sen ylläpitämään ja hallinnoimaan FINCSC -sertifiointijärjestelmään, Finnish Cyber Security Certificate. Järjestelmä on osa Turvallisuuskomitealle raportoitavaa jatkuvaa kansallista toimintaa Suomen kyberuhkien sietokyvyn eli kyberresilienssin kehittämiseksi. (Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, 19.)

2.3 Kansallinen kyberturvallisuuden arviointimalli

FINCSC-sertifiointijärjestelmä kansallisena kyberturvallisuuden arviointimallina on tulosta Jyväskylän ammattikorkeakoulussa tehdystä soveltavasta tutkimus-, kehitys- ja innovaatiotoiminnasta. Sertifiointijärjestelmä on kehitetty vuosina 2015-2016 käynnissä olleessa Cyber Scheme Finland –pilottiprojektissa ja tätä vuosina 2017-2018 jatkaneessa FINCSC PLUS –projektissa. Kehitystyötä on tehty aluelähtöisesti Keski-Suomalaisten yritysten kanssa alueellisten innovaatioiden ja kokeilujen käynnistämiseen kohdennetusta AIKO –määrärahasta sekä maakunnan kehittämisrahasta ja Keski-Suomen kehittämisrahastosta myönnetyllä tuella. (Keski-Suomen liiton rahoitusraportti 2016, 7-8; Hankeraportti 2018, 9-10.)

Kehitystyöhön on menneen projektitoiminnan kautta osallistunut useita yrityksiä eri toimialoilta ja kokoluokista. Projektitoimintaan välittömästi osallistuneiden yritysten

yhteenlaskettu lukumäärä on ollut 25 organisaatiota. Tästä yhteenlasketusta lukumäärästä 22 organisaatiota otti osaa Cyber Scheme Finland –pilottiprojektiin ja kolme organisaatiota FINCSC PLUS –projektiin. Lähes kaikki projektitoimintaan osallistuneet organisaatiot suorittivat sertifioinnin hyväksytysti loppuun. Jokainen projektitoiminnassa mukana ollut organisaatio toi kehitystyöhön omat erityispiirteensä sekä ennakko-odotuksensa ja valmiutensa kyberturvallisuuden käsittelyyn. (Loppuraportti: Cyber Scheme Finland –pilotti 1.9.2015 – 30.11.2016, 3; Loppuraportti: FINCSC PLUS 1.11.2016 – 31.8.2018, 3; ks. Pellinen 2018.)

Ensimmäisenä käynnissä olleella Cyber Scheme Finland –pilottiprojektilla luotiin elinkeinoelämälle ensimmäiset, yhteiset matalan kynnyksen perusteet kyberturvallisuuden vaatimusten hallinnalle ja arviointitoiminnan järjestämiselle kansallisesti. Pilottiprojektissa vaatimustenhallintaa rakennettiin organisaation itsearviointiin perustuvan sertifiointitason varaan. (Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, 19; Loppuraportti: Cyber Scheme Finland –pilotti 1.9.2015 – 30.11.2016, 4-18.) Tuotettua mallia on täydennetty viimeiseksi käynnissä olleella FINCSC PLUS –projektilla, jossa jo aiemmin luodun mallin oheen tuotettiin arviointilaitoksen suorittamaan ulkoiseen auditointiin perustuva sertifiointitaso (Loppuraportti: FINCSC PLUS 1.11.2016 – 31.8.2018, 5-8).

FINCSC-sertifiointijärjestelmän kehitystyötä on tehty hyödyntäen ulkomailla jo aiemmin saatuja kokemuksia vastaavaan tarkoitukseen kehitetyistä arviointimalleista (Loppuraportti: Cyber Scheme Finland –pilotti 1.9.2015 – 30.11.2016, 18-19; Loppuraportti: FINCSC PLUS 1.11.2016 – 31.8.2018, 8). Ulkomaisista malleista vertailukohteena on toiminut erityisesti Iso-Britanniassa vuodesta 2014 lähtien käytössä ollut Cyber Essentials –sertifiointijärjestelmä, ja sen kaksi sertifiointitasoa Cyber Essentials ja Cyber Essentials Plus (FINCSC Booklet 2018, 12; New scheme to help businesses defend against cyber threats goes live 2014). Toisinkuin vertailukohteensa FINCSC-sertifiointijärjestelmän käyttöä on yleisen velvoittavuuden sijaan rakennettu omaehtoisen tietoturvatyön varaan erilaisiin käyttötapauksiin (FINCSC Booklet 2018, 4).

FINCSC-sertifiointijärjestelmän kehitystyössä on brittiläisen mallin ohella hyödynnetty Suomessa julkisella sektorilla, valtionhallinnon tietoturvallisuuden arvioinneissa

käytössä olevia arviointikriteeristöjä (ks. Ohje tietoturvallisuuden arviointilaitoksille 2020, 8-9). Arviointikriteeristöistä vertailukohteena ovat toimineet valtiovarainministeriön VAHTI-ohjeet, ulkoministeriön tietoturvallisuuden auditointityökalu KATAKRI sekä kansainvälinen tieturvallisuuden hallintajärjestelmästandardi ISO/IEC 27001 (ks. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010; Katakri 2015; SFS-ISO/IEC 27001). Vertailua mallien välillä on tehty sekä niiden sisällöllisistä, että toiminnallista lähtökohdista valtionhallinnon viranomaisten tietoturvallisuuden arviointitoimintaan liittyvät poikkeavat näkökulmat huomioon ottaen.

2.4 Toiminnallisen opinnäytetyön kehittämistehtävä

Tämän toiminnallisen opinnäytetyön tarkoituksena oli jatkaa Cyber Scheme Finland ja FINCSC PLUS –projekteissa aikaansaatujen tulosten edelleen kehittämistä. Työ pyrki suoritettavalla kehittämistehtävällään järkeistämään olemassa olevia sertifiointipalveluita. Palveluita oli tavoite tehdä nykyistä ymmärrettävämmäksi sertifioinneissa noudatettavista arviointimenettelyistä. Arviointimenettelyitä pyrittiin täsmentämään arviointilaitoksen palveluiden aikaisilta toimilta asiakkaan kybertoimintaympäristön suojaamiseksi toteuttamien tietoturvakontrollien riittävyyden ja tarkoituksenmukaisuuden arvioimisessa sekä niiden todentamisessa.

Opinnäytetyössä sertifiointeihin kuuluvien arviointimenettelyjen tarkastelu pyrki huomioimaan molemmat sertifiointitasot. Arviointimenettelyitä tarkasteltiin vertaisoppimisen ja kehittämällä oppimisen keinoin tarkoituksena hyödyntää työn toimeksiantajan hallinnoimaan kyberturvallisuuslaboratorioon rakennettua virtuaaliympäristöä. Virtuaaliympäristöllä mallinnettiin sertifiointia hakevan kuvitteellisen organisaation tietojärjestelmä- ja teknologia-arkkitehtuuria sen toiminnassa käytettävistä tietojärjestelmä- ja teknologiapalveluista.

Opinnäytetyön tuotoksena oli määrä laatia esitys arviointilaitoksen käyttöön tarkoitetusta kyberturvallisuuden arviointiohjeistuksesta. Ohjeistuksen tavoitteena oli jäsentää sertifiointipalveluihin kuuluvia arviointimenettelyitä kyberturvallisuuden arviointitoiminnan yhteydessä tarkasteltavista arviointikohteista ja toiminnassa käytettävistä arviointitekniikoista. Opinnäytetyön odotettiin kehittämistehtävän

yhteydessä ottavan tarvittaessa kantaa sertifioinneissa arviointiperusteina käytettävien sertifiointivaatimusten uudelleen asetteluun ja sertifiointijärjestelmän kehityskohteisiin.

Opinnäytetyön onnistumista kehittämistehtävän toteutuksessa arvioitiin Jyväskylän ammattikorkeakoulun tutkintosäännön nojalla hyväksyttyjen opinnäytetyön arviointikriteereiden mukaisesti (ks. Opinnäytetyön arviointikriteerit ammattikorkeakoulututkinnoissa (EQF 6-taso) 2014; Jyväskylän ammattikorkeakoulun tutkintosääntö 2019). Työn arviointi perustui tässä dokumentissa esitettävän kirjallisen raportoinnin ohella suoritettuun opinnäytetyöprosessiin, valmiin työn osalta järjestettyyn seminaariesitykseen sekä opinnäytetyön tuotoksiin ja työn toimeksiantajan antamaan kirjalliseen lausuntoon. Opinnäytetyön laatijan kokemuksia opinnäytetyöprosessista ja sen lopputuloksena syntyneestä tuotoksesta analysoidaan raportin lopun pohdintaluvussa.

Opinnäytetyön toimeksiantajana toimi Jyväskylän ammattikorkeakoulun IT-instituutin alaisuudessa vaikuttava kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus JYVSECTEC, Jyväskylä Security Technology. JYVSECTEC on tieto- ja kyberturvallisuuden ratkaisuihin erikoistunut kotimainen palveluntuottaja sekä aktiivinen tutkimus-, kehitys- ja innovaatiotoiminnan harjoittaja. Osana toimintaansa JYVSECTEC ylläpitää ja kehittää FINCSC-sertifiointijärjestelmää yhteistyössä elinkeinoelämän ja julkishallinnon edustajista koostuvan ohjausryhmän kanssa.

2.5 Opinnäytetyön kehittämis- ja analyysimenetelmät

Toiminnallisen opinnäytetyön kehittämis- ja analyysimenetelminä käytettiin kehittämispohjaista oppimista ja vertaisoppimista sekä sisällönanalyysia. Kyseisten kehittämis- ja analyysimenetelmien valinnan perusteena oli niiden erityinen soveltuvuus opinnäytetyön kehittämistehtävän tarkoitukseen aiemmin käynnissä olleen projektityöskentelyn jatkamisesta. Menetelmät mahdollistivat sekä FINCSC-sertifiointijärjestelmän kehityksen taustalla vaikuttaneiden vertailukohtien uudelleen katselmoinnin että kokemuksellisuuden kautta oppimisen.

FINCSC-sertifiointijärjestelmän kehitykseen viimeksi liittyneessä FINCSC PLUS -projektissa sertifiointitason kehitystoiminnan katsottiin jääneen osin vaillinaiseksi. Projektin rahoitushakemuksessa sertifiointitason pilotointiin oli asetettu tavoitteeksi osallistua yhteensä 20 organisaatiota, joista projektissa toteutui alkuperäisen projektiaikataulun viivästymisen jälkeen kolme organisaatiota. Osallistujatavoitteiden täyttymättä jäämisestä ja aikatauluviivästyksistä johtuen käyttökokemusten ja erityisesti niiden perusteella tehtävien jatkotoimien koettiin osin jääneen jälkeen odotetusta. (Loppuraportti: FINCSC PLUS 1.11.2016 – 31.8.2018, 3.)

Kehittämismenetelmiin kuuluva kehittämispohjainen oppiminen tarjosi tilaisuuden palata projektiaikaiseen toimintaan opinnäytetyössä tehtävän kehitystyön muodossa. Kehittämispohjainen oppiminen, englanniksi Learning by Developing, tarkoittaa Laurea ammattikorkeakoulussa luotua pedagogista mallia, jossa oppija aktiivisena osapuolena osallistuu aidon työelämän kehittämistyöhön. Kehittämispohjaisen oppimisen mallissa keskeistä on paitsi opiskelijan osallisuus myös jatkuva vuoropuhelu kehittämistehtävään liittyvien osapuolten välillä. (LbD eli kehittämispohjainen oppiminen 2020.)

Englanninkielen sanasta benchmarking johdetulla suomen kielen vertaisoppiminen termikäännöksellä tarkoitetaan puolestaan kehittämismenetelmää, jossa oppivana osapuolena oleva opiskelija tekee havaintoja toisen, vertailtavana olevan toimijan työtavoista ja olosuhteista. Havaintoja tehdessään opiskelija pyrkii ottamaan osia toiselta hyviksi havaitsemistaan käytännöistä osaksi omaa kehitettävää toimintaansa. Vertaisoppiminen tapahtuu useimmiten epävirallisesti ja strukturoimattomasti vertailtavien osapuolten välisen vastavuoroisuuden jäädessä taka-alalle. (Mäkelä, Salonen & Salonen 2016, 9.)

Opinnäytetyössä käytettävillä kehittämismenetelmillä kerättyä tietoaineistoa analysoitiin laadullista sisällönanalyysiä mukaillen. Sisällönanalyysillä tarkoitetaan menetelmää, jossa jo tekstimuotoisen tai sellaiseksi muutetun aineiston osalta pyritään muodostamaan tiivistetty sanallinen kuvaus tarkasteltavan aineiston sisällöstä (Seitamaa-Hakkarainen 2014). Opinnäytetyössä sisällönanalyysiä hyödynnettiin vertaisoppimisen yhteydessä tehtyjen havaintojen tulkitsemisessa

nostamalla esiin vertailtavien kohteiden erityispiirteitä sekä eri arviointimallien välisiä yhtäläisyyksiä ja eroja.

3 Tieto- ja kyberturvallisuuden arviointimallit

3.1 FINCSC-sertifiointijärjestelmä

3.1.1 Yleistä

FINCSC-sertifiointijärjestelmä on kaikenkokoisille organisaatioille kehitetty kansallinen kyberturvallisuuden arviointimalli. Järjestelmän tarkoituksena on tarjota erityisesti pienille ja keskisuurille yrityksille kevyt ja kustannustehokas menetelmä arvioida riskiperusteisesti tietoverkkojen ja –järjestelmien suojaamiseksi toteutettavia turvallisuusratkaisuita ja –käytänteitä. Lisäksi sertifiointijärjestelmän tarkoituksena on mahdollistaa organisaatiossa jo käyttöönotettujen tietoturvakontrollien kokonaisvaltainen kehittäminen Suomen kansalliselle vähimmäistasolle. (Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, 19; FINCSC Booklet 2018, 12.)

FINCSC-sertifiointijärjestelmä on tarkoitettu soveltuvan käytettäväksi paitsi organisaatioiden oman toiminnan tarkasteluun kyberuhkille altistavien haavoittuvuuksien varalta myös liikekumppaneiden luotettavuuden arviointiin ja alihankintaverkostojen turvallisuuden varmistamiseen. Järjestelmää voidaan hyödyntää sekä yritysten välisissä, kahden- ja monenkeskisissä liikesuhteissa että yritysten ja kuluttajien välisessä kaupankäynnissä hallittaessa kanssakäymiseen liittyviä riskejä. Järjestelmän käyttö varmistaa sopijapuolten yhteisten oikeuksien, vapauksien ja etujen toteutumista. (FINCSC Booklet 2018, 2-3.)

FINCSC-sertifiointijärjestelmässä tietoverkkojen ja –järjestelmien suojaamiseksi toteutettavia tietoturvakontrolleja arvioidaan neljästä kyberturvallisuuden peruslähtökohdasta käsin. Ensimmäinen ja toinen näkökulma mittaavat organisaation hallinnollisia ja toiminnallisia edellytyksiä huolehtia toiminnassa hyödynnettävien tietoverkkojen ja –järjestelmien turvallisesta ja asianmukaisesta käytöstä ja ylläpidosta. Kolmas

ja neljäs näkökulma arvioivat organisaation fyysisiä ja teknisiä puitteita varmistua tietoverkkojen ja –järjestelmien tarkoituksenmukaisesta suojasta kyberuhkaa vastaan. (FINCSC Booklet 2018, 2-3 ja 8-9.)

Kyberturvallisuuden tasoa tarkastellaan kybertoimintaympäristön ja siellä käsiteltävien tietojen luottamuksellisuuden, eheyden ja saatavuuden näkökulmista. Erityistä huomiota kiinnitetään organisaation menetelmiin ennalta ehkäistä tietoa tahattomalta tai tahalliselta vahingoittumiselta ja vaarantumiselta sekä niiden oikeudettomalta ja asiattomalta käytöltä. Ennalta ehkäisevien toimenpiteiden ohella tarkastelussa kiinnitetään huomiota organisaation kykyyn havaita tietoturvapoikkeamia ja suorittaa korjaavia toimenpiteitä poikkeamista johtuvien vahinkojen rajaamiseksi ja vaikutusten minimoimiseksi. (FINCSC Booklet 2018, 2.)

Kyberturvallisuuden tason tarkastelua toteutetaan kerrallaan joko koko organisaation kattavasti tai sen yksittäiseen loogiseen osaan keskittyen. Tarkastelun rajausperusteena voi olla organisaation yksittäinen fyysinen toimipiste tai hallinnollinen toimialue, johon kyberturvallisuuden arviointitoiminta halutaan sillä hetkellä kohdistettavan. Tarkastelun mahdollisesta rajauksesta päättää sertifiointipalvelua käyttävä organisaatio sen osallistuessa sertifiointiin. Rajauksen jälkikäteinen muuttaminen edellyttää tarkastelun ulkopuolelle jätettyjen organisaation osien sertifioimista. (FINCSC Booklet 2018, 8-9.)

3.1.2 Sertifiointitasot

FINCSC-sertifiointijärjestelmä koostuu kahdesta organisaatioille palveluna tuotettavasta sertifiointitasosta FINCSC ja FINCSC PLUS. Sertifiointipalvelut ovat saatavilla kaupparekisteriin rekisteröidyille, suomalaisen yritys- ja yhteisötunnuksen omaaville organisaatioille. Organisaatioille tarjottavia sertifiointipalveluita tuotetaan sertifiointiin hakeutumisen yhteydessä hyväksyttävien toimitusehtojen mukaisesti. FINCSC-sertifiointi perustuu organisaatiolta veloitettavaan kiinteään kertamaksuun, FINCSC PLUS-sertifioinnin noudattaessa tarjousperusteista hinnoittelua. (FINCSC Booklet 2018, 6-7.)

FINCSC-sertifiointi ensimmäisenä kahdesta sertifiointitasosta mittaa organisaation kyberturvallisuuden tasoa sähköisesti täytettävällä itsearvioinnilla. Itsearviointi on organisaation täytettävissä yhdessä tai useammassa osassa ajasta ja paikasta riippumatta. Itsearviointiin vastaaminen tapahtuu tätä tarkoitusta varten tuotetussa verkkoportaalissa ennalta annettujen aikamääreiden puitteissa. Valmiin itsearvioinnin katselmoi arviointilaitos sen luottaessa arviointitoiminnassa sertifiointiin osallistuvan organisaation itsearvioinnissa antamien tietojen oikeellisuuteen. (FINCSC Booklet 2018, 6-7.)

FINCSC PLUS -sertifiointi jälkimmäisenä kahdesta sertifiointitasosta mittaa organisaation kyberturvallisuuden tasoa toisen tai kolmannen osapuolen ulkoisella auditoinnilla. Auditointi suoritetaan perustuen organisaation aiemmin hyväksytysti suorittamaan, voimassa olevaan FINCSC-sertifiointiin palvelun yhteydessä sovittavan aikataulun puitteissa. Auditoinnin toteuttaa arviointilaitos sen tarkastellessa sertifiointiin osallistuvan organisaation itsearvioinnissa antamien tietojen oikeellisuutta ja kattavuutta vaatimusten osalta esitettävään auditointinäyttöön perustuen. (FINCSC Booklet 2018, 6-7.)

Sertifioinnin hyväksytystä suorittamisesta sertifiointiin osallistuneelle organisaatiolle myönnetään joko FINCSC tai FINCSC PLUS -sertifikaatti. Sertifikaatti on voimassa määräajan edellyttäen, ettei sertifikaatin voimassaoloaikana organisaatiossa tapahdu sellaisia muutoksia, joilla voisi olla vaikutuksia sertifikaatin myöntämisen epäämiseen. Sertifioinnin lopputuloksesta riippumatta sertifiointiin osallistuneelle organisaatiolle luovutetaan sertifioinnista arviointiraportti. Raportti on kertomus sertifioinnin yhteydessä tehdyistä arviointimerkinnöistä ja mahdollisista kehityskohteista tietoverkon ja tietojärjestelmin suojaamiseksi tunnetuilta kyberuhkilta. (FINCSC Booklet 2018, 4-5.)

Sertifioinnin hyväksytysti suorittaneet organisaatiot esitetään fincsc.fi verkkosivustolla. Tiedot ovat saatavilla verkkosivustolla organisaatioiden sertifiointien voimassaoloajan, minkä jälkeen ne poistuvat, mikäli sertifiointia ei uusita annettuun määräaikaan mennessä. FINCSC-sertifiointi on voimassa yhden vuoden sertifikaatin myöntä-

misestä. FINCSC PLUS-sertifikaatti myönnetään sertifioinnin hyväksytysti suorittaneelle organisaatiolle kolmeksi vuodeksi kerrallaan palveluun osallistumisen ehtona olevan FINCSC-sertifikaatin myöntämispäivästä lukien. (FINCSC Booklet 2018, 4-7.)

3.1.3 Sertifiointivaatimukset

FINCSC-sertifiointijärjestelmässä sertifiointien välillä noudatetaan organisaatioille yhteisiä sertifiointivaatimuksia. Vaatimukset ovat kaikille sertifiointiin osallistuville lähtökohtaisesti samat organisaatioiden toisistaan eriävästä yhtiömuodosta, koosta tai toimialasta riippumatta. Vaihtelua vaatimusten välillä syntyy sertifioinnin suorittamisen yhteydessä organisaatioiden vastatessa omaa toimintaa kuvaaviin kysymyksiin. Sertifiointivaatimukset mukautuvat automaattisesti noudattamaan sertifiointiin osallistuvan organisaation kybertoimintaympäristön laajuutta ja luonnetta. (FINCSC Booklet 2018, 4.)

Sertifiointivaatimuksia koskevat kysymykset jakautuvat laajempiin kysymysosa-alueisiin. Sertifiointiin kuuluvia kysymysosa-alueita on yhteensä 11:sta kappaletta, joista jokainen kuvaa omaa erityistä aihepiiriä. Aihepiirien käsittely pyrkii toteuttamaan sertifioinnin taustalla vaikuttavaa ideologiaa kokonaisvaltaisesta ja syvyyssuuntaisesta turvallisuusperiaatteesta kyberturvallisuuden varmistamiseen käytettävistä peräkkäisistä ja toisistaan riippumattomista suojauksista. Aihepiirien käsittelyn laajuudet voivat poiketa toisistaan kysymysten lukumäärällä ja pisteytyksellä mitattuna. (FINCSC sertifiointivaatimukset 2018.)

Sertifioinneissa sertifiointivaatimusten täyttymistä organisaatiossa arvioidaan hyväksytty/hylätty-asteikolla hyväksytyn sertifioinnin voidessa sisältää erinäisen määrän vaatimuspoikkeamia. Poikkeamaa epäiltäessä sertifioinnissa kiinnitetään erityistä huomiota poikkeaman todelliseen olemassa oloon tarkastelemalla sekä sen perusteltavuutta, että organisaatiossa vaatimuksen varalta mahdollisesti käytössä olevia kompensoivia kontrolleja. Vaatimuspoikkeaman esiintyessä poikkeamat pisteytetään niiden vakavuuden mukaan yhteen kolmesta käytettävästä luokitustasosta. (FINCSC sertifiointivaatimukset 2018.)

Vaatimuspoikkeamien pisteytyksessä käytettävät luokitustasot ovat pieni, keskisuuri ja suuri poikkeama. Poikkeaman osalta käytettävä luokitus kuvaa poikkeamasta organisaatiolle aiheutuvia haitallisia vaikutuksia taikka alttiutta joutua näiden haitallisten vaikutusten kohteeksi. Pienen poikkeaman vaikutukset organisaatioon ovat oletusarvoisesti vähäisiä, kun taas keskisuuri poikkeama voi toteutuessaan olla omiaan aiheuttamaan vahinkoa organisaatiolle. Suuren poikkeaman vaikutukset organisaation ja tietojärjestelmien toiminnalle voivat olla merkittäviä. (FINCSC sertifiointivaatimukset 2018.)

Vaatimuspoikkeamien osalta noudatettavat pisteytysperusteet ja –rajat kuvataan sertifiointivaatimusten yhteydessä. Sertifiointivaatimukset ovat kysymystyypiltään joko avoimia tai suljettuja kysymyksiä. Suljetut kysymykset sisältävät sekä kyllä/ei-kysymyksiä että monivalintakysymyksiä. Kysymys voi kerrallaan tuottaa enintään yhden pisteytettävän poikkeaman, joka huomioidaan lopullisessa sertifiointia koskevassa arviossa. Monivalintakysymyksissä kysymysten vastaukset pisteytetään kysymyskohdassa valitun suurimman poikkeaman aiheuttaman vastausvaihtoehdon mukaan. (FINCSC sertifiointivaatimukset 2018.)

3.1.4 Sertifiointiprosessi

FINCSC-sertifiointijärjestelmässä sertifiointipalvelut noudattavat palvelukohtaisesti määriteltyä prosessin kulkua. Prosessin kulku jakautuu kummankin palvelun osalta viiteen päävaiheeseen. Päävaiheet määrittävät sertifiointia hakevan organisaation palvelun käytön aikaisia toimia ja toimien tuloksena syntyviä tuotoksia. Prosessin kulku on riippuvainen sertifiointiin osallistuvien osapuolten palvelun aikaisille päätöksille sekä yksittäisissä toimissa suoriutumiselle. (FINCSC Booklet 2018, 10-11.)

FINCSC-sertifiointi käynnistyy organisaation jättäessä sertifiointihakemuksen fincsc.fi verkkosivustolla valitsemalleen arviointilaitokselle. Arviointilaitoksen hyväksyttyä hakemuksen, organisaatio saa käyttöönsä käyttäjätunnukset FINCSC -verkkoportaaliin kirjautumiseksi ja itsearvioinnin aloittamiseksi. Valmis itsearviointi palautetaan arviointilaitokselle katselmoitavaksi. Itsearviointia katselmoidessaan arviointilaitos voi

palauttaa arvioinnin organisaatiolle täydennettäväksi ennen lopullisen päätöksen antamista sertifioinnin hyväksymisestä tai hylkäämisestä. (FINCSC Booklet 2018, 10-11.)

FINCSC PLUS-sertifiointiin hakeudutaan tarjousmenettelyllä organisaation jättäessä tarjouspyynnön FINCSC –verkkoportaalissa valitsemilleen arviointilaitoksille. Palveluntarjoajan selvittyä organisaatio tekee päätöksen tilauksesta. Organisaation päästessä sopimukseen arviointilaitoksen kanssa palvelun toimittamisesta, kerää se kasaan vaatimustenmukaisuuden todentamisessa käytettävän auditointinäytön. Arviointilaitos suorittaa organisaatiossa ulkoisen auditoinnin. Auditoinnin päätteeksi arviointilaitos tekee päätöksen sertifioinnin hyväksymisestä tai hylkäämisestä. (FINCSC Booklet 2018, 10-11.)

FINCSC PLUS –sertifiointiin kuuluvassa ulkoisessa auditoinnissa organisaation vaatimustenmukaisuutta arvioidaan arviointilaitoksen käytettävissä olevin ja sille määrättävin arviointimenetelmin ja -tekniikoin. Sertifioinnissa käytettäviin arviointimenetelmiin sisältyy arvioinnin piiriin kuuluvaan organisaation hallinnolliseen, toiminnalliseen, fyysiseen ja tekniseen ympäristöön kohdistettavat testaukset, tarkastukset ja haastattelut. Arviointimenetelmien käyttöä sertifiointivaatimusten täyttymisen todentamisessa ohjaa pyrkimys mahdollisimman kattavan ja todenmukaisen kuvan muodostamiseen arviointialueesta sekä kuuluvista yksittäisistä arviointikohteista.

3.1.5 Arviointitoiminta

FINCSC-sertifiointijärjestelmään kuuluvien sertifiointipalveluiden toimittamisesta organisaatioille vastaavat pätevyyden omaavat auktorisoidut arviointilaitokset. Arviointilaitokset hakevat pätevyyden tunnustamista kullekin sertifiointitasolle erikseen. Arviointilaitosten pätevyyden tunnustaa JYVSECTEC sen varmistuttua auktorisointivaatimusten täyttymisestä ja päästyä sopimukseen sertifiointipalveluiden toimittamisesta. Sertifiointipalveluiden toimittamisesta ja siihen liittyvistä ehdoista sovitaan kirjallisesti auktorisoinnin yhteydessä tehtävin palvelusopimuksin. (Authorization 2020.)

Auktorisoinnissa arviointilaitokseksi hakeutuvan organisaation pätevyyden tunnustaminen perustuu sekä yritykselle organisaationa, että arviointitehtäviä suorittaville

tarkastajille henkilöinä asetettaviin ennakkovaatimuksiin. Yrityskohtaisten vaatimusten osalta organisaatiolta edellytetään voimassa olevaa FINCSC-sertifikaattia sekä ulkoisin selvityksin osoitettavaa toiminnallista laatua ja taloudellista vakautta huolehtia liiketoimintavelvoitteistaan ja sitoumuksistaan. Henkilöstölle asetettavat vaatimukset kohdistuvat tarkastajien koulutuksen ja työkokemuksen kautta hankkiman riittävän ammatillisen osaamisen osoittamiseen. (Authorization 2020.)

Auktorisointi arviointilaitoksille tarjottavana palveluna pitää sisällään arviointitehtäviä suorittavien tarkastajien kouluttamisen ja ohjeistamisen sertifiointijärjestelmään. Auktorisoinnissa tarkastajat perehdytään arviointilaitoksen pätevyysalueen mukaisten sertifiointipalveluiden toimittamiseen liittyviin käytännön toimiin kyberturvallisuuden arviointitoiminnan harjoittamisesta. Arviointilaitoksen lukuun arviointitehtäviä suorittavien tarkastajien odotetaan ennen arviointitoimintaan osallistumista tuntevan sertifiointijärjestelmän ja hallitsevan arviointilaitoksen pätevyysalueen mukaisiin sertifiointipalveluihin kuuluvien arviointimenetelmien ja –tekniikoiden käytön. (Authorization 2020.)

Arviointilaitosten harjoittaman kyberturvallisuuden arviointitoiminnan tarkoituksena on paitsi arvioida sertifiointivaatimusten täyttymistä myös tuottaa tietoa toiminnan kehityskohteista ja kasvattaa ymmärrystä kyberturvallisuudesta. Ratkaisevaa arviointitoiminnan harjoittamisessa on kyky erottaa arviointitoiminta suorasta konsultoinnista. Arviointitoiminnassa toiminnan tarkoituksena on vaikuttaa asiakasorganisaatioiden tietoisuuteen kyberturvallisuudesta ja oman toiminnan tilasta kyberhäiriötilanteisiin varautumisessa eikä niinkään valmentaa yksittäisten tietoturvakontrollien käyttöönotossa tai sertifiointivaatimuksiin vastaamisessa.

Arviointitoimintaa harjoittaessaan arviointilaitosten odotetaan toimivan ammattitaitoisesti, riippumattomasti ja läpinäkyvästi. Ammattitaitoisuuteen liittyy keskeisesti asiakaslähtöinen työskentelytapa toteuttaa arviointitoimintaa parhaaseen saatavilla olevaan tietoon ja osaamiseen pohjautuen. Riippumattomuus merkitsee arviointilaitokselle velvoitetta pidättäytyä kaikista sellaisista tilanteista, joissa ulkopuoliset, arvi-

ointiin kuulumattomat tekijät voisivat päästä vaikuttamaan sertifiointitulokseen. Läpinäkyvyys tarkoittaa puolestaan, että arviointilaitoksen on mitään salaamatta kyettävä avoimesti viestimään asiakasorganisaatiolle toteuttamistaan arviointitoimista.

3.2 Cyber Essentials -sertifiointijärjestelmä

3.2.1 Yleistä

Cyber Essentials -sertifiointijärjestelmä on Iso-Britannian hallinnon 5.päivänä kesäkuuta vuonna 2014 julkaisema ja elinkeinoelämän tukema kyberturvallisuuden arviointimalli. Mallin tarkoituksena on ollut tuoda Iso-Britannian sisämarkkinoille sieltä aiemmin puuttunut kaikille yrityksille soveltuva, yhteinen kyberturvallisuussertifikaatti. Sertifikaatilla hallinto on pyrkinyt luomaan edullisen ja käytännöllisen välineen, jolla se on voinut kannustaa yrityksiä ottamaan käyttöön perustietoturvakontrolleja yleisimmiltä kyberuhkilta suojautumiseksi ja kyberrikollisuuden torjumiseksi. (New scheme to help businesses defend against cyber threats goes live 2014.)

Cyber Essentials -sertifiointijärjestelmä on perustunut 25. päivänä marraskuuta vuonna 2011 julkaistun Iso-Britannian kansallisen kyberturvallisuus strategian toimeenpanoon. Kyberturvallisuusstrategian visiona on ollut saavuttaa Iso-Britanniassa vuoteen 2015 mennessä mittava taloudellinen ja sosiaalinen arvo elinvoimaisesta, joustavasta ja turvallisesta kybertoimintaympäristöstä (The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world 2011, 21). Cyber Essentials -sertifiointijärjestelmällä on tuettu tämän tahtotilan toteutumista vastaamalla strategian tavoitteisiin kyberrikollisuuden torjunnasta ja kyberuhkien sietokyvyn kehittämisestä. (2010 to 2015 government policy: cyber security 2015, 21).

Cyber Essentials -sertifiointijärjestelmän käyttö pohjautuu sekä yritysten omaehtoisuuteen, että yleiseen velvoittavuuteen. Hallinto on julkista hankintamenettelyä koskevalla ilmoituksellaan tehnyt Cyber Essentials -sertifiointijärjestelmän pakolliseksi vuoden 2014 lokakuun 1. päivän jälkeen julkaistuihin siviilihallinnon hankintoihin. Yrityksiltä on edellytetty sertifiointijärjestelmän mukaisiin sertifiointeihin osallistumista toimituksissa, joihin on sisältynyt henkilötietojen tai muiden sensitiivisten tietojen

käsittelyä taikka tiettyjen tieto- ja viestintätekniikan tuotteiden ja –palvelujen tarjoamista. (Procurement Policy Note 09/14: Cyber Essentials Scheme 2014.)

Cyber Essentials -sertifiointijärjestelmän käyttövelvoitteella hallinto on pyrkinyt paitsi vähentämään toimitusketjuihinsa kohdistuvia kyberturvallisuusriskejä myös tukemaan sertifiointijärjestelmän vankempaa jalkautumista elinkeinoelämään. Sertifiointijärjestelmän käytön on nähty tuovan elinkeinoelämän toimijoille sekä uutta liiketoimintaa että vahvistavan asiakkaiden mielikuvaa toiminnan turvallisuudesta ja rakentavan käsitystä yrityksen tietoturvallisuustasosta. Käytöllä koetaan parannettavan yritysten kyberhygieniaa parhaiden käytänteiden omaksumisessa osaksi liiketoimintaa. (Procurement Policy Note 09/14: Cyber Essentials Scheme 2014.)

Iso-Britannian hallinnon toimeksiannosta 1990-luvun alkupuolelta lähtien laaditussa turvallisuustutkimuksessa on selvitetty kybertoimintaympäristössä harjoitettavaan liiketoimintaan kohdistuvia riskejä ja tietoturvapoikkeamien esiintyvyyttä. Vuodelta 2014 julkaistussa raportissa tutkimustulokset osoittivat, että pienyrityksistä 60% ja suuryrityksistä 81% oli kokenut edeltävän vuoden aikana tietoturvapoikkeaman. Tietoturvapoikkeamien kuvattiin johtuvan sekä haittaohjelmatartunnoista, kyberhyökkäyksistä, henkilökunnan aiheuttamista tapaturmista, että varkauksista ja petoksista. (2014 information security breaches survey: technical survey 2014, 4 ja 13.)

3.2.2 Sertifiointitasot

Cyber Essentials -sertifiointijärjestelmä koostuu kahdesta sertifiointitasosta Cyber Essentials ja Cyber Essentials Plus. Sertifiointitasot ovat kaiken kokoisten organisaatioiden saatavilla niiden toimialaan tai kotipaikkaan katsomatta. Organisaation hakeutuessa sertifiointiin tulee sen hyväksyä palvelun yhteydessä esitettävät toimitusehdot. Cyber Essentials -sertifiointi perustuu organisaatiolta veloitettavaan kiinteään kertamaksuun, Cyber Essentials Plus -sertifioinnin noudattaessa tarjousperusteista hinnoittelua. (Cyber Essentials 2020.)

Cyber Essentials -sertifiointi ensimmäisenä mainituista sertifiointitasoista pohjautuu organisaation vastuuhenkilön vahvistamaan itsearviointiin. Sertifioinnissa organisaatio arvioi omakohtaisesti toiminnassaan käyttöönottamien tietoturvakontrollien asianmukaisuutta kyselylomakkeessa esitettäviin kysymyksiin todenmukaisesti vastaamalla. Kyselylomakkeeseen täytettyjen vastausten tarkistamisesta vastaa arviointitoimintaa harjoittava akkreditoitu sertifiointielin sen luottaessa arvioinnissa itsearvioinnin täyttäneen organisaation vastausten paikkansa pitävyyteen. (Cyber Essentials 2020; Cyber Essentials – Self-Assessment Preparation Booklet 2020, 1.)

Cyber Essentials Plus -sertifiointi toisena, jälkimmäisenä sertifiointitasona täydentää Cyber Essentials -sertifiointia korkeamman varmuustason arviointimenettelynä. Cyber Essentials Plus -sertifiointi tarkistaa haavoittuvuustestauksella suojaavatko itsearvioinnissa väitetyt tietoturvakontrollit tosiallisesti organisaatiota kyberhyökkäyksiltä. Tiukemmasta arvioinnista johtuen kyseistä sertifiointia suositellaan käytettävän silloin, kun organisaation riski joutua kyberhyökkäyksen kohteeksi tai kärsiä kyberhäiriötilanteiden haittavaikutuksista arvioidaan korkeammaksi. (Cyber Essentials 2020.)

Sertifioinnin hyväksytystä suorittamisesta sertifiointiin osallistuneelle organisaatiolle myönnetään joko Cyber Essentials tai Cyber Essentials Plus -sertifikaatti. Sertifikaatti on voimassa määräajan edellyttäen, ettei sertifikaatin voimassaoloaikana organisaatiossa tapahdu sellaisia muutoksia, jotka voisivat johtaa sertifikaatin epäämiseen. Sertifioinnin lopputuloksesta riippumatta sertifiointiin osallistuneelle organisaatiolle luovutetaan sertifioinnista arviointiraportti. Raportti on kertomus sertifioinnin yhteydessä tehdyistä arviointimerkinnöistä ja mahdollisista kehityskohteista tietoverkon ja tietojärjestelmin suojaamiseksi yleisesti tunnetuilta kyberuhkilta. (Cyber Essentials 2020.)

3.2.3 Sertifiointivaatimukset

Cyber Essentials -sertifiointijärjestelmässä sertifiointien välillä noudatetaan organisaatioille yhteisiä sertifiointivaatimuksia. Sertifiointivaatimusten yhteenlaskettu luku-

määrä on 45 vaatimusta viidessä eri osa-alueessa, kun jätetään huomiotta organisaation toimintaa tai vastuuvakuutuksen myöntämistä koskevat taustakysymykset. Vaatimusten lopulliseen lukumäärään vaikuttaa lisäksi sertifiointiin kuuluvan itsearvioinnin yhteydessä annettavat vastaukset. Sertifiointivaatimukset mukautuvat noudattamaan vastauksissa esiintyvän organisaation kybertoimintaympäristön laajuutta ja luonnetta. (Cyber Essentials – Self-Assessment Preparation Booklet 2020.)

Sertifiointivaatimusten osalta käytettävät viisi osa-aluetta perustuvat Iso-Britannian hallinnon aiemmin 5. päivänä syyskuuta vuonna 2012 julkaisemaan ohjeeseen 10 askelta kyberturvallisuuteen. Ohjeessa hallinto kuvaa tyypillisen kyberhyökkäyksen etenemistä hyökkäyksessä käytettävistä tekniikoista ja taktiikoista sekä opastaa organisaatioille kymmenen tapaa torjua valtaosan organisaatioita vastaan kohdistuvista kyberhyökkäyksistä. Ohjeesta Cyber Essentials -sertifiointijärjestelmään johdetut sertifiointivaatimusten viisi osa-aluetta painottuvat teknisiin tietoturvakontrolleihin. (Procurement Policy Note 09/14: Cyber Essentials Scheme 2014, 2.)

Tekniset tietoturvakontrollit käsittelevät organisaation tapoja suojata verkkoyhteyksiä, hallita tietoturva-asetuksia, toteuttaa käyttäjähallintaa, torjua haittaohjelmatartuntoja sekä huolehtia ohjelmistopäivityksistä. Osa-alueiden kautta tarkastelun ulkopuolelle jäävät IASME konsortion omaan IASME Governance standardiin sisältyvät organisaation kybertoimintaympäristön suojaamiseen liittyvät fyysiset, hallinnolliset ja toiminnalliset tekijät. Cyber Essentials -sertifiointi voi koko organisaation sijaan keskittyä tarkastelemaan vain tiettyä organisaation loogista osaa ja sen vaatimuksiin vastaavuutta. (Procurement Policy Note 09/14: Cyber Essentials Scheme 2014, 2; Frequently asked questions 2020; IASME Governance includes GDPR requirements & Cyber Essentials 2020.)

Sertifioinneissa tietoturvavaatimusten täyttymistä arvioidaan hyväksytty/hylätty-asteikolla hyväksytyn sertifioinnin edellyttäessä jokaisen vaatimuskohdan täyttymistä. Sertifioinnin poiketessa vaaditusta ei sertifiointia voida hyväksyä ilman perusteltua syytä tai korvaavaa turvallisuuskontrollia. Täyttymättä jäävät vaatimukset raportoidaan sertifioinnin hylkäävinä vaatimuspoikkeamina. (Frequently asked questions 2020.)

3.2.4 Sertifiointiprosessi

Cyber Essentials -sertifiointijärjestelmässä sertifiointiprosessi noudattaa sertifiointitasoittain määriteltyä työnkulkua. Cyber Essentials -sertifiointi koostuu kolmesta päävaiheesta, joita Cyber Essentials Plus -sertifiointiin kuuluvat kaksi vaihetta täydentävät. Sertifiointitasot voidaan suorittaa joko yksittäin sertifiointitaso kerrallaan tai samanaikaisesti peräjälkeen. Cyber Essentials Plus -sertifiointiin osallistuminen edellyttää Cyber Essentials- sertifiointiin kuuluvan itsearvioinnin hyväksyttyä suorittamista. (Frequently asked questions 2020.)

Cyber Essentials -sertifiointi käynnistyy IASME konsortion verkkosivujen kautta jätettävällä sähköisellä hakemuksella. Hakemus välittyy automaattisesti käsiteltäväksi sattuman varaisesti arvottavalle akkreditoidulle arviointilaitokselle. Vaihtoehtoisesti sertifiointiin hakeutuva organisaatio voi ottaa suoraan yhteyttä haluamaansa akkreditoituun arviointilaitokseen valitakseen itse sertifioinnin tuottavan palvelutoimittajan. Arviointilaitos voidaan valita kyseisen sertifiointitason pätevyysalueen mukaisten akkreditoitujen arviointilaitosten joukosta. (Apply for Cyber Essentials verified self assessment 2020.)

Sertifiointimaksun suoritettuaan organisaatio saa tunnukset IASMEn verkkoalustaan sertifioinnin aloittamiseksi. Aikaa sertifioinnin suorittamiseen on varattu kuusi kuukautta hakemuksesta. Itsearvioinnin täytettyään akkreditoitu arviointilaitos katselmoi kysymysten vastaukset ja arvioi organisaation kyberturvallisuustason vaatimustenmukaisuutta. Vaatimusten täyttämättä jäämisestä johtuvat poikkeamat kirjataan kommentteineen organisaatiolle sertifioinnin päätteeksi luovutettavaan arviointiraporttiin kyberturvallisuuden kehittämiseksi. (Apply for Cyber Essentials verified self assessment 2020.)

Asetettujen sertifiointivaatimusten täyttyessä organisaatiolle myönnetään Cyber Essentials -sertifikaatti. Organisaatiolla on kolme kuukautta sertifikaatin myöntämisestä aikaa hakeutua ja suorittaa Cyber Essentials Plus -sertifiointi. Cyber Essentials Plus -sertifiointiin hakeudutaan joko IASME konsortion verkkosivuilta jätettävällä tarjous-

pyynnöllä tai arviointilaitokseen suoraan kontaktoimalla. Organisaation päästessä arviointilaitoksen kanssa sopimukseen palvelumaksuista voidaan sertifioinnin suorittaminen aloittaa. (Get a quote for Cyber Essentials Plus 2020.)

Cyber Essentials Plus -sertifioinnissa arviointilaitos varmistuu Cyber Essentials -sertifiointitasolla suoritetun itsearvioinnin tulosten oikeellisuudesta. Arviointilaitos suorittaa itsearvioinnin tulosten tarkastamiseksi sekä sisäisiä että ulkoisia testejä. Testit koostuvat kuudesta organisaatiossa paikan päällä tai etänä verkon ylitse suoritettavasta testitapauksesta. Testitapauksilla selvitetään organisaation kybertoimintaympäristön haavoittuvuuksia, ohjelmistopäivitysten ajanmukaisuutta ja haittaohjelmatartuntojen käsittelyä päätelaitteilla. (Get a quote for Cyber Essentials Plus 2020; Cyber Essentials Plus: Illustrative Test Specification 2020.)

3.2.5 Arviointitoiminta

Cyber Essentials -sertifiointijärjestelmään kuuluvien sertifiointien jakelusta on 1. päivästä huhtikuuta 2020 lähtien yksinomaan vastannut Iso-Britannian kyberturvallisuuskeskuksen kanssa kumppanuussopimuksen laatinut IASME konsortio. Ennen nykyiseen asemaansa nimittämistä, IASME konsortio toimi samaisessa tehtävässä jaetussa vastuussa The Council for Registered Ethical Security Testers, CREST kanssa. Akkreditointielimenä IASME konsortio hyväksyy Cyber Essentials ja Cyber Essentials Plus -sertifiointien toimituksesta vastaavat akkreditoidut arviointilaitokset. (New look scheme protects businesses from cyber attack 2020.)

Akkreditoituna arviointilaitoksena toimiakseen organisaation edellytetään täyttävän toiminnalle asetetut turvallisuus- ja laatuvaatimukset. Turvallisuus- ja laatuvaatimusten täyttämisen todentamiseksi arviointilaitoksen on osoitettava omassa toiminnassaan noudattaman tietoturvallisuuden hallintajärjestelmän ja laatujärjestelmän vaatimustenmukaisuus IASMEn hyväksymiä sertifiointijärjestelmiä käyttäen. Johtamisjärjestelmien sertifiointien ohella organisaation edellytetään läpäisevän Cyber Essentials -sertifioinnin sekä osallistuvan pätevyysalueittain järjestettäviin koulutuksiin. (Become an assessor 2020.)

Pätevyysalueittain järjestettäviä koulutuksia tarjotaan akkreditoitujen arviointilaitosten lukuun sertifiointeja suorittavalle henkilöstölle osana arvioijaksi hyväksyntää. Arvioijaksi hyväksyntä edellyttää akkreditoidun arviointilaitoksen henkilöstöltä paitsi koulutukseen osallistumista myös siihen kuuluvan kokeen läpäisyä. Kokeen sijasta henkilö voi osoittaa asianhallintaa IASMEn hyväksymillä henkilösertifioinnilla. Henkilösertifioinnit toimivat myös pohjavaatimuksena henkilöille, joiden on tarkoitus toteuttaa Cyber Essentials Plus -sertifiointeja tai toimia sertifioinnin päätarkastajana. (Become an assessor 2020.)

Hyväksyntää akkreditoiduksi arviointilaitokseksi haetaan sertifiointitasoittain IASME konsortiolta toiminnalle ja henkilöstölle asetettujen ennakkoehtojen täyttyessä. Akkreditointiprosessin päättyessä IASME laatii sertifiointipalvelujen tarjoamiseen oikeutettujen akkreditoitujen arviointilaitosten kanssa asiaan liittyvän sopimuksen. Sopimuksen allekirjoituksen myötä arviointilaitos listataan IASMEn ylläpitämään hakemistoon akkreditoiduista arviointilaitoksista. Hakemistolistauksen perusteella organisaatiot voivat tilata kyseiselle pätevyysalueelle kuuluvia sertifiointeja arviointilaitokselta. (Become an assessor 2020.)

3.3 Valtionhallinnon tietoturvallisuuden arvioinnit

3.3.1 Yleistä

Suomen eduskunnan päätöksen mukaisesti 21. päivänä toukokuuta vuonna 1999 säädetty laki viranomaisten toiminnan julkisuudesta (621/1999) on edellyttänyt valtion- ja julkishallinnon viranomaisten toimivan avoimesti ja hyvää tiedonhallintatapaa toteuttaen. Hyvän tiedonhallintatavan toteuttamiseksi viranomaisen on kuulunut huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen tietoturvallisuudesta. Velvoite tietoturvallisuudesta huolehtimiseen on ollut voimassa käsiteltäessä tietoja niin viranomaisissa kuin viranomaisen toimeksiannoissa. (L 621/1999, 4:18§ ja 7:26§.)

Valtionhallinnon viranomaisten tietoturvallisuuden eteen tehtävistä toimenpiteistä on säädetty tarkemmin valtioneuvoston päätöksellä 1. päivänä heinäkuuta vuonna

2010 annetussa valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010). Tietoturvallisuusasetus määritteli kaikkia valtionhallinnon viranomaisia koskevat yleiset tietoturvallisuusvaatimukset sekä asetuksen mukaisesta asiakirjojen luokittelusta päättäneitä koskevat erityisvaatimukset (A 681/2010. 1:1§ ja 2:7§). Asetuksen täytäntöönpanoa tehostettiin Valtiovarainministeriön toimesta annetulla ohjeistuksella (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 6).

Valtiovarainministeriö kuvasi 19. päivänä lokakuuta vuonna 2010 hyväksytyssä ohjeessaan tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta VAHTI 2/2010 tietoturvallisuutta koskevat yksityiskohtaiset vaatimukset. Ohjeessa kuvatut vaatimukset kohdistuivat menettelytapoihin ja prosesseihin teknisten ja fyysisten ratkaisuiden jäädessä sivuun. Tietoturvallisuuden toteuttamiseksi ja arvioimiseksi oli viranomaisen tästä johtuen huomioitava myös asetuksen voimaantulon jälkeen julkaistut muut valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI-ohjeet sekä osin kansallinen turvallisuusauditointikriteeristö, KATAKRI. (Ohje tietoturvallisuuden arviointilaitoksille 2020, 11-12.)

KATAKRI on sisäisen turvallisuuden ministeriryhmän toimesta 26. päivänä marraskuuta vuonna 2009 valmistuneeksi hyväksytty sisäisen turvallisuuden ohjelman toimenpide. Toimenpiteellä on luotu yhteinen yritysturvallisuuskriteeristö yhteisöturvallisuusmenettelyn yhtenäistämiseksi ja omavalvonnan sekä auditoinnin parantamiseksi. KATAKRIn ensisijaisena tehtävänä on ollut toimia työkaluna kansallisen turvallisuusviranomaisen varmentaessa suomalaisten yritysten ja yhteisöjen tietoturvallisuuden tasoa suhteessa kansainvälisiin tietoturvavelvoitteisiin sekä toissijaisesti tukea yrityksiä omaehtoisen tietoturvallisuustyön kehittämisessä. (Turvallinen elämä jokaiselle 2008, 34-37; Kansallinen turvallisuusauditointikriteeristö 2009, 1-6; ks. L 726/2014, 5:33§.)

KATAKRI on vuonna 2011 ilmestyneen toisen päivitetyn julkaisuversion myötä täyttänyt kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) ohella tietoturva-asetuksen (681/2010) ja VAHTI-ohjeiden mukaiset tietoturvavaatimukset. Päivityksen myötä KATAKRIa on voitu käyttää sen alkuperäisen käyttötarkoituksen

ohella myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuuden arvioinneissa. (Kansallisen turvallisuusauditointikriteeristön (KATAKRI) neuvoa-antava työryhmä 2012.) Tietoturvallisuuden arviointiperusteena on edellä olevien lisäksi voinut toimia myös muun muassa Suomessa kansallisesti vahvistettu kansainvälinen tietoturvallisuuden hallintajärjestelmästandardi ISO/IEC 27001 (Ohje tietoturvallisuuden arviointilaitoksille 2020, 8-9).

3.3.2 Tietoturvallisuustasot

VAHTI-ohjeita ja KATAKRIa arviointiperusteena käyttävät valtionhallinnon tietoturvallisuuden arvioinnit jakautuvat tietoturvavaatimusten osalta kolmeen toisistaan eriävään tasoon. *”Alin viranomaisen tietojenkäsittely-ympäristöille sallittu taso on tietoturvallisuuden perustaso.”* Tätä seuraavat kaksi tasoa ovat tietoturvallisuuden korotettu ja korkea taso. Tietoturvallisuuden taso ilmaisee, minkä luokituksen mukaisia viranomaisen salassa pidettäviä asiakirjoja tai sensitiivisiä tietoja kyseisessä tietojenkäsittely-ympäristössä on sallittua käsitellä ja säilyttää selväkielisessä muodossa. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 13-16.)

Tietoturva-asetuksen (681/2010) mukaisesti asiakirjojen luokittelusta päättäneen valtionhallinnon viranomaisen salassa pidettävät asiakirjat luokitellaan neljään suojaustasoon. Asiakirjojen luokittelussa käytettävät suojaustasot ovat suojaustaso IV, III, II ja I. Suojaustasoon IV voidaan luokitella myös muita kuin salassa pidettäväksi säädettyjä asiakirjoja, jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa tai siihen sisältyviä tietoja saa käyttää tai luovuttaa vain määrättyyn tarkoitukseen ja jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä. (A 681/2010, 2:7§ ja 3:8-9§.)

Tietoturvallisuuden perustason ympäristö mahdollistaa suojaustasoa IV sisältävien tietojen ja asiakirjojen selväkielisen käsittelyn. Suojaustasoa III sisältävien tietojen ja asiakirjojen käsittely selväkielisessä muodossa edellyttää vähintäänkin korotetun tie-

toturvallisuustason ympäristöä. Korkean tietoturvallisuustason ympäristö sallii suojaustasoa II ja sitä luokituksessaan alempana olevien asiakirjojen käsittelyn. Suojaustasoa I sisältävien tietojen selväkielinen käsittely voidaan toteuttaa vain erillisverkkoympäristöissä, joissa ei ole liitäntöjä alemman tietoturvallisuustason ympäristöihin. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 15-16.)

Tietoturvallisuustasojen mukaisella toiminnalla viranomainen tai tämän lukuun toimiva voi varmistua riittävästä tietoturvallisuuden tasosta suhteessa suojattavaan etuun. Suojaustason IV asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa yleiselle tai yksityiselle edulle kun suojaustason III asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai käyttö voi haitan sijasta aiheuttaa vahinkoa yleiselle tai yksityiselle edulle. Suojaustason II ja I asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi taas edellä mainitussa järjestyksessä lueteltuna joko aiheuttaa merkittävää tai erityisen suurta vahinkoa yleiselle edulle. (A 681/2010, 3:8-9§.)

Asiakirjaan tai siihen sisältyvän salassa pidettävän tiedon oikeudettoman paljastumisen tai käytön voidessa aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle julkisuuslain määrätyissä kohdissa eritellylle yleiselle edulle voidaan asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta käyttää erityistä turvallisuusluokitusmerkintää. Suojaustasoja IV-I vastaavat turvallisuusluokitusmerkinnät ovat järjestyksessä lueteltuina käyttö rajoitettu, luottamuksellinen, salainen ja erittäin salainen. Turvallisuusluokiteltu aineisto noudattaa suojaustasoluokitellun aineiston kanssa yhtäläisiä tietoturvavaatimuksia. (A 681/2010, 3:11§.)

3.3.3 Arviointiperusteet

Valtionhallinnon tietoturvallisuuden arvioinneissa arviointiperusteena käytettävä tietoturva-asetus (681/2010) ja sen täytäntöönpanoon liittyvä VAHTI-ohjeistus pitää sisällään 1200 vaatimusta. Vastaavasti kansallisen turvallisuusauditointikriteeristön uusimmassa julkaisuversiossa KATAKRI 2015 on 45 vaatimusta kolmessa osa-alueessa.

Mainitut osa-alueet ovat organisaation johtamisvalmiuksia mittaava turvallisuusjohtamisen osa-alue, tietojen käyttöympäristöä tarkasteleva fyysisen turvallisuuden osa-alue ja tekniseen tietojenkäsittely-ympäristöön painottuva teknisen turvallisuuden osa-alue. (Luottamuksen lähteillä 2019, 22; Katakri 2015.)

Tietoturvallisuuden arvioinnit kohdistuvat organisaation siihen osaan, jossa viranomaisen salassa pidettävää tai muutoin sensitiivistä tietoa on määrä käsitellä ja säilyttää. Arviointi voidaan toteuttaa joko kokonaisena tai osittaisena keskittyen tiettyyn arviointiperusteiden mukaiseen osa-alueeseen. Esimerkiksi KATAKRI-arvioinneissa arviointi voidaan tehdä vain fyysisen turvallisuuden osa-aluetta vasten. Osittaisen arvioinnin perusteella organisaatio ei voi kuitenkaan saavuttaa yleispätevää VAHTI- tai KATAKRI kelpoisuutta. (Ohje tietoturvallisuuden arviointilaitoksille 2020, 13-14.)

Tietoturvallisuuden arvioinneissa tietoturvavaatimusten täyttymistä arvioidaan hyväksytty/hylätty-asteikolla hyväksytyn arvioinnin edellyttäessä kaikkien arviointiperusteissa esitettyjen vaatimuskohtien täyttymistä. Toiminnan poiketessa asetetusta raportoidaan kyseiset kohdat poikkeamina. Poikkeamat priorisoidaan niiden vakavuuden mukaan kolmeen tasoon. Käytettävät tasot ovat lievä poikkeama, keskitason poikkeama ja vakava poikkeama. Yksittäinen vaatimuskohta voidaan myös tulkita arviointikohteeseen soveltumattomaksi. (Ohje tietoturvallisuuden arviointilaitoksille 2020, 13-14.)

3.3.4 Arviointimenettely

Arviointiperusteena VAHTI-ohjeita ja KATAKRIa käyttävät valtionhallinnon tietoturvallisuuden arvioinnit noudattavat soveltuvilta osin työnkulultaan kansainvälisen ISO/IEC 17021 ja tätä täydentävän ISO/IEC 27006 standardin mukaista menettelyä. Standardit kuvaavat yksityiskohtaiset prosessivaatimukset johtamisjärjestelmäsertifiointien, kuten tietoturvallisuuden hallintajärjestelmäsertifiointien toteuttamiseksi. Arvioinneissa voidaan tietoturvallisuuden arviointilaitoksille annetun ohjeen nojalla käyttää myös standardien ISO 19011 ja ISO/IEC 27007 mukaisia menettelyitä. (Ohje tietoturvallisuuden arviointilaitoksille 2020, 15).

Valtionhallinnon tietoturvallisuuden arvioinnit käynnistyvät viranomaisen tai toimeksiannosta tämän lukuun toimivan yrityksen tai yhteisön arviointitaholle esittämästä pyynnöstä. Pyynnön tietoturvallisuuden arvioinnista voi tehdä myös valtiovarainministeriö koskien valtionhallinnon viranomaisen määräämisvallassa olevaa tietojärjestelmien tai tietoliikennejärjestelyjen yleistä tietoturvallisuuden tasoa. Tietoturvallisuuden arviointia koskevasta pyynnöstä käytetään yleisesti nimitystä toimeksianto sen ollessa arviointitahon ja arviointia pyytävän välillä laadittu kirjallinen sopimus. (L 1406/2011, 4-5§; Ohje tietoturvallisuuden arviointilaitoksille 2020, 13-14.)

Toimeksiannossa sovitaan muun ohella arvioinnin kohteesta ja arviointiperusteista sekä arvioinnin laajuudesta ja kestosta että arviointitehtävästä perittävästä maksusta (Ohje tietoturvallisuuden arviointilaitoksille 2020, 13-14.). Arviointitehtävästä perittävistä maksuista säädetään valtion maksuperustelaissa (150/1992) ja Liikenne- ja viestintäministeriön asetuksessa Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista (1453/2019). Arvioinnin toimeksiantajalla on ennen tilaamista ja toimeksiantosopimuksen laatimista oikeus saada arvio arvioinnista muodostuvista kustannuksista (Ohje tietoturvallisuuden arviointilaitoksille 2020, 13-14.).

Tietoturvallisuuden arvioinnin toteutusta arviointikohteessa määrittelee TRAFICOMin ohje tietoturvallisuuden arviointilaitoksille ja siinä eritellyt seikat arvioinnissa käytettävistä todentamismenetelmistä. Arvioinnissa vaatimusten täyttymisen tilaa tarkastellaan vähintään TRAFICOMin ohjeistamien ja sille tietoturvallisuuden arviointilaitoksen hyväksynnän yhteydessä vaatimuskohdittain esitettyjen todentamismenetelmien mukaisesti. Todentamismenetelmät koostuvat paikan päällä organisaation toimitiloissa tehtävistä ja etäältä tietoverkon yli suoritettavista tarkastustoimista. (Ohje tietoturvallisuuden arviointilaitoksille 2020, 18-23.)

Tietoturvallisuuden arvioinnista ja sen yhteydessä suoritetuista tarkastuksista on määrätty laadittavaksi arviointiraportti. Arviointiraportissa edellytetään noudatettavan standardien ISO/IEC 17021 ja ISO/IEC 27006 vaatimuksia. Arviointiraporttiin on VAHTI- ja KATAKRI-arvioinneissa liitettävä mukaan vaatimustaulukko arviointituloksi-

neen ja perusteluineen. Perusteluista on käytävä ilmi kunkin vaatimuskohdan arviointiin vaikuttaneet seikat. Arviointia koskevia keskeisiä arviointituloksia edellytetään säilytettävän kuusi vuotta arviointitapahtuman päättymisestä arviointitulosten jälkikäteistä todentamista varten. (Ohje tietoturvallisuuden arviointilaitoksille 2020, 16.)

3.3.5 Arviointitoiminta

Valtionhallinnon viranomaisten tietoturvallisuuden arviointeja sääntelee laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuuden arvioinneista (1406/2011). Laki määrittelee TRAFICOMin tehtäväksi arvioida viranomaisen pyynnöstä tämän määräämisvallassa olevien tai hankittavaksi suunnittelemien tietojärjestelmien ja tietoliikennejärjestelyiden vaatimustenmukaisuutta, ja antaa vaatimusten täyttämisen hyväksymistä koskeva todistus. TRAFICOMin on lisäksi valtiovarainministeriön pyynnöstä selvitettävä valtionhallinnon viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden yleistä tietoturvallisuuden tasoa. (L 1406/2011, 4-5§.)

TRAFICOM suorittaa tietoturvallisuuden arviointeja käytettävissään olevien voimavarojen mukaisesti kansainväliset tietoturvallisuusvelvoitteet sekä pyydettyjen toimenpiteiden merkitys huomioon ottaen. Valtionhallinnon viranomainen voi TRAFICOMin sijasta käyttää tietoturvallisuuden arviointien toteutukseen TRAFICOMin hyväksynnän saanutta tietoturvallisuuden arviointilaitosta. Tietoturvallisuuden arviointilaitoksen hyväksymismenettelystä ja tehtävistä säädetään laissa tietoturvallisuuden arviointilaitoksista (1405/2011). (L 1406/2011, 3-4§.)

Tietoturvallisuuden arviointilaitokseksi hakeutuvan organisaation edellytetään tehtävässä toimiakseen täyttävän tietoturvallisuuden arviointilaitokselta vaadittavat ennakkoehdot. Tehtävään voidaan hyväksyä vain organisaatio, joka on toiminnallisesti ja taloudellisesti riippumaton arvioinnin kohteesta, ja jonka henkilökunnalla on hyvä koulutus ja kokemus toimintaan kuuluvista tehtävistä, ja joka omaa tehtävässä tarvittavat laitteet, välineet ja järjestelmät. Lisäksi organisaation edellytetään täyttävän vastuuhenkilöiden luotettavuudelle ja tietojenkäsittelyn turvallisuudelle asetetut ehdot. (L 1405/2011, 2:5§; Ohje tietoturvallisuuden arviointilaitoksille 2020, 6-8.)

Hyväksyntää tietoturvallisuuden arviointilaitokseksi haetaan pätevyysalueittain erikseen jokaista tietoturvallisuuden arviointiperustetta vasten. Arviointilaitokseksi hyväksytyksi tullakseen organisaation on haettava aina ensin pätevyyttä ISO/IEC 27001 standardin mukaisia arviointeja varten. Pätevyyttä haetaan Suomen kansalliselta akkreditointielimeltä FINAS, Finnish Accreditation Service, siten kuin laissa vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta (920/2005) säädetään. Pätevyyden toteamisen jälkeen organisaatio on vielä hyväksyttävä TRAFICOMin toimesta tietoturvallisuuden arviointilaitoksen tehtävien aloittamiseksi. (Ohje tietoturvallisuuden arviointilaitoksille 2020, 6-10.)

TRAFICOMin hyväksyntää tietoturvallisuuden arviointilaitokseksi haetaan vapaamuotoisella hakemuksella, johon on liitettävä kaikki asian käsittelyä varten tarpeelliset tiedot. Hakemuksen liitteenä toimitettavista tarvittavista tiedoista ohjeistetaan TRAFICOMin ohjeessa tietoturvallisuuden arviointilaitoksille. Ohje kuvaa TRAFICOMin toimia organisaation vastuuhenkilöiden luotettavuuden ja tietojenkäsittelyn turvallisuuden selvittämiseksi. Tietojenkäsittelyn turvallisuutta koskevat vaatimukset todennetaan kulloinkin voimassa olevan KATAKRI version perusteella. (Ohje tietoturvallisuuden arviointilaitoksille 2020, 6-10.)

4 Toiminnallinen viitekehys

4.1 Arviointikriteerit

Kyberturvallisuuden arviointitoimintaa suunniteltaessa alun perin kysymysmuotoon puetuista sertifiointivaatimuksista johdettiin opinnäytetyön laadinnan yhteydessä kirjalliset arviointikriteerit. Arviointikriteereillä kuvataan niitä yksityiskohtaisia ehtoja ja tavoitteita, joita vasten sertifiointikohteessa kyberuhkien varalle käyttöön otettuja tietoturvakontrolleja verrataan. Arviointikriteerien ja organisaation toteuttamien tietoturvakontrollien välisellä vertailulla pyritään joko toteamaan organisaation kyberturvallisuustason vaatimustenmukaisuus tai tunnistamaan vaatimuspoikkeamat.

Arviointikriteerit laadittiin sertifiointivaatimusten osalta jokaiselle sertifioinnin lopputuloksen kannalta merkitykselliselle kysymyskohdalle erikseen. Merkityksselliseksi katsottiin kysymyskohdat, joilla oli sertifiointikriteeristössä määritelty olevan vaikutusta sertifioinnin pisteytykseen. Vastausten pisteytyksen osalta merkityksettömät kysymyskohdat jätettiin määrittelyn ulkopuolelle varsinaiseen sertifiointipäätökseen vaikuttamattomina seikkoina. Arviointikriteerien määrittelytyötä tehtiin auktorisoitujen arviointilaitosten työskentelyn tukena käytettävään sertifiointikriteeristöön (Liite 1).

Vertailukohtaa määrittelytyön toteutukseen haettiin FINCSC-sertifiointijärjestelmän kehitystyön taustalla käytetyistä kansallisista ja kansainvälisistä tietoturvallisuuden arviointimalleista. Cyber Essentials –sertifiointijärjestelmä käsittelee kybertoimintaympäristön suojaksi toteutettujen tietoturvakontrollien todentamisvaatimuksia antamassaan erillisohjeessa (Cyber Essentials Plus: Illustrative Test Specification 2020). Valtionhallinnon tietoturvallisuuden arvioinneissa käytettävät arviointimallit sisältävät pääosin itsessään kybertoimintaympäristön suojaamiselle asetettavat vaatimukset (ks. Ohje tietoturvallisuuden arviointilaitoksille 2020).

Arviointikriteerit on määrittelyn päätteeksi koostettu kyberturvallisuuden osatekijöittäin laadittuihin tarkistuslistoihin (Liite 2). Tarkistuslistojen jaottelussa käytetyillä osatekijöillä tarkoitetaan kyberturvallisuuteen vaikuttavia toiminnallisia, hallinnollisia, fyysisiä ja teknisiä tekijöitä. Kyseinen jaottelumalli on omaksuttu käyttöön FINCSC-sertifiointijärjestelmän osalta jo aiemmin käytössä olleesta lähestymistavasta. Lähestymistapa viestii FINCSC-sertifiointijärjestelmän osalta käytetystä sertifiointivaatimusten rakenteen selkeyttämiseen tähtäävästä viestintälinjan muutoksesta.

4.2 Arviointimenetelmät

Kyberturvallisuuden arviointitoiminnan suunnittelua jatkettiin arviointikriteerien ja toteutettujen tietoturvakontrollien välisen vertailun suorittamiseksi käytettävien arviointimenetelmien määrittelyllä. Arviointimenetelmillä viitataan yleisiin toimintatapoihin arvioida ja todentaa sertifiointivaatimusten täyttymistä sertifioinnin kohteena

olevan organisaation kybertoimintaympäristössä. Arviointimenetelmien jaottelu testaukseen, tarkastukseen ja haastatteluun pohjaa Yhdysvaltain kauppaministeriön alaisen viraston antamaan tekniseen ohjeistukseen tietoturvatestauksen ja –arvioinnin toteutuksesta (Cody, Orebaugh, Scarfone & Souppaya 2008, 2-1).

Arviointimenetelmiin kuuluvalla testauksella tarkoitetaan prosessia, jolla verrataan yhden tai useamman arviointikohteen todellista ja odotettua toimintaa tietyissä olosuhteissa. Tarkastaminen tarkoittaa puolestaan yhden tai useamman arviointikohteen katselmointia, havainnointia tai tutkimista niiden asianmukaisuuden selvittämiseksi. Haastattelulla viitataan organisaation henkilöstön jäsenten kanssa yksitellen tai ryhmässä käytäviin vallitsevaa asiantilaa selventäviin ja täydentäviin keskusteluihin. (Cody ym. 2008, 2-1).

Arviointimenetelmät määriteltiin arviointikriteerien tapaan jokaiselle sertifioinnin lopputuloksen kannalta merkitykselliselle kysymyskohdalle erikseen. Merkityksellisiksi katsottiin jälleen ne kysymyskohdat, joilla oli määritelty olevan vaikutusta sertifioinnin pisteytykseen. Vastausten pisteytyksen osalta merkityksettömät kysymyskohdat jätettiin määrittelyn ulkopuolelle varsinaiseen sertifiointipäätökseen vaikuttamattomina seikkoina. Arviointimenetelmien määrittelytyötä tehtiin auktorisoitujen arviointilaitosten työskentelyn tukena käytettävään sertifiointikriteeristöön (Liite 1).

Arviointimenetelmien määrittelytyötä ohjasi työn toimeksiantajan toimesta entuudestaan tehdyt valinnat. Työn toimeksiantaja oli menneen kehitystoiminnan kautta päätynyt käyttämään edellä mainittuja arviointimenetelmiä erottuen vertailukohteena käytetystä tekniseen testaamiseen ja tarkastamiseen keskittyvästä Cyber Essentials –sertifiointijärjestelmästä (vrt. Cyber Essentials Plus: Illustrative Test Specification 2020). Omaksuttu malli mukailee suurelta osin valtionhallinnon tietoturvallisuuden arvioinneissa käytettävää lähestymistapaa henkilöhaastatteluista, dokumentaation katselmoinnista, teknisestä testauksesta ja fyysisestä tarkastamisesta (Ohje tietoturvallisuuden arviointilaitoksille 2020, 20-23.)

4.3 Arviointitekniikat

Kyberturvallisuuden arviointitoiminnan suunnittelua täydennettiin arviointimenetelmiin liittyvien arviointitekniikoiden kuvaamisella. Arviointitekniikoilla tarkoitetaan niitä käytännön keinoja, joilla arviointimenetelmiin kuuluvaa testaus- ja tarkastustoimintaa voidaan toteuttaa todellisen ja odotetun toiminnan vertaamiseksi tai arviointikohteen asianmukaisuuden selvittämiseksi. Organisaation kyberturvallisuustason tarkastelussa käytettävät arviointitekniikat jaoteltiin Yhdysvaltain kauppaministeriön alaisen viraston antaman teknisen ohjeistuksen määritelmien mukaisesti aktiivisiin ja passiivisiin arviointitekniikoihin. (Cody ym. 2008, 3-1–5-7.)

Aktiivisilla arviointitekniikoilla tarkoitetaan keinoja, joilla vaikutetaan tarkasteltavan arviointikohteen toimintaan vastareaktion aikaansaamiseksi. Passiiviset arviointitekniikat tutkivat arviointikohdetta ilman vastareaktioon toimintansa perustavia arviointitoimia. (Cody ym. 2008, 3-1–5-7.) Käytettävien arviointitekniikoiden valintaa ohjasi sertifiointivaatimuksittain määritetyt arviointikriteerit organisaation kybertoimintaympäristön suojaamiseksi edellytetyistä tietoturvakontrolleista.

Aktiivisia arviointitekniikoita käytetään hyväksi arviointikohteen tunnistamisessa ja analysoinnissa. Tekniikoilla testataan arviointikohdetta sen todellisen ja odotetun toiminnan vertaamiseksi. Testaaminen käsittää arviointialueeseen kuuluvien viestintäverkkojen skannaamisen laitteiden ja niihin liittyvien avoimien tietoliikenneporttien ja -palveluiden varalta. Tunnistettuja laitteita analysoidaan haavoittuvuus- ja murtotestein mahdollisten tietoturva-aukkojen löytämiseksi ja validoimiseksi.

Passiivisilla arviointitekniikoilla tuetaan aktiivisten arviointitekniikoiden käyttöä sekä tarkastetaan arviointialueeseen kuuluvien yksittäisten tietoturvakontrollien asianmukaisuutta. Tarkastaminen käsittää vastausten yhteydessä esitettyyn auditointinäyttöön perehtymisen. Tarkastamisessa käydään lävitse arviointialueeseen kuuluvia laite- ja tietojärjestelmäasetuksia sekä käytöstä kerättyjä lokitietoja. Tarkastuksissa varmennutaan lisäksi tilaturvallisuusratkaisuiden olemassa olosta.

Arviointilaitokset valitsevat vapaasti arviointitekniikoiden toteuttamiseksi käytettävät arviointivälineet. Arviointilaitosten on arviointitekniikoiden ja –välineiden käyttöä suunnitellessaan oltava yhteydessä sertifioinnin kohteena olevaan organisaatioon arviointitoiminnassa tarvittavien arviointijärjestelyiden sopimiseksi. Arviointilaitoksella on oltava vapaa tai rajoitettu käyttö- ja kulkuoikeus kaikkiin arviointitoiminnan kannalta välttämättömiin arviointikohteisiin.

4.4 Arviointitulokset

Organisaation kyberturvallisuustason tarkastelun yhteydessä saadut arviointitulokset ja tehdyt arviointitoimet määriteltiin taltioitavaksi sertifioinnin suoritusalustana käytettävään verkkoportaaliin. Verkkoportaaliin tehtävät kirjaukset laaditaan arviointimerkinnöille varattuihin vapaisiin tekstikenttiin. Tekstikenttiin tehtävät merkinnät tallentuvat arviointitoiminnan päätteeksi sertifioinnin kohteena olevalle organisaatiolle ladattavaksi saatettavaan arviointiraporttiin. Arviointiraportti on ladattavissa verkkoportaalista käyttäjätilin voimassaoloajan.

Arviointiraportin tarkoituksena on yhdessä organisaatiolle myönnettävän sertifikaatin kanssa toimia paitsi näyttönä sertifioinnin suorituksesta myös palvella sellaisenaan kyberturvallisuuden kehitystyön suunnittelussa. Arviointiraportti koostaa yhteen tietyllä arviointihetkellä vallinneen kybertoimintaympäristön tilan ja organisaation tavan suhtautua turvallisuuteen. Arviointiraporttia voidaan hyödyntää organisaation sidosryhmäsuhteissa vastattaessa sopimusten tietoturvavaatimuksiin.

Arviointiraporttiin tehtävissä merkinnöissä arviointilaitokset ottavat kantaa sekä yksittäisten vaatimuskohtien pisteytykseen että pisteytysten antamisperusteisiin. Pisteytysperusteissa arviointilaitos kuvaa arviointitulokseen johtaneita arviointitoimia ja arviointikohdetta mahdollisesti koskevia epäkohtia. Poikkeaman tuottavissa vaatimuskohdissa arviointilaitoksen tehtävänä on nostaa esille poikkeaman korjaamiseksi suoritettavia parhaita käytänteitä ja ohjata oikean tiedon lähteille.

Arviointiraportin laadinnan taustalla käytettyä keskeistä arviointiaineistoa säilytetään arviointilaitoksen hallussa kuusi vuotta arviointitapahtuman päättymisestä. Arviointiaineiston säilytyksellä mahdollistetaan arviointitoimien jälkikäteinen todentaminen. Arviointiaineiston säilytyksessä noudatetaan erityistä huolellisuutta ja turvallisuutta koko tiedon elinkaaren ajan. Säilytysajan umpeuduttua arviointiaineisto hävitetään tietoturvallisesti asiaankuuluvia menettelyitä noudattaen.

5 Opinnäytetyön tuotokset

Opinnäytetyön tuotoksena laadittiin kyberturvallisuuden arviointiohje FINCSC ja FINCSC PLUS -sertifiointien vaatimustenmukaisuuden arviointiin (Liite 3) ja tätä täydentävät tietoturvakontrollien tarkistuslistat (Liite 2). Ohjeen tarkoituksena on yhdessä tarkistuslistojen kanssa tarjota tietoa sertifiointikriteerien täyttymisen todentamiseksi käytettävistä arviointimenetelmistä ja arviointitoimintaa ohjaavista yleisistä periaatteista. Tuotoksissa kyberturvallisuuden arviointitoimintaa lähestytään arvioinnin toteuttajan näkökulmasta huomioiden toimintaan liittyvät arviointijärjestelyt.

Tuotokset on tarkoitettu kyberturvallisuuden arviointitoimintaa harjoittavien auktorisoitujen arviointilaitosten ja heidän lukuunsa arviointitehtäviä suorittavien turvallisuustarkastajien käyttöön. Tuotosten käytöstä on määrä hyötyä lisäksi sertifiointeihin valmistautuvat organisaatiot ja heitä tässä työssä konsultoivat tahot. Tuotoksiin perehtymistä suositellaan kaikille sertifiointeihin osallistuville ennen arviointitoiminnan käynnistymistä. Tuotos on suunniteltu julkaistavan myöhemmin avoimena verkkoversiona tai jaettavan sertifiointiin osallistuville.

Tuotokset koostuvat kyberturvallisuuden arviointitoimintaa käsittelevistä tekstisisällöistä ja sisältöjen visualisointia koskevista suunnitelmista. Tuotokset edellyttävät ennen niiden julkaisua teosten taittoa toimituksellisen tekstisisällön ja visuaalisten elementtien sommittelemiseksi. Tuotosten graafinen suunnittelu ja taitto on alun alkujaan rajattu opinnäytetyön ulkopuolelle työhön kuulumattomana osana. Työn toimeksiantaja on pidättänyt itsellään oikeuden ja vastuun ohjeen julkaisuun sekä julkaisua edeltäviin mahdollisiin sisällöllisiin muutoksiin ja päivityksiin.

Tuotosten laadintaa ohjaavana tavoitteena on ollut pyrkiä tekstin selkokielisyyteen ja visuaalisuuteen siten, että ne avautuisivat eri käyttäjäryhmille. Käyttäjäryhmien osalta arviointilaitoksilla ja heidän lukuunsa toimivilla tarkastajilla on jo heiltä pätevyyden todentamiseksi edellytettyjen auktorisointivaatimusten kautta katsottu olevan kiitettävät valmiudet tuotosten sisällön omaksumiseen ja ymmärryksen rakentamiseen. Sertifiointiin hakeutuvissa organisaatioissa valmiudet tekstin sisäistämiseen on ennakoitu vaihteleviksi. Tuotokset pyrkivät puhuttelemaan myös niitä organisaatioita, joille kyberturvallisuus käsitteenä ja aihealueena on vieras.

6 Pohdinta

Tämän toiminnallisen opinnäytetyön tarkoituksena oli jatkaa kansallisen kyberturvallisuusstrategian toisen toimeenpano-ohjelman toimenpiteisiin kuuluvan FINCSC-sertifiointijärjestelmän edelleen kehittämistä. Kehittämistehtävällä pyrittiin järkeistämään olemassa olevia sertifiointipalveluita tekemällä FINCSC ja FINCSC PLUS –sertifioinneissa noudatettavista arviointimenettelyistä nykyistä ymmärrettävämpiä. Arviointimenettelyitä oli tavoite täsmentää auktorisoitujen arviointilaitoksen palveluiden aikaisilta toimilta asiakkaan kyberturvallisuustason selvittämiseksi.

Opinnäytetyössä vastattiin työn toimeksiantajan työlle ennalta asettamaan tavoitteeseen auktorisoitujen arviointilaitosten käyttöön tuotettavasta kyberturvallisuuden arviointiohjeesta ja tätä täydentävistä tarkistuslistoista. Arviointiohjeessa kuvataan niitä menettelytapoja, joilla asiakkaan kybertoimintaympäristön suojaamiseksi toteutettujen tietoturvakontrollien riittävyyttä ja tarkoituksenmukaisuutta on määrä arvioida ja todentaa. Kyberturvallisuuden arviointiohje on syntynyt opinnäytetyön lähestymistavaksi valikoitujen kehittämis- ja analyysimenetelmien käytön tuloksena.

Opinnäytetyön kehittämismenetelminä hyödynnettiin vertaisoppimista ja kehittämällä oppimista kerätyn tietoaineiston käsittelyn mukaillessa laadullista sisällön analyysiä. Kehittämismenetelmät paremmin huomioidakseen opinnäytetyössä oli alun perin tarkoituksena toteuttaa opinnäytetyön tuotoksena syntyneen kyberturvallisuu-

den arviointiohjeen validointi hyödyntäen työn toimeksiantajan kyberturvallisuuslaboratorioon rakennettua kuvitteellista asiakasorganisaatiota. Ajallisista syistä johtuen kyberturvallisuuden arviointiohjeen testauksesta jouduttiin luopumaan.

Opinnäytetyön perusteella tuotettua kyberturvallisuuden arviointiohjetta suositellaan testattavaksi käytännössä tulevien opinnäytetöiden tai kehittämistehtävien yhteydessä. Muina kehittämiskohteina opinnäytetyöprosessin aikana nousi esiin FINCSC-sertifiointikriteerien ristiin vertailu opinnäytetyön vertailukohteina käytettyihin tieto- ja kyberturvallisuuden arviointimalleihin. Lisäksi opinnäytetyöprosessi herätti kehitysajatuksen sertifiointivaatimusten pisteytysperusteiden tarkastelusta tutkittuun uhkatietoon ja uhkamalleihin pohjautuen. Arviointitoiminnan tehostamiseksi sertifiointijärjestelmän käyttöön olisi edullista määritellä arviointivälinekohtaiset testausparametrit sisältävät tarkistuslistat.

Opinnäytetyön aikana toimintaympäristössä ennätti tapahtumaan useita muutoksia sekä kansallisella että Euroopan unionin tasolla, joiden vaikutusten tutkiminen voi tarjota jatkoaiheita tulevalle tutkimus- ja kehitystyölle. Suomessa muun muassa hyväksyttiin 3.päivänä lokakuuta vuonna 2019 käyttöön uusi Suomen kyberturvallisuusstrategia (Suomen kyberturvallisuusstrategia 2019). Ennen strategian hyväksyntää eduskunta oli antanut päätöksen laista julkisen hallinnon tiedonhallinnasta (906/2019), jonka myötä valtionhallinnon tietoturvallisuuden arviointeihin kohdistui muutospaineita. Lisäksi Euroopan parlamentti päätti 13.päivänä maaliskuuta vuonna 2019 Euroopan unionin laajuisen kyberturvallisuussertifioinnin säätämisestä osana kesäkuussa voimaan astunutta Euroopan unionin kyberturvallisuusasetusta (Atallah & Lottonen 2019).

Lähteet

A 1453/2019. Sähköisen viestinnän maksuasetus. Liikenne- ja viestintäministeriön asetus Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista. https://www.finlex.fi/fi/laki/alkup/2019/20191453

A 681/2010. Tietoturva-asetus. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. Annettu 1.7.2010. Viitattu 20.4.2020. https://www.finlex.fi/fi/laki/ajantasa/2010/20100681#L3P12

Apply for Cyber Essentials verified self assessment. 2020. IASME verkkosivustolla. Viitattu 20.4.2020. https://iasme.co.uk/cyber-essentials/cyber-essentials-apply-now/

Atallah, M. & Lottonen, J. 2019. Uusi EU:n kyberturvallisuusasetus astui voimaan kesäkuussa 2019. Julkaistu 20.8.2019. Uutinen Nordic Law verkkosivustolla. Viitattu 20.4.2020. https://nordiclaw.fi/uusi-eun-kyberturvallisuusasetus-astui-voimaan-kesakuussa-2019/

Authorization. 2020. FINCSC – Finnish Cyber Security Certificate verkkosivut. Viitattu 20.4.2020. https://www.fincsc.fi/

Become an assessor. 2020. IASME verkkosivustolla. Viitattu 20.4.2020. https://iasme.co.uk/become-an-assessor/

Cody, A., Orebaugh, A., Scarfone, K. & Souppaya, M. 2008. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Viitattu 20.4.2020. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Cyber Essentials. 2020. IASME verkkosivustolla. Viitattu 20.4.2020. https://iasme.co.uk/cyber-essentials/

Cyber Essentials Plus: Illustrative Test Specification. 2020. Versio 2. National Cyber Security Centre. Viitattu 20.4.2020. https://www.ncsc.gov.uk/files/Cyber-Essentials-Plus-Illustrative-Test-Specification-April-2020.pdf

Cyber Essentials – Self-Assessment Preparation Booklet. 2020. Versio 11b. IASME. Viitattu 20.4.2020. https://iasme.co.uk/wp-content/uploads/2020/03/Cyber-Essentials-only-question-booklet-v11b.pdf

FINCSC Booklet. 2018. Jyväskylä Security Technology. Viitattu 20.4.2020. https://www.fincsc.fi/wp-content/uploads/2018/10/FINCSC-booklet-web.pdf

FINCSC sertifiontivaatimukset. 2018. Päivitetty 8.3.2018. Jyväskylä Security Technology. Excel-dokumentti.

Frequently asked questions. 2020. IASME verkkosivustolla. Viitattu 20.4.2020. https://iasme.co.uk/frequently-asked-questions

Get a quote for Cyber Essentials Plus. 2020. IASME verkkosivustolla. Viitattu 20.4.2020. https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-get-a-quote/

Hankeraportti 2018. Euroopan aluekehitysrahasto (EAKR), Alueelliset innovaatiot ja kokeilut (AIKO), Keski-Suomen kehittämisrahasto. 2018. Julkaisu C 157. Keski-Suomen liitto. Viitattu 20.4.2020. https://www.keskisuomi.fi/filebank/25930-C_157.pdf

IASME Governance includes GDPR requirements & Cyber Essentials. 2020. IASME verkkosivustolla. Viitattu 20.4.2020. https://iasme.co.uk/iasme-governance/

Internet yrityksissä. 2019. Tietotekniikan käyttö yrityksissä. Tilastokeskuksen verkkojulkaisu. Viitattu 23.4.2020. http://www.stat.fi/til/icte/2019/icte_2019_2019-12-03_kat_002_fi.html

Internet yrityksissä. 2018. Tietotekniikan käyttö yrityksissä. Tilastokeskuksen verkkojulkaisu. Viitattu 23.4.2020. http://www.stat.fi/til/icte/2018/icte_2018_2018-11-30_kat_002_fi.html

Jyväskylän ammattikorkeakoulun tutkintosääntö. 2019. Pdf-dokumentti. Viitattu 20.4.2020. https://opinto-oppaat.jamk.fi/globalassets/opinto-opas-amk/jamk/tutkintosaanto/tutkintosaanto.pdf

Kansallinen turvallisuusauditointikriteeristö. 2009. Sisäisen turvallisuuden ohjelman toisen vaiheen toimenpide 6.4 tp 2. Puolustusministeriö. Viitattu 20.4.2020. https://www.defmin.fi/files/1525/Katakri.pdf

Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma. 2014. Annettu 11.3.2014. Turvallisuuskomitean julkaisu. Viitattu 20.4.2020. https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Kyberturvallisuusstrategian-toimeenpano-ohjelma.pdf

Kansallisen turvallisuusauditointikriteeristön (KATAKRI) neuvoa-antava työryhmä. 2012. Sisäasianministeriön hankesivu. Hankenumero SM042:00/2010. Viitattu 20.4.2020. https://intermin.fi/hankkeet/hankesivu?tunnus=SM042:00/2012

Katakri 2015. 2015. Tietoturvallisuuden auditointityökalu viranomaisille. Puolustusministeriö. Viitattu 20.4.2020. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Keski-Suomen liiton rahoitusraportti 2016. EU:n rakennerahastot, maakunnan kehittämisraha, Keski-Suomen kehittämisrahasto. 2016. Julkaisu C 152. Keski-Suomen liitto. Viitattu 20.4.2020. https://www.keskisuomi.fi/filebank/25434-C_152.pdf

Kyberturvallisuuden sanasto. 2018. Sanastokeskuksen julkaisu. Viitattu 20.4.2020. https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

L 150/1992. Valtion maksuperustelaki. Annettu 21.2.1992. Viim. muutos 7.8.2015. Viitattu 10.4.2020. https://www.finlex.fi/fi/laki/ajantasa/1992/19920150#mvs

L 588/2004. Laki kansainvälisistä tietoturvallisuusvelvoitteista. Annettu 24.5.2004. Viim. muutos 9.8.2019. Viitattu 20.4.2020. https://www.finlex.fi/fi/laki/ajantasa/2004/20040588#mvs

L 621/1999. Julkisuuslaki. Laki viranomaisten toiminnan julkisuudesta. Annettu 21.5.1999. Viim. muutos 8.8.2019. Viitattu 20.4.2020. https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

L 726/2014. Turvallisuusselvityslaki. Annettu 19.9.2014. Viim. muutos 9.8.2019. Viitattu 20.4.2020. https://www.finlex.fi/fi/laki/ajantasa/2014/20140726#mvs

L 906/2019. Laki julkisen hallinnon tiedonhallinnasta. Annettu 9.8.2019. Viitattu 20.4.2020. https://www.finlex.fi/fi/laki/ajantasa/2019/20190906

L 1405/2011. Laki tietoturvallisuuden arviointilaitoksista. Annettu 22.11.2011. Viim. muutos 19.9.2017. Viitattu 20.4.2020. https://www.finlex.fi/fi/laki/ajantasa/2011/20111405#L2P3

L 1406/2011. Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. Annettu 22.12.2011. Viim. muutos 19.9.2014. Viitattu 20.4.2020. https://finlex.fi/fi/laki/ajantasa/2011/20111406#P4

LbD eli kehittämispohjainen oppiminen. 2020. Laurea-ammattikorkeakoulu. Viitattu 20.4.2020. https://www.laurea.fi/koulutus/pedagogisia-innovaatioita/lbd/

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. ja Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017.. Viitattu 20.4.2020. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kyberturvallisuuden_nykytila%2C__tavoitetila_ja.pdf

Loppuraportti: Cyber Scheme Finland –pilotti 1.9.2015 – 30.11.2016. 2016. Pdf-dokumentti. Jyväskylän ammattikorkeakoulu.

Loppuraportti: FINCSC PLUS 1.11.2016 – 31.8.2018. 2018. Pdf-dokumentti. Jyväskylän ammattikorkeakoulu.

Luottamuksen lähteillä. 2019. Näkökulmia tietoturvan standardointiin ja sertifiointiin. 31/2019. Liikenne- ja viestintävirasto TRAFICOM. Viitattu 20.4.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

Mäkelä, M., Salonen, M ja Salonen, N. 2016. Vertaansa vailla – vertaiskehittämisen käsikirja. Viitattu 20.4.2020. http://www.lapaisy.fi/wp-content/uploads/2016/12/vertaansa_vailla_web.pdf

New look scheme protects businesses from cyber attack. 2020. National Cyber Security Centre tiedote. Viitattu 20.4.2020. https://www.ncsc.gov.uk/news/new-look-scheme-protects-businesses-from-cyber-attack

New scheme to help businesses defend against cyber threats goes live. 2014. Press release. Julkaistu 5.6.2014. Department for Business, Innovation & Skills ja The Rt Hon David Willetts. Viitattu 20.4.2020. https://www.gov.uk/government/news/new-scheme-to-help-businesses-defend-against-cyber-threats-goes-live--2

Ohje tietoturvallisuuden arviointilaitoksille. 2020. Julkaisu 120/2016 O. Annettu 7.5.2013. Viim. muutos 28.1.2020. Liikenne- ja viestintävirasto TRAFICOM. Viitattu 20.4.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Arviointilaitosohje_v_8_1.pdf

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. 2010. VAHTI 2/2010. Valtiovarainministeriön julkaisu. Viitattu 20.4.2020. https://www.vahtiohje.fi/c/document_library/get_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229

Opinnäytetyön arviointikriteerit ammattikorkeakoulututkinnoissa (EQF 6-taso). 2014. Jyväskylän ammattikorkeakoulu. Docx-dokumentti. Viitattu 20.4.2020. https://elmo.jamk.fi/

Pellinen, A. 2018. Pk-yritysten varautuminen kyberturvallisuusuhkien varalle – tutkimus nykytilasta pienyrityksissä. Opinnäytetyö, ylempi AMK. Jyväskylän ammattikorkeakoulu, tekniikan ja liikenteen ala, teknologiaosaamisen johtamisen tutkinto-ohjelma. Viitattu 20.4.2020. http://urn.fi/URN:NBN:fi:amk-2018061213613

Procurement Policy Note 09/14: Cyber Essentials Scheme. 2014. Julkaistu 26.9.2014. Viim. muutos 26.5.2016. Cabinet Office. Viitattu 20.4.2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/526200/ppn_update_cyber_essentials_0914.pdf

Seitamaa-Hakkarainen, P. 2014. Kvalitatiivinen sisällönanalyysi. Viitattu 20.4.2020. https://metodix.fi/2014/05/19/seitamaa-hakkarainen-kvalitatiivinen-sisallon-analyysi/

SFS-ISO/IEC 27001. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Aihealueet: Informaatioteknologia, turvallisuustekniikat. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 9.12.2013. Viitattu 7.6.2016. https://janet.finna.fi, SFS Online.

Sisäisen turvallisuuden ohjelman toimeenpano. 2010. Väliraportti 1/2010. Julkaistu 18.3.2010. Sisäasiainministeriön julkaisu. Viitattu 20.4.2020. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80023/sm_052010.pdf

Suomen kyberturvallisuusstrategia 2019. 2019. Valtioneuvoston periaatepäätös 3.10.2019. Turvallisuuskomitean julkaisu. Viitattu 20.4.2020. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Suomen kyberturvallisuusstrategia. 2013. Valtioneuvoston periaatepäätös 24.1.2013. Turvallisuuskomitean julkaisu. Viitattu 20.4.2020. https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf

Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020. 2017. Annettu 20.4.2017. Turvallisuuskomitean julkaisu. Viitattu 20.4.2020. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

Suomen kyberturvallisuusstrategia valmis. 2013. Puolustusministeriön tiedote 24.1.2013. Viitattu 20.4.2020. https://www.defmin.fi/ajankohtaista/tiedotteet/2013/suomen_kyberturvallisuusstrategia_valmis.5368.news

The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. 2011. Cabinet Office. Viitattu 20.4.2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Turvallinen elämä jokaiselle. 2008. Sisäisen turvallisuuden ohjelma. Julkaistu 8.5.2008. Sisäasiainministeriö. Pdf-dokumentti.

Yhteiskunnan turvallisuusstrategia. 2010. Valtioneuvoston periaatepäätös 16.12.2010. Puolustusministeriön julkaisu. Viitattu 20.4.2020. https://www.defmin.fi/files/1696/Yhteiskunnan_turvallisuusstrategia_2010.pdf

2010 to 2015 government policy: cyber security. 2015. Policy paper. Päivitetty 8.5.2015. Cabinet Office. Viitattu 20.4.2020. https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security

2014 information security breaches survey: technical survey. 2014. Department for Business, Innovation & Skills ja The Shareholder Executive. Viitattu 20.4.2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/307296/bis-14-767-information-security-breaches-survey-2014-technical-report-revision1.pdf

Liitteet

Liite 1. FINCSC sertifiointikriteeristö

Liite 2. Tietoturvakontrollien tarkistuslistat

Liite 3. Kyberturvallisuuden arviointiohje