Tiina Virta

ISO 27001 -STANDARDIIN PERUSTUVA TIETOTURVA-JOHTAMISEN HALLINTAMALLI THL:LLE

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Virta, Tiina
ISO 27001 -standardiin perustuva tietoturvajohtamisen hallintamalli THL:lle
Jyväskylä: Jyväskylän yliopisto, 2020, 116 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

ISMS eli tietoturvan hallintamalli on joukko prosesseja ja politiikkoja, joiden tarkoituksena on ohjata ja hallinnoida organisaation arkaluontoista dataa. Se vähentää riskejä ja turvaa jatkuvuudenhallintaa ja sillä hallinnoidaan käytössä olevia prosesseja, dataa ja teknologioita. Hallintamallin tulee olla yhteensopiva voimassa olevien lakien ja asetusten kanssa. Terveyden ja hyvinvoinnin laitos (THL) suunnittelee ISO 27001 -sertifikaatin hankkimista tulevaisuudessa. Tutkimuksen tehtävänä oli kartoittaa, millainen hallintamalli THL:n tulisi ottaa käyttöön, jotta ISO 27001 -standardin vaatimukset täyttyvät sekä miten organisaation tietoturvavastuut tulisi jakaa.

Tutkimuksessa tarkasteltiin ensin tietoturvan hallintamalleja ja standardeja yleisellä tasolla. Sitten käytiin tarkasti läpi ISO 27001 -standardi ja THL:n nykytila. Työssä oli haasteena juuri samaan aikaan meneillään oleva THL:n organisaatio- ja johtamisuudistus, mutta tutkimus perustettiin johonkin tiettynä ajankohtana olevaan hetkeen ja tehtiin sen verran väljästi, että sitä on helppo muokata muutosten jälkeen.

Lopputuloksena syntyi standardin vaatimusten mukainen Excel-taulukko, joka auttaa sertifikaatin hankkimisen alkaessa työkaluna. Työkalu sisältää kaikki standardin tietoturva- ja riskinhallintavaatimukset, ehdotukset organisaation vastuutahoiksi sekä ehdotetut asiakirjat, joilla voidaan todistaa vaatimuksenmukaisuus.

Asiasanat: ISO27001, tietoturvajohtaminen, hallintamalli, ISMS

ABSTRACT

Virta, Tiina
Information Security Management System for THL based on ISO 27001 standard
Jyväskylä: University of Jyväskylä, 2020, 116 pp.
Information Systems / Cyber Security, Master's Thesis
Supervisor: Lehto, Martti

An information security management system (ISMS), is a set of processes and policies designed to guide and manage an organization's sensitive data. It reduces risks, secures continuity management and manages existing processes, data and technologies. The governance model must be compatible with applicable laws and regulations. Finnish Institute for Health and Welfare (THL) is planning to obtain ISO 27001 certification in the future. The task of this study was to map out what kind of management model THL should implement in order to meet the requirements of the ISO 27001 standard and how the organisation's information security responsibilities should be divided.

At first, the study looked at different information security management models and existing security standards. The ISO 27001 standard and THL's present state were then carefully reviewed. The challenge was the ongoing organizational and management reform of THL, but the study was set up to a point in time and was done so loosely that it could be easily modified after the changes.

The result of the study was an Excel spreadsheet that meets the requirements of the standard, helping to get certification started, as a tool. The tool includes all the security and risk management requirements of the standard, proposals for the organisation's responsible parties, and proposed documents that can be used to prove compliance.

Keywords: ISO27001, Information Security Management System, ISMS, governance

KUVAT

ALKUSANAT

Tämä pro gradu -työ on tehty Jyväskylän yliopiston kyberturvallisuuden maisteriohjelman päättötyönä. Haluan lämpimästi kiittää työn tilaajana toiminutta Terveyden ja hyvinvoinnin laitosta (THL) ja aivan erityisesti työn toisena ohjaajana toiminutta THL:n tietoturvapäällikköä Andrei Laurénia, jonka kannustus ja tuki olivat tämän työn etenemisen kannalta aivan korvaamattomia. Andrei, opin sinulta paljon!

Haluan myös kiittää yliopistolla työn ohjaajana toiminutta kyberturvallisuuden työelämäprofessori Martti Lehtoa. Kiitos erinomaisesta opastuksesta ja joustamisesta yllättävissä tilanteissa.

Erityiskiitos ystävälleni Pia Leskiselle. Ilman kannustustasi loppuvaiheessa tämä työ olisi saattanut jäädä tekemättä.

Vantaalla 11.11.2020

Tiina Virta

SISÄLLYS

1 JOHDANTO

Kiistämätön tosiasia on, että maailma lepää tänään tietotekniikan varassa ja se on kaiken liiketoiminnan mahdollistaja, ei enää vain pienten erikoisalojen käytössä (Lehto & Neittaanmäki, 2014). Parhaiten sen merkityksen huomaa silloin, kun se pettää; kun internetiin pääsy estyy palveluntarjoajan palvelimen rikkouduttua, kun verkkokaupan palvelimelta varastetaan luottokorttinumeroita tai kun kaupungin kaikki tietokoneet saavat ruudulleen lunnasvaatimuksen tietojen palauttamisesta. Kaikkia uhkakuvia ei edes halua miettiä. Ilkka Remes kuvaa näitä kaikkein pelottavimpia uhkia kirjoissaan, jotka tuntuvat joskus liiankin todellisilta. Toivokaamme että ne jäävät kirjailijan mielikuvituksen tasolle. Sen sijaan lähes kaikkiin uhkiin pystyy ennalta varautumaan ja useimmilla yrityksillä onkin käytössä jonkinlainen varautumissuunnitelma ja -keinoja käytettävissään. Koska tieto on yrityksen tärkeintä omaisuutta, sen suojaamisen merkitys korostuu. Miten tieto järjestetään ja miten sen turvallisuutta valvotaan, on yksi avainkysymyksistä.

Terveyden ja hyvinvoinnin laitos (THL) on julkinen laitos, joka tutkii ja seuraa suomalaisväestön hyvinvointia ja terveyttä. Se huolehtii kaikkien kansalaisten terveyden turvasta, joten sen tiedot ovat meille kaikille henkilökohtaisesti tärkeitä, minkä lisäksi iso osa tiedoista on salassa pidettäviä jo lakienkin mukaan. THL:n tarkoituksena on hankkia ISO 27001 -tietoturvasertifikaatti tulevaisuudessa, mutta tällä hetkellä heidän hallintamallinsa ei vielä vastaa sitä. Siksi he ovat palkanneet tutkijan selvittämään tämänhetkisen tilanteen ja sen vertaamisen ISO 27001 -standardin mukaiseen hallintamalliin.

Julkisen hallinnon digitaalinen turvallisuus -nimisessä Valtiovarainministeriön (2020) julkaisussa valotetaan vuosien 2020–2023 linjauksia kyberturvallisuuden suhteen valtion laitoksissa. Sosiaali- ja terveysministeriön kohdalla muistutetaan sen alaisten laitosten käsittelemän tiedon ja niitä käsittelevien järjestelmien sertifioinnin tärkeydestä. THL onkin pyrkinyt varautumaan sertifiointiin jo etukäteen teettämällä tämän tutkimuksen. Tässä tutkimuksessa tutustutaan siis yleisesti kyberturvallisuuden johtamiseen, ISO 27001 -tietoturvasertifikaattiin ja luodaan niiden pohjalta Terveyden ja hyvinvoinnin laitokselle tietoturvajohtamisen hallintamalli (Lauren_a, 2020).

Tutkimus tehdään käyttäen kvalitatiivista eli laadullista menetelmää ja siinä käytetään tapaustutkimuksen lähestymisnäkökulmaa. Ensimmäisessä luvussa selvitetään tutkimuksen taustaa, tutkimusongelmaa ja rajausta. Toisessa luvussa perustellaan tutkimuksen tieteellinen lähestymistapa ja kolmas luku käsittelee tutkimuksen viitekehyksen eli ISO 27001 -standardin tarkemman tutkimisen, aikaisemmat tutkimukset ja niistä saadun tiedon sekä THL:n nykytilan tutkimisen. Empiirinen tutkimus ja tulokset käsitellään luvussa neljä ja tulosten analysointi ja pohdinta esitellään viimeisessä eli viidennessä luvussa.

1.1 Tutkimuksen taustaa

Suomi on päättänyt pääministeri Sanna Marinin hallitusohjelman mukaisesti tehostaa julkisen hallinnon strategiajohtamista sekä linjata digitaalisen toimintaympäristön strategista johtamista (Valtiovarainministeriö, 2020). Euroopan Komissio puolestaan listasi muutama vuosi sitten lehdistötiedotteessaan muutamia kyberturvallisuuteen liittyviä tunnuslukuja:

- 86 % eurooppalaisista uskoo riskin joutua kyberrikollisuuden uhriksi kasvavan koko ajan
- muun muassa kuljetus-, energia-, terveys- ja taloussektorit ja niiden ydintoiminnot ovat nykyään erittäin riippuvaisia tietotekniikasta ja verkoista
- vuonna 2016 maailmassa tapahtui yli 4 000 kiristyshaittaohjelmahyökkäystä päivässä
- joissain EU:n jäsenvaltioissa 50 % kaikista rikoksista on kyberrikoksia
- tietoturvaloukkaukset kaikilla aloilla kasvoivat 38 % vuonna 2015, mikä oli suurin vuosikasvu kahteentoista vuoteen
- 80 % eurooppalaisista yrityksistä koki ainakin yhden tietoturvaloukkauksen vuonna 2016
- yli 150 maata ja yli 230 000 internetiin kytkettyä elintärkeää järjestelmää kaikilta yhteiskunnan aloilta joutuivat kärsimään vakavia seurauksia kyberhyökkäyksien takia, mukana muun muassa sairaaloita ja ambulanssipalveluita. (Euroopan komissio, 2017.)

Erilaisilta kyberhyökkäyksiltä varautumiseen on useita keinoja aina nakkikioskin ”mitä tekisin sähkökatkon sattuessa” -ajatuksesta pienyrittäjän päässä suuryritysten mietittyihin, järjestelmällisiin ja dokumentoituihin keinoihin. Varautuminen käy kuitenkin koko ajan tärkeämmäksi, sillä maailma globalisoituu ja teknistyy kiihtyvällä vauhdilla. Siksi standardien tekijät ovat tarttuneet aiheeseen ja luoneet yleispätevän standardin ISO 27001, joka antaa puitteet tietoturvan järjestämiseksi yrityksessä sen koosta riippumatta. Yritys voi sertifioida oman tietoturvajohtamisen hallintamallinsa standardia vasten, jolloin se voi osoittaa asioiden olevan tietyssä kansainvälisesti ja yleisesti hyväksytyssä järjestyksessä.

Puhuttaessa viranomaistoiminnasta kyberturvallisuuden toimenpiteet korostuvat, sillä viranomaiset huolehtivat meidän kaikkien henkilökohtaisista

tiedoista ja yleisestä yhteiskunnan toimivuudesta. Siksi Suomessa viranomaiset on ohjeistettu tietoturvatoimenpiteisiin liittyen. Suomessa laki, joka säätää viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista, velvoittaa valtion virastoja ja laitoksia hyväksyttämään tietoturvajärjestelynsä Viestintäviraston säädösten mukaan. Useat lait ja asetukset ohjaavat viranomaistoimintaa myös kyberturvallisuuden suhteen ja sen tärkeimmät osa-alueet on kirjoitettu Suomen kyberturvallisuusstrategiaan, jonka tuorein versio on vuodelta 2019. Viestintävirasto on ainoa taho, joka voi antaa todistuksen siitä, että virasto tai laitos käyttää kansainväliset vaatimukset täyttävää järjestelmää. VAHTI-ohjeet ja esimerkiksi juuri ISO/IEC 27001 -standardi ovat usein käytettyjä viitekehyksiä julkishallinnon kyberturvallisuuden arvioinnissa. (Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista, 2011/1406; Pietikäinen, 2013; Pietikäinen, 2014.)

THL (Terveyden ja hyvinvoinnin laitos) on julkinen laitos, joka tutkii ja seuraa suomalaisväestön hyvinvointia ja terveyttä. Se myös kehittää toimenpiteitä terveyden edistämiseksi ja kerää tietoa, jonka avulla se raportoi ja ohjeistaa terveyteen ja hyvinvointiin liittyvissä asioissa ja näin auttaa sidosryhmiään päätöksenteossa. Sidosryhmiä voivat olla valtion, kuntien ja maakuntien päättäjät, sosiaali- ja terveydenhuolto, järjestöt, tutkijat ja kansalaiset. Kuten korona-aika on julkisuudessa selkeästi osoittanut, THL toimii myös valtion tasolla turvallisuusviranomaisten kanssa yhteistyössä. THL toimii sosiaali- ja terveysministeriön alaisuudessa itsenäisenä tutkimuslaitoksena. (THL_a, 2020.) Tämän tutkimuksen tarkoituksena on luoda yhtenäinen hallintamalli siitä, miten tietoturvaa johdetaan THL:n organisaation sisällä, mitkä ovat päävastuut, ja ehdotus siitä, miten hallintamalli sulautetaan olemassa olevaan organisaatioon tai miten sitä voisi muuttaa. Sitä ennen tulee selvittää nykyinen organisaatio ja sen rakenne ja vastuut.

1.1.1 Kyberturvallisuutta muuttuvassa maailmassa

ISACA (Information Systems Audit and Control Association) on kansainvälinen hallinnollisen johtamisen asiantuntijajärjestö, joka toimii yli 180 maassa ja palvelee yli 145.000 jäsentään järjestämällä koulutusta, resurssienjakoa, tukea, verkostoitumista ja muita etuja. Nykyään sen jäsenet toimivat mitä erilaisimmilla ammattinimikkeillä vakuutusalalla, hallinnollisissa tehtävissä sekä riski- ja tietoturvatehtävissä ympäri maailmaa. Järjestö julkaisee näihin aloihin liittyviä uusia tutkimuksia ja resursseja säännöllisesti. (ISACA_a, 2020.) ISACA:lta löytyy jo muutama julkaisu koskien kyberturvallisuuden tilaa maailmassa vuonna 2020, vaikkei vuosi ole vielä lopussa. Raportin mukaan lausunto maailman muuttumisesta dramaattisesti vuonna 2020 ei ole liioiteltua, koronapandemia lieveilmiöineen on pitänyt siitä huolen. Teknologia on tullut avuksi koronan selättämisessä, sillä ihmisten linnoittautuessa koteihinsa tekemään työtä, teknologia mahdollistaa kommunikaation ja yhteistyön organisaatioiden työntekijöiden välillä fyysisen yhteyden puuttuessa. Tietoturva-alalla on tavattu sanoa, että liike-elämä toimii teknologian avulla – nykyisin maailma ei enää pysty pyörimään täysillä

ilman teknologiaa, sillä se on globaali ratkaisu myös pandemiaan. Se on myös saanut tietoturva-alan ihmiset sopeutumaan nopeasti: he ovat nopeampia, joustavampia ja innovatiivisempia kuin ennen sekä uusien haasteiden että tuntemattoman edessä. Monet IT-organisaatiot kohtaavat taloudellista epävakautta ja pandemiasta johtuvaa pelkoa ja inhimillistä tragediaa hyödyntävät kyberrikolliset kehittävät uusia strategioita varastaakseen ja muuten häiritäkseen normaalia toimintaa. Kyberturvallisuus on muuttunut entistä tärkeämmäksi, jotta yhteiskunta ja liike-elämä voivat toimia edelleen tehokkaasti. (ISACA_b, 2020.) Eräs hyvä esimerkki tästä on THL:n oma Koronavilkku-sovellus, joka on koodattu avoimella lähdekoodilla melko nopeasti ja testattu useilla eri tahoilla; tätä kirjoittaessa sen on ladannut puhelimeensa jo yli kaksi miljoonaa suomalaista.

ISACA listaa useita uhkakuvia perustuen alkuvuoden 2020 tapahtumiin:

- Tietoturvahyökkäykset ovat kasvussa, vaikka kasvukäyrä onkin loivempi kuin viime vuosikymmenellä.
- Tietoturvan toteuttaminen on edelleen hajallaan IT-osastojen harteilla. Vaikka monissa organisaatioissa on erillinen DevOps-toimintamalli, johon on keskitetty ohjelmistokehityksen, testauksen ja ylläpidon IT-palvelutoiminnot, kyberturvallisuudesta vastaavat toiminnot ovat edelleen kyselyn mukaan alimiehitettyjä ja ne ovat usein vain yksi työtehtävä IT-osastolla.
- Kyberrikokset ovat edelleen huonosti raportoituja. 62 % alan ammattilaisista uskoo organisaatioiden jättävän kyberrikokset ilmoittamatta, jopa silloin kun niillä olisi lain mukainen ilmoitusvelvollisuus.
- Tietoturvahenkilöiden vähyys yrityksissä vaikuttaa yrityksen operatiivisiin toimintoihin. Alan ammattilaisista 62 % ilmoittaa olevansa liian vähällä henkilökunnalla ja tietoturvaa ei silloin pystytä tuottamaan täydellä teholla.
- Kiristyshaittaohjelmat palasivat suosituimmaksi rahaa tuottavaksi strategiaksi kryptovaluutan louhimisen pidettyä johtoasemaa viime vuonna. (ISACA_b, 2020.)

Viimeinen kohta näkyi surullisesti uutisissa syyskuussa. Ambulanssi oli viemässä saksalaisnaista sairaalaan, joka oli joutunut kiristyshaittaohjelman uhriksi ja järjestelmien toimimattomuuden takia nainen oli käännytetty toiseen sairaalaan. Hän kuoli ambulanssiin matkalla sinne. Tämä tapaus sai paljon huomiota maailmalla, sillä naisen sanotaan mahdollisesti olevan maailman ensimmäinen kyberhyökkäyksen suora kuolonuhri. (BBC, 2020.)

1.1.2 ISMS

Information Security Management System (ISMS) on joukko politiikkoja ja prosesseja, jotka systemaattisesti ohjaavat ja hallinnoivat organisaation arkaluontoista dataa. Sen tarkoituksena on vähentää riskejä ja varmistaa se, että organisaation jatkuvuudenhallinta on turvattu etukäteen estämällä esimerkiksi tietovuodot tai vähentämällä niiden vaikutuksia. Yleensä ISMS:llä hallinnoidaan

ihmisten käyttäytymistä, käytössä olevia prosesseja, dataa ja teknologioita. Se voi koskea ainoastaan tiettyä dataryhmää, kuten esimerkiksi asiakastietoja, tai se voi koskea kattavasti organisaation kaikkea dataa ja muodostua osaksi organisaation työskentelykulttuuria. ISMS on siis systemaattinen tapa lähestyä tietoturvaa ja se sisältää prosessit, teknologian ja ihmiset. Sen tehtävänä on suojata organisaation tietoa tehokkaan riskinhallinnan avulla. ISMS:n tulee olla yhteensopiva voimassa olevien lakien ja asetusten kanssa, myös esimerkiksi GDPR:n (General Data Protection Regulation), joka on EU:n tietosuojalaki. Tietoja tulisi suojata yleisen tietoturvallisuudessa käytetyn CIA-mallin mukaisesti, joka määritetään seuraavasti: C tarkoittaa luottamuksellisuutta (confidentiality), I tarkoittaa yhteneväisyyttä (integrity) ja A saatavuutta (availability). (TechTarget, 2011; Dutton, 2019.)

1.1.3 Tietoturvastandardeja

Maailman muuttuessa koko ajan digitaalisemmaksi ja reaaliaikaisemmaksi yritysten toiminta vaatii uusia keinoja luottamuksen varmistamiseksi toimijoiden välillä. Tähän pyritään erilaisilla standardeilla, joita käytetään toiminnan laadun ja turvallisuuden kehittämiseksi ja sen osoittamiseksi standardeihin nojautuvilla sertifikaateilla. Standardeja on monia erilaisia ja valinta niiden välillä joskus hankalaa. Hyvä standardi on kansainvälinen, joustava, läpinäkyvä, prosessiltaan avoin, ennustettava, sopiva kohteeseensa ja saatavilla. Standardin noudattamista valvotaan ensin sertifikaatin hankkimisella ja myöhemmin auditoinneilla, jotka varmistavat jatkuvuuden. Tietoturvavaatimusten sertifioinnit ovat kasvaneet hitaasti mutta selvästi. EU:n Kyberturvallisuusasetus, joka tuli voimaan vuonna 2019, tullee kasvattamaan standardien ja sertifikaattien kysyntää ja käyttöä Euroopassa. (Kyberturvallisuuskeskus_a, 2019.) Seuraavaksi käsitellään erilaisia tietoturvaan keskittyviä standardeja maailmassa.

ISO-standardeja on lähes viisikymmentä erilaista, mutta tässä mainitaan vain tunnetuimmat. ISO/IEC 15408 -standardi tunnetaan paremmin nimellä **Common Criteria** eli CC. Se on viitekehys sille, että tuote täyttää tietyt toiminnalliset ja laadulliset kriteerit tietoturvan suhteen. Sitä käytetään paljon tietoturvatuotteiden sertifioinnissa, esimerkiksi palomuurien, käyttöjärjestelmien ja älykorttien kohdalla. (Thales_a, 2020; Wikipedia_b, 2020.)

PCI DSS -standardi on maailman suurimpien luottokorttiyhtiöiden hallinnoima tietoturvastandardi liittyen korttimaksuihin. Se määrää muun muassa pankkien, korttimaksamista käyttävien kauppiaiden, korttimaksujen kuljettajien, korttiyhtiöiden ja korttien liikenteeseen laskijoiden tietoturvan kriteerit, joilla korttimaksaminen pidetään mahdollisimman turvallisena kaikille osapuolille.

ISO 27799:2016 on kansainvälinen standardi, jossa määritellään paras tapa terveysviranomaisille pitää jokaisen henkilökohtaiset terveystiedot turvassa järjestelmissä. Henkilökohtaisten terveystietojen säilyttämisen tulee täyttää tarpeeksi vahvat tietoturvakriteerit luottamuksellisuuden, muuttumattomuuden ja saatavuuden osalta. (Academic, 2020; Thales_b, 2020.)

Sarbanes-Oxley Act, lyhyemmin **SOX** on Yhdysvaltain liittovaltion laki, joka määrittää yritysten kirjanpidosta, tilintarkastuksista, yritysjohdon vastuista

ja sisäpiirikaupoista, monen muun asian lisäksi. Vaikka se on puhtaasti Yhdysvaltoja koskeva laki, sitä käytetään usein myös eurooppalaisissa yrityksissä, jos niillä on kytkentöjä Yhdysvaltoihin. Toki laki koskee ilman muuta yhdysvaltalaisten yritysten tytäryhtiöitä ympäri maailmaa. (Soxlaw, 2008.)

GDPR eli General Data Protection Regulation on Euroopan laajuinen tietosuoja-asetus, joka velvoittaa yritykset pitämään EU:n kansalaisia koskevat yksilöivät tiedot turvassa. Se laajensi voimaantullessaan myös kansalaistensa oikeuksia omiin tietoihinsa ja edellytti yritykset nimittämään tietosuojavastaavan, jos yrityksen toimintaan sisältyy arkaluonteisten tietojen laajamittaista käsittelyä, tai jos yritys on julkishallinnon toimija. Myös tietoturvaloukkausten raportoinnit säädettiin ilmoitettaviksi.

Maailmanlaajuiseen standardisointiin perustuva järjestelmä, johon ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) kuuluvat, on tuottanut yrityksille suunnatun kansainvälisen tietoturvastandardin **ISO 27001**. Se linjaa kansainvälisesti hyväksytyn metodin tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitämiseen ja jatkuvaan parantamiseen yksittäisessä organisaatiossa. Standardi ei anna yksityiskohtaisia ohjeita, vaan tavoitteena on ollut luoda kaikille yrityksille soveltuva yleisluontoinen ohje. Jos yritys todistaa noudattavansa tätä standardia, se voi hakea aiheeseen liittyvää sertifikaattia. (SFS, 2017.)

National Institute of Standards and Technology eli **NIST** on osa Yhdysvaltain kaupallista ministeriötä ja sen tehtävänä oli alun perin edistää USA:n teollista kilpailukykyä. Nykyään se kehittää kaikkeen materiaan liittyviä teknologioita, mittauksia ja standardeja. Vaikka NIST on saanut myös kritiikkiä yhteistyöstään Yhdysvaltain kansallisen turvallisuusviraston NSA:n kanssa, sen kyberturvallisuusviitekehys (NIST cybersecurity framework) on kuitenkin laajasti käytössä. (NIST, 2017; DigitalGuardian, 2020.

VAHTI eli Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä on elin, joka tähtää hallinnollisen tietoturvan kehittämiseen Suomessa ja jonka on nimittänyt Suomen valtiovarainministeriö. Sen tarkoituksena on edistää suomalaisten yritysten ja kansalaisten luottamusta tietoyhteiskuntaan. VAHTI-tietoturvaohjeet on luotu valtion- ja kunnallishallinnon käyttöön, mutta niitä käytetään myös elinkeinoelämässä. Ohjeet ovat dokumentteja, jotka perustuvat kansalliseen ja kansainvälisiin linjauksiin ja sääntöihin. Ne eivät ole itsessään lainsäädäntöä, vaan niiden tarkoitus on ohjeistaa ja tukea. Tästä huolimatta esimerkiksi VAHTI 2/2010 -ohje tulkitaan usein vaatimukseksi ja siksi se voidaan tässä yhteydessä tulkita standardiksi. Se myös perustuu suurelta osalta ISO 27001 -standardiin. VAHTI-ohjeistus jaetaan kahdeksaan osa-alueeseen:

- hallinnollinen turvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus

- käyttöturvallisuus.

VAHTI 100 -työnimellä kulkeva päivitystyö on käynnissä, sillä vuoden 2020 voimaan tullut tietohallintalaki laajentaa velvoittavuutta ja jatkossa se koskee valtionhallinnon lisäksi myös kuntia ja maakuntia. (Wikipedia_c, 2019; Suomidigi, 2020; Kyberturvallisuuskeskus_a, 2019; Lauren_b, 2020; Lauren_e, 2020; Helsingin yliopisto, 2003.)

KATAKRI (kansallinen turvallisuusauditointikriteeristö) on puolustusministeriön hyväksymä kriteeristö, jota vastaan julkishallinnon tietoturvajärjestelmiä arvioidaan. Sitä on tyypillisesti käytetty silloin, kun suomalainen yritys tai organisaatio käsittelee toisen maan salassa pidettävää tietoa. Se sisältää esimerkkejä toteutustavoista, mutta ne eivät ole sitovia, vaan tulkinnanvaraa on jätetty. KATAKRI jakaa auditointikriteerit kolmeen osa-alueeseen:

- turvallisuusjohtaminen
- fyysinen turvallisuus
- tekninen turvallisuus.

KATAKRI:a käyttämällä voidaan todentaa organisaation käyttämien tapojen ja menetelmien turvallisuutta. Esimerkiksi Puolustusvoimat vaatii kaikilta alihankkijoiltaan KATAKRI-auditoinnin hyväksyttyä läpikäyntiä. Turvallisuusauditointeja voivat tehdä vain erillisen turvallisuusauditoijan koulutuksen saaneet henkilöt. Koulutusta järjestetään Laurea ammattikorkeakoulussa ja se on 15 opintopisteen laajuinen. Koulutuksen hinta on tällä hetkellä 3.224 euroa ja seuraava toteutus järjestetään keväällä 2021. (Kyberturvallisuuskeskus_a, 2019; Puolustusministeriö, 2011; Laurea ammattikorkeakoulu, 2020.) Kyberturvallisuuskeskuksen laatima **PiTuKri** puolestaan on KATAKRI:n kaltainen auditointikriteeristö, mutta se keskittyy pilvipalveluihin ja on tarkoitettu työkaluksi arvioimaan pilvipalveluiden turvallisuutta (Traficom, 2019; Lauren_c, 2020).

1.1.4 Tietoturvan hallintamalleja

Tietoturvan tehokasta hallintaa on mietitty jo kauan ja erilaisia hallintamalleja on kehitetty toiminnon viitekehykseksi. Tietoturvaan keskittyvän hallintamallin tarkoituksena on kehittää tietoturvan ja riskien hallintaa, sillä tietoisuus lisääntyy ja riskit pienenevät sen avulla. Kun tietoturvavaatimukset ovat aktiivisesti mukana uusien teknologien hankinnassa, riskit pienenevät edelleen. Tietoturvan tasoa on myös tarkoitus koko ajan parantaa, sillä tunnetusti tietoturva ei ole stabiili, vaan itseään parantava prosessi. Tietoa pitää suojata mahdollisimman tehokkaasti mahdollisimman pienin resurssein ja tässä hallintamalli auttaa. Tapaa osoittaa tietoturvan hallinnoinnin järjestelmällisyyttä kutsutaan yleisesti lyhenteellä ISMS (Information Security Management System). Se on kokoelma kontrolleja, joilla voidaan arvioida ja osoittaa, että tietojen luottamuksellisuus, yhteneväisyys ja saatavuus uhkia ja haavoittuvuuksia vastaan on otettu huomioon yrityksen toiminnassa. Alla on lueteltu joitain yleisimpiä hallintamalleja:

EISA (Enterprise Information Security Architecture) on prosessi, jossa tietoturva on sulautettu osaksi yrityksen kokonaisarkkitehtuuria. Sen mukaan yritys ja sen toiminnot ovat turvattavia asioita ja esimerkiksi tietovälineiden ja

verkkojen turvaaminen ovat vain keinoja, joilla se saavutetaan. Gartner EISA on siihen perustuva hallintamalli, joka määrittää kolme käsitteellistä tasoa: ajatuksen, loogisen ja istuttamisen tasot, sekä kolme näkökulmaa: liiketoiminnallisen, informatiivisen ja teknisen. (CIO Wiki, 2020; Shariati et al., 2011.)

SABSA on kuusikerroksinen arkkitehtuuri**,** joka ottaa huomioon riskienhallinnan, tiedonvarmistuksen, yrityshallinnon ja jatkuvuushallinnan. SABSA on ilmainen hallintamalli ja se on käytössä viidessäkymmenessä maassa esimerkiksi pankki-, ydinlaitos-, IT-, tuotanto- ja valtionhallintosektoreilla. Se on yhteensopiva ITIL:in ja TOGAF:in kanssa. Sen sydän on liiketoimintaominaisuuksien profiilidokumentti (Business Attributes Profile) ja se on myös ensimmäisiä hallintamalleja, joka toi aikajatkumon eli jatkuvan parantamisen mukaan hallintamalleihin. (SABSA Institute, 2020; Shariati et al., 2011.)

DoDAF (Department of Defence Architecture Framework) on Yhdysvaltain puolustusministeriön käyttämä arkkitehtuuri tietoturvan hallinnassa. Se keskittyy määrittämään organisaation monimutkaisimmatkin toiminnot selkeäkielisesti, jotta kaikki erilaiset sidosryhmät pystyvät ymmärtämään asian omalta kannaltaan. Organisaation toimintaprosessit esitetään ylemmällä tasolla, yksittäiset kapea-alaiset toiminnot asiantuntijatasolla ja riippuvuussuhteet ja rajapinnat huomioon ottaen. DoDAF jakaa mallinsa seuraaviin näkökulmiin: yleiseen, suoritusperusteiseen, digitaaliseen, operationaaliseen, projektiperusteiseen, palveluperusteiseen ja systeemiperusteiseen. (DoD CIO, 2020.)

E2AF (Extended Enterprise Architecture Framework) on Hollannissa kehitetty hallintamalli organisaation arkkitehtuurille ja se julkaistiin ensimmäisen kerran 2003. Se perustuu IEEE 1471 -standardiin ja on tarkoitettu organisaatioille, jotka ovat riippuvaisia teknologiasta. Siinä käytetään kaksiulotteista matriisia, joka muistuttaa Zachman Frameworkin matriiseja, joskin on enemmän teknologiakeskeinen kuin Zachman. E2AF määrittää neljä eri soveltamisalaa: liiketoiminnan, tiedon, systeemin ja infrastruktuurin. (Magoulas et al., 2012.)

Zachman Framework suunniteltiin alun perin ohjaamaan organisaatioita pois vanhakantaisesta katsantokannasta, jossa käytettiin staattisia malleja ja jätettiin kokonaan yhteydet ja riippuvuudet huomioimatta. (Magoulas et al., 2012.)

TOGAF (The Open Group Architecture Framework) on yleinen tietovaltaisen organisaation arkkitehtuuria luotaava malli. Se ei keskity suoraan tietoturvaan, mutta voidaan käyttää myös siihen tarkoitukseen. TOGAF käyttää muista malleista poiketen omanlaistaan näkökulmaa, jota voidaan luonnehtia sanoilla enemmänkin kokonaisvaltaiseksi organisaation kaikkien komponenttien viralliseksi kuvaukseksi. Se kuvaa metodit kokonaisarkkitehtuurin ja sen elinkaaren kehittämiseksi. (Open Group, 2020; Magoulas et al., 2012.)

MODAF (British Ministry of Defence Architecture Framework) on arkkitehtuurimalli, joka standardisoi organisaatioissa käytössä olleen sekavan hallintamallikäytännön Britanniassa ja se julkaistiin vuonna 2008. Alun perin sen tarkoituksena oli tarjota täsmällistä rakennetta tukemaan puolustusvoimien omien laitteiden ominaisuuksien määrittelyä ja integrointia, erityisesti tukemalla verkkoyhteyksiä. (GOV.UK, 2020.)

GERAM (Generalised Enterprise Reference Architecture and Methodology) on muotoiltu tavalla, joka mahdollistaa hallintamallin käyttäjän yhdistelemään erilaisia malleja uniikin ja henkilökohtaisen mallin luomiseksi. Näin arkkitehtuurin malli on joka organisaatiossa erilainen. Näin ollen se on laaja standardinomainen malli, joka sisältää huolelliset kuvaukset viitearkkitehtuureista, mallintamiskielistä, tekniikoista ja työkaluista. (Magoulas et al., 2012.)

1.1.5 Kohdeyritys

THL (Terveyden ja hyvinvoinnin laitos) on julkinen laitos, joka tutkii ja seuraa suomalaisväestön hyvinvointia ja terveyttä. Se myös kehittää toimenpiteitä terveyden edistämiseksi ja kerää tietoa, jonka avulla se raportoi ja ohjeistaa terveyteen ja hyvinvointiin liittyvissä asioissa ja näin auttaa sidosryhmiään päätöksenteossa. Sidosryhmiä voivat olla valtion, kuntien ja maakuntien päättäjät, sosiaali- ja terveydenhuolto, järjestöt, tutkijat ja kansalaiset. THL toimii sosiaali- ja terveysministeriön alaisuudessa itsenäisenä tutkimuslaitoksena. (THL_a, 2020.)

Tätä tutkimusta kirjoitettiin juuri pahimman koronavirusaallon aikana, jolloin THL:n merkitys suomalaisessa yhteiskunnassa korostui voimakkaasti. THL muodosti pandemian tilannekuvaa, raportoi hallitukselle ja antoi suosituksia kansalaisille ministeriön kanssa säännöllisesti. Tutkija koki myös oman työnsä entistä tärkeämmäksi, onneksi se ei muuttunut tilanteessa akuutimmaksi, joten tutkimusta sai tehdä huolellisesti ja rauhassa

1.2 Tutkimusongelma, tavoitteet ja tutkimuskysymykset

Tietoturvauhkat ovat tulleet jäädäkseen ja viimeistään nyt yritysten olisi hyvä reagoida suunnittelemalla puolustusta. Vaikka monenlaisia keinoja näiden uhkien torjumiselle onkin jo olemassa, ne kaikki ovat erillisiä toimia ja niitä on paljon. Tehokkaaseen suojautumiseen kuuluu se, että kysymyksiin mitä, miksi, milloin ja kuka on vastattu. Tämä edellyttää tietoturvan tehokasta hallintaa, ettei koko käsite jää hienoksi ajatukseksi työpöydälle.

Tämän tutkimuksen tavoitteena on tilauksesta luoda Terveyden ja hyvinvoinnin laitokselle johtamisen hallintamalli, joka ottaa huomioon kyberturvallisuuteen liittyvät asiat. Tätä hallintamallia tarvitaan ISO 27001 -sertifikaatin hakemiseen. Kyseinen standardi on hyväksytty eurooppalaiseksi standardiksi, ja sen virallinen nimi on EN ISO/IEC 27001:2017. Standardi ei ole vapaasti ladattavissa internetistä, vaan se pitää ostaa Suomen Standardisoimisliiton verkkokaupasta. THL halusi tutkimuksen suomeksi, joten käytetty standardikin on virallinen suomennos alkuperäisestä englanninkielisestä.

Tarkoituksena on luoda yhtenäinen hallintamalli siitä, miten tietoturvaa johdetaan THL:n organisaation sisällä, mitkä ovat päävastuut, ja ehdotus siitä, miten hallintamalli sulautetaan olemassa olevaan organisaatioon eli miten

vastuut tulisi jakaa. Sitä ennen tulee selvittää nykyinen organisaatio ja sen rakenne ja vastuut.

Tutkimuksen tavoitteen mukainen päätutkimuskysymys on:

”Millainen hallintamalli THL:n tulisi ottaa käyttöön, jotta ISO 27001 -sertifikaatin vaatimukset täyttyisivät?”

Tutkimuksen alakysymys on:

”Miten tietoturvan vastuut jaetaan tietoturvastandardin mukaan?”

Maailmassa on paljon yrityksiä, jotka erillistä korvausta vastaan auttavat yrityksiä hankkimaan ISO 27001 -sertifikaatin. Julkista tutkimusta ei ole kovin paljoa saatavilla, mutta aiheesta löytyi kuitenkin muutamia julkisesti saatavilla olevia ylemmän korkeakoulututkinnon opinnäytetöitä. Sen lisäksi ilmaista tietoa on saatavilla internetistä, mutta ne on tehty myymään yrityksen palveluita, joten ne eivät vastaa tieteellistä tutkimusta. Niitä voi kuitenkin käyttää hyödyksi siinä vaiheessa, kun standardiin tutustuu.

Tutkimuksen tilaaja on Terveyden ja hyvinvoinnin laitos THL ja tutkimuksen tekee THL:n vieraileva tutkija Tiina Virta, jonka pro gradu -työ tämä tutkimus on. Tutkija opiskelee Jyväskylän yliopistossa kyberturvallisuuden maisteriohjelmassa. Ohjaajana toimii kyberturvallisuuden työelämäprofessori Martti Lehto ja THL:n puolelta tietoturvapäällikkö Andrei Laurén.

1.3 Rajaukset ja tulosten arviointi

Työ on rajattu niin, että malliin otetaan tarkemmin mukaan vain standardin mukaisesti tietoturvan hallinnointiin liittyvät asiat. Tavoitteena on tutkia koko standardi, mutta mallissa ei puututa siihen, kuka vastuita kantaa alemmilla tasoilla, korkeintaan ehdotus siitä, mille osastolle mikäkin tukitoiminto kannattaisi työtehtävien takia sisällyttää. Standardi joudutaan kuitenkin käymään läpi melko yksityiskohtaisesti, joten jos aika riittää, myös toimintojen suhteen tehdään ehdotuksia. Mallin implementointi on rajattu ulos tästä tutkimuksesta. Tutkimuksesta jätetään pois myös ISO 27001 -standardin lisäosa ISO 27701:2019, joka laajentaa varsinaisen standardin huomioimaan myös GDPR:n eli Euroopan tietosuoja-asetuksen. Jos aikaa riittää, saatetaan malliin saada kirjattua ehdotukset tarvittavista asiakirjoista.

2 TIETEELLINEN LÄHESTYMISTAPA

Nykymaailmassa mikään muu ei ole muuttumatonta kuin muutos itse. Organisaatio, joka ei varaudu muutokseen, ei kehity eikä myöskään pysty vastaamaan ajan haasteisiin. Yrityksen tulisi pystyä ennustamaan millaisia muutoksia on tulossa, arvioimaan niiden vaikutusta organisaatioon ja tekemään niihin perustuvia strategisia valintoja. (Ojasalo et al., 2009.)

Usein helpoin tapa varautua tiedettyyn muutokseen on tehdä siitä tutkimus, jos resurssit antavat myöten. Yritykset käyttävät mielellään opiskelijoita tähän, sillä silloin hyöty on molemminpuolinen; yritys saa halvalla tai ilmaiseksi ylimääräisen resurssin käyttöönsä ja opiskelija saa tehtyä opinnäytetyön, jonka avulla voi osoittaa osaamisensa ja valmistua.

Tieteellisen tutkimuksen tekeminen on määrämuotoista ja sen tulee täyttää tietyt kriteerit. Yleensä tutkimus alkaa aiheen kehittelyllä ja lopuksi tulokset esitellään ja työ arvioidaan. Hyväksyttyjä menetelmiä on monia eivätkä ne ole aina yksiselitteisiä, siksi tässä luvussa esitellään tutkijan itsensä järkeväksi kokemia menetelmien kuvauksia.

2.1 Tutkimisen tarkoitus

Tutkimuksen perimmäinen tarkoitus on aina ratkaista ongelma. Ongelma muotoillaan kysymykseksi, johon tutkimuksen lopussa pystytään vastaamaan ainakin jollain tasolla. Tieteellisen tutkimuksen tarkoitus on saada tiettyjen kriteerien mukaista järjestelmällisesti kerättyä ja luotettavaa tietoa ongelmasta ja mahdollisesti löytää siihen ratkaisu.

2.2 Tutkimusmenetelmiä

Jotta tutkimuksesta saadaan tehokas, tulee tutkimusmenetelmä valita oikein. Ikävä kyllä tutkimusmenetelmiä on enemmän kuin yksikään professori kykenee opettamaan; internet ja kirjasto ovat täynnä kaiken kirjavia oppaita ja vaikeutena on valita yksi, minkä perusteella metodeita voi järkevästi vertailla. Tähän tutkimukseen valittiin kaksi todennäköisesti eniten käytettyä opasta: Hirsjärvi, Remes & Sajavaaran opas ”Tutki ja kirjoita” sekä Ojasalo, Moilanen & Ritalahden opas ”Kehittämistyön menetelmät”.

Hirsjärven et al. (1997: 121) mukaan tutkimusote voidaan jakaa kahteen ryhmään, kvalitatiivisiin ja kvantitatiivisiin menetelmiin ja lähestymistapa voi puolestaan olla joko akateeminen (usein yliopistot) tai sovellettu (usein ammattikorkeakoulut). Akateeminen ymmärretään usein teoreettisempana, kun taas sovellettu tutkimus yleensä pyrkii selvittämään käytännön ongelmia. He määrittelevätkin soveltavan tutkimuksen verrattuna akateemisen olevan enemmänkin:

- ongelmanselvitystä kuin datan keräämistä
- seurausten ennakoimista kuin syiden löytämistä
- vaikuttavien seurausten luomista kuin suhteiden mittaamista ja testaamista
- ohjelmien ja palveluiden kehittämistä ja testausta kuin teorioiden kehitystä ja testausta
- tehtävissä tuotannossa kuin laboratoriossa
- tehtävissä organisaation ulkopuolelta kuin tutkimusinstituutissa
- sidottu tiukemmin aikatauluun ja budjettiin
- vähemmän sopusointua tutkijoiden kesken
- tutkimuksen aiheen tulevan työn tilaajalta eikä tutkijalta itseltään
- tutkijoiden olevan enemmänkin yleis- kuin huippututkijoita
- useita metodeita yhdistelevää yhden sijaan
- suunnattu asiakkaalle kuin tiedeyhteisölle ja
- hieman epäilyttävää akateemisesta näkökulmasta, verrattuna korkeaan kunnioitukseen akateemisesti.

Tutkimuksella on aina oltava tarkoitus tai päämäärä, mikä luonnollisesti ohjaa metodien ja strategioiden valintaa. Hirsjärven et al. (1997: 128) mukaan tutkimuskysymys ohjaa tutkimuksen strategiaa seuraavasti:

- kuvaileva tutkimus: tarkoituksena kuvata tarkasti ihmisiä, tapahtumia, ilmiöitä tai dokumentoida jonkin ilmiön mielenkiintoisimpia ja keskeisimpiä piirteitä
- ennustava tutkimus: tarkoituksena ennustaa tapahtumien tai henkilöiden käyttäytymistä seurauksena tietystä ilmiöstä
- haastattelututkimus: tarkoituksena nähdä mitä tapahtuu esimerkiksi prosessissa, löytää uusia lähestymistapoja, selventää vähemmän tunnettua ilmiötä tai kehittää tietty hypoteesi
- tulkitseva tutkimus: tarkoituksena löytää selitys tilanteelle tai ilmiölle, usein käyttäen kausaalisia suhteita tai löytää mahdollisia syy-seurausketjuja.

Ojasalon et al. (2009: 38) mukaan tutkimuksen lähestymiselle on neljä eri tapaa: tapaustutkimus (ns. case study), tapahtumatutkimus, rakentava tutkimus ja innovaatiotutkimus. Tapaustutkimus on yleisesti käytössä silloin, kun tarkoituksena on tuottaa tarkkaa tietoa tietystä asiasta tai löytää kehitettäviä kohtia organisaatiossa. Puhdas tapaustutkimus ei puutu muutoksen tekemiseen, mutta yleensä helpottaa tulevaa muutosta antamalla uusia ideoita tai ehdotuksia tietyn ongelman ratkaisemiseksi. Tapahtumatutkimusta käytetään usein silloin, kun tarkoituksena on saada konkreettista tietoa, joka edesauttaa muutosta, ja sen jälkeen muuttaa tutkittua asiaa sekä mitata muutoksen vaikutuksia. Tämän tutkimusmetodin vaatimuksena on organisaation henkilöstön aktiivinen panos. Rakentava tutkimus pyrkii ratkaisemaan käytännön ongelman luomalla uusia rakennelmia, kuten esimerkiksi tuote, datasysteemi, ohje tai manuaali. Se on yleensä hyvin samankaltainen kuin tapahtumatutkimus, mutta kun edellinen keskittyy lähinnä ihmisten toimintaan, tämä lähestymistapa keskittyy

puolestaan muuttamaan elottomia kohteita. Nämä kaksi tutkimusta sidotaan aikaisempiin tutkimuksiin ja se erottaa ne konsultoinnista. Innovaatiotutkimus on hyvin lähellä rakentavaa tutkimusta ja osittain ne menevät päällekkäin. Suurin ero on innovaation asteessa. Rakentavassa tutkimuksessa tulos voi olla muutos olemassa olevasta eikä siten innovaatio. Innovaatiotutkimuksessa tärkeintä on uuden keksinnön toteuttaminen ja kaupallistaminen, sillä uuden idean keksiminen ei itsessään ole vielä innovaatio. (Ojasalo et al., 2009.)

2.3 Valitut menetelmät

Tutkimusmenetelmäksi valittiin laadullinen eli kvalitatiivinen tutkimus. Ongelmaa lähestytään tapaustutkimuksen eli case-tutkimuksen näkökulmasta, mikä on siis käytetty strategia. Case-tutkimus katsotaan parhaaksi silloin, kun

- tutkimuksen kohteena on yksittäinen tapaus tai organisaatio
- kiinnostuksen kohteena on prosessi tai prosessit
- tutkimus sisältää monimenetelmäisyyttä eli triangulaatiota
- tutkittavasta asiasta halutaan muodostaa tarkka ja syvällinen kuva
- tutkimuksen yhtenä kriteerinä on sen konteksti eli ympäristö on merkittävässä asemassa tutkimuksen kannalta
- tapauksen ymmärtäminen on tärkeämpää kuin yleistäminen
- toistettavuus on yleensä heikko. (Kananen, 2019: 81; Hirsjärvi et al., 2000: 123; Koppa, 2015; Wikipedia_a, 2020; Saaranen-Kauppinen & Puusniekka, 2006.)

Kvalitatiiviseen tutkimusmenetelmään ja case-tapauksen strategiaan päädyttiin, koska tutkimuksen kohteena on THL ja sen organisaatio, erikoistapauksenaan johto ja keskijohto. Kiinnostuksen kohde on juuri tietoturvallisuuden johtamisen prosessi ja sen saattaminen ISO 27001 -standardissa hyväksyttyyn muotoon. Tutkimuksessa käytetään triangulaatiomenetelmää, sillä tutkimusaineiston hankinnassa käytetään useita tiedonhankintamenetelmiä, kuten ISO 27001 -standardi, ulkoiset julkiset tiedonlähteet, yrityksen sisäinen dokumentaatio, haastattelut, aikaisemmat tutkimukset aiheesta ja niin edelleen. Tarkoituksena on kohteen (THL) syvällisen tutkimisen perusteella luoda malli, jota voidaan käyttää juuri kyseisessä organisaatiossa, mutta sen ei ole tarkoituskaan olla yleispätevä. Tapauksen ymmärtäminen omassa kontekstissaan on siis tutkimuksen kannalta olennaisin asia.

3 TUTKIMUKSEN VIITEKEHYS

Tutkimuksen viitekehyksellä tarkoitetaan tutkimuksen teoreettista pohjaa. Tutkimus tarvitsee suuntaviivat, jotka saavat tutkimuksen pysymään tietyssä muotissa, jolloin yksittäiset tutkimusaineistosta nousevat tekijät eivät päädy liian tärkeään osaan tai vie tutkijaa sivupoluille. Se osoittaa suunnan myös sille, mitkä ovat tutkimuksen kannalta keskeisimmät tutkittavat asiat ja niiden suhteet toisiinsa. Tässä luvussa käsitellään ensin valitun standardin ISO 27001:n luomaa viitekehystä, sitten aiheesta tehtyjä aikaisempia tutkimuksia ja lopuksi THL:n nykytilaa. Näitä kolmea vertailemalla pystytään siirtymään empiiriseen tutkimukseen eli luomaan THL:n tietoturvajohtamiselle hallintamalli.

3.1 ISO 27001 -standardi

ISO 27001 -standardia pidetään tehokkaan tietoturvallisuuden benchmarkina eli alan parhaisiin käytäntöihin nojautuvana. ISO 27001 Global Report 2017:n mukaan 91 % tutkimukseen vastanneista uskoi standardin parantavan tietoturvaa. Se on myös maailman kolmanneksi nopeimmin kasvava hallinnon standardi, jonka sertifioinnit kasvoivat yli 450 % viimeisen kymmenen vuoden aikana. Organisaatiot jotka mukauttavat toimintansa standardin mukaiseksi, voivat hakea ulkopuolisen tarkastajan myöntämää sertifikaattia todisteena sekä asiakkaille että sidosryhmille organisaationsa parhaisiin kansainvälisiin käytäntöihin perustuvasta tietoturvan tasosta. (IT Governance, 2020.)

Suurin hyöty ISO 27001 -sertifioinnista on organisaation vahva näyttö sen tietoturvan hallinnoinnista ja samalla tietoturvaloukkausten riskien pienentämisestä. ISO 27001 -standardin lähestymistapa tietoturvaan on kokonaisvaltainen ja siksi se tarjoaa käytännöllisen ja tehokkaan menetelmän todistaa organisaation noudattavan myös useita tietosuojaa ohjaavia kansainvälisiä määräyksiä ja suosituksia, kuten GDPR, NYDFS (Cybersecurity Requirements for Financial Services Companies) ja NIS-direktiivi. ISO 27001 -standardi ei suojaa ainoastaan organisaation sähköistä dataa, vaan myös dataa kannettavilla tietokoneilla, mobiililaitteilla ja muilla elektronisilla laitteilla, suojeltavan tiedon paperisia versioita, immateriaalista pääomaa, organisaation luottamuksellisia tietoja ja asiakastietoja. (IT Governance, 2020.)

Sertifioinnista voidaan katsoa olevan muitakin hyötyjä, esimerkiksi:

- kansainvälisten parhaiden käytänteiden sovittaminen organisaation toimintaan
- riskien parempi tunnistaminen ja niiden tehokkaampi hallinta
- tärkeän datan ja immateriaalioikeuksien parempi suojaaminen
- helpottaa organisaation tulevaisuuden suunnittelua
- uhkien, haavoittuvuuksien ja niiden seurausten tehokkaampi määrittely

- Uusien asiakkaiden löytyminen osoittamalla luotettavuutta ja olemassa olevan asiakaskunnan säilyttäminen
- osoitus siitä, että organisaatio ottaa kyberturvallisuuden tosissaan
- globaalin yhteistyön helpottuminen (esimerkiksi Japanissa ja Intiassa sertifiointi on usein yhteistyövaatimus)
- luo organisaatioon dokumentoidun ja arkistoidun hallintajärjestelmän, joka kantaa kauas tulevaisuuteen
- parantaa yhteensopivuutta
- organisaation toiminnan paraneminen, koska tietoturvaprosessit ja -vastuut on määritelty ja ohjeistettu
- arkaluontoisten tietojen asianmukainen käytön varmistaminen
- todistaa johdon asianmukaisesta huolellisuudesta yrityksen hoidossa (tämä on erityisen tärkeää yrityskaupassa, missä se puoltaa due diligence -pykälää)
- kattaa useat kaupalliset, sopimukselliset ja lain vaatimukset
- todistaa organisaation eri osien toimivan yhteistyön tietoturvan suhteen
- suojaa ja edistää organisaation mainetta
- parantaa henkilöstön, urakoitsijoiden ja alihankkijoiden tietoturvaa
- auditointiprosessien helpottuminen, koska yksi auditointi turvallisuuteen liittyen riittää
- sidosryhmien, osakkaiden ja erilaisten tarkastajien vakuuttaminen tietoturvan tasosta
- taloudellisten rangaistusten ja sakkojen välttäminen. (Baker, 2017; Krypsys, 2020; Pro Pilvipalvelut; 2020; Nixu, 2017.)

Organisaatiolla on yleensä neljä erilaista keinoa käsitellä riskejä, jotka kohdistuvat suojattavaan tietoon yrityksessä:

- välttäminen: riski eliminoidaan kokonaan, esimerkiksi korvaamalla vanhentuneet ohjelmat ja laitteet uusilla teknologioilla
- muokkaaminen: muokataan tiedon suojaustasoa ja asetetaan enemmän kontrollipisteitä, esimerkiksi ISO 27001 -standardin neuvomilla tavoilla, jotta saadaan riskien tapahtumisen todennäköisyyttä pienennettyä
- jakaminen: jaetaan riski kolmannen osapuolen, esimerkiksi vakuutusyhtiön kanssa
- hyväksyminen: organisaatio voi hyväksyä riskin tekemättä sille mitään, esimerkiksi silloin, kun riskin pienentämisen kustannukset ovat suuremmat kuin riskin tapahtumisen kustannus.

Riskien pienentämisen keinoja voivat olla esimerkiksi:

- Tietoturvapolitiikat
- Tietoturvan organisointi (sisältäen mobiililaitteiden käyttöohjeet ja omien laitteiden käytön organisaatiossa)
- Henkilöstöpolitiikka
- Tärkeimpien voimavarojen hallinnointi

- Pääsynhallinta (kuten ohjelmistojen sisäänpääsyn ja käyttäjien velvollisuuksien kontrollointi)
- Tietojen salaaminen (sisältäen salausavainten hallinnan)
- Fyysinen ja ympäristön turvaaminen (sisältäen puhtaan pöydän ja tyhjän ruudun politiikat)
- Operatiivinen turvallisuus (sisältäen haittaohjelmien ja varmuuskopioiden politiikat sekä lokien, uhkien ja haavoittuvuuksien monitoroinnin)
- Viestintäturvallisuus (verkkojen erillistäminen, viestintäkanavien turvaaminen ja varmistustoimenpiteet)
- Järjestelmien hankkimisen, kehittämisen ja huoltamisen turvaaminen
- Alihankkijoihin liittyvien tietoturvariskien kontrollit
- Tietoturvaloukkauksien havainnointien organisointi (sisältäen monitoroinnin ja oikean reagoinnin)
- Liiketoiminnan jatkuvuuden varmistaminen tietoturvan näkökulmasta
- Lakien ja asetusten säännönmukainen noudattaminen. (IT Governance, 2020.)

Tutkimuksen tilaaja THL halusi nimenomaan ISO 27001 -tieto-turvastandardin työn pohjaksi. Tämä standardi esittää vaatimukset organisaation tietoturvan hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitämiseen ja jatkuvaan parantamiseen. Standardi on jaettu seuraaviin osa-alueisiin:

- organisaation toimintaympäristöön
- johtajuuteen
- suunnitteluun
- tukitoimintoihin
- toimintaan
- suorituskyvyn arviointiin ja
- parantamiseen. (SFS, 2017.)

Näitä eri osa-alueita tarkastellaan lähemmin alla. Osa-alueet eivät ole missään tärkeysjärjestyksessä, vaan järjestys määräytyy suoraan standardista.

Organisaation toimintaympäristö

Organisaatio ja sen toimintaympäristön keskeisimmät asiat tulee tuntea ja ymmärtää, sillä siitä riippuu organisaation kyky saavuttaa halutut tulokset hallintajärjestelmältä. Myös sidosryhmien tarpeet ja odotukset tulee ymmärtää: mitkä ovat olennaiset sidosryhmät ja niiden vaatimukset tietoturvalta. Nämä vaatimukset voivat tulla viranomaisilta, olla lakisääteisiä tai vaihtoehtoisesti sopimusvelvoitteita. Tietoturvan hallintajärjestelmä pitää määritellä tarkasti, missä sitä sovelletaan ja missä ei. Yksi tärkeitä selvitettäviä on myös rajapinnat ja riippuvuudet muihin organisaatioihin. Kaiken yllä mainitun dokumentoiminen on ensiarvoisen tärkeää. Luotua hallintajärjestelmää tulee ylläpitää ja parantaa standardin vaatimusten mukaisesti. (SFS, 2017.)

Johtajuus

Johtajuus käsittää eri osa-alueita. Ylimmän johdon tulee olla sitoutunut hallintajärjestelmään varmistamalla, että organisaatiossa on turvallisuusstrategia ja tietoturvapolitiikka, sille on asetettu tavoitteet ja että se on ylipäätään linjassa organisaation strategian kanssa. Johdon tulee myös varmistaa, että vaatimukset yhdistetään organisaation prosesseihin, että tarvittavat resurssit ovat saatavilla ja että viesti asian tärkeydestä saavuttaa organisaation työntekijät. Johdon tehtävänä on edelleen varmistaa haluttujen tulosten saavuttaminen ja tietoturvan hallintajärjestelmän jatkuva parantaminen sekä muiden johtoon kuuluvien tukeminen heidän osa-alueillaan. (SFS, 2017.)

Tietoturvapolitiikan tulee olla organisaation toiminta-ajatukseen soveltuva, sisältää tietoturvatavoitteet sekä sitoutumisen vaatimusten täyttämiseen ja hallintajärjestelmän jatkuvaan parantamiseen. Sen tulee löytyä dokumentoituna tietona koko organisaation saatavilla ja tarvittaessa myös sidosryhmien saatavilla. Ylin johto vastaa siitä, että eri tietoturvaroolien vastuut ja valtuudet määritellään, viestitään oikeille tahoille ja että hallintamallin suorituskyvystä raportoidaan sille säännöllisesti. (SFS, 2017.)

Suunnittelu

Tietoturvan hallintamallin suunnittelu sisältää muun muassa seuraavia asioita:

- riskit ja mahdollisuudet, joiden avulla määritellään haluttujen tulosten saavutettavuus, ei-toivottujen vaikutusten estäminen ja mallin jatkuva parantaminen
- miten riskeihin ja mahdollisuuksiin kohdistuvat toimenpiteet yhdistetään prosesseihin ja toteutetaan, sekä miten niiden vaikuttavuus arvioidaan
- tietoturvariskien arviointiprosessit, jotka sisältävät hyväksymiskriteerit, tuottavat päteviä ja verrattavia tuloksia ja jotka varmistavat tiedon peruselementtien (luottamuksellisuus, eheys, saatavuus) menettämiseen liittyvät riskit
- tunnistamalla riskien omistajat, jotta voidaan varautua seurauksiin, määrittää realistinen todennäköisyys ja riskin taso, sekä verrata riskianalyysin tuloksia laadittuihin kriteereihin ja priorisoimalla riskit
- tietoturvariskien käsittely tulee määrittää ja toteuttaa käsittelyprosessina sekä varmistaa sen aukottomuus
- riskien käsittelysuunnitelman laatiminen, sen hyväksyttäminen riskien omistajilla ja jäljelle jäävien riskien kohtalosta päättäminen
- tietoturvatavoitteiden yhdenmukaisuuden ja mitattavuuden varmistaminen, niiden viestittävyyden ja päivitettävyyden varmistaminen sekä dokumentointi
- ohjeiden laatiminen, resurssien varmistaminen, vastuuhenkilöiden nimeäminen, työn aikatauluttaminen ja arviointi. (SFS, 2017.)

Tukitoiminnot

Organisaation tukitoiminnot sisältävät resurssien varmistamisen, työntekijöiden pätevyyden määrityksen ja sen mahdollisen hankkimisen, pätevöitymisen dokumentoinnin, organisaatiossa työskentelevien tietoisuuden lisäämisen tietoturvapolitiikasta, miten he voivat siihen vaikuttaa, miten se hyödyttää organisaatiota ja mitä seurauksia siitä poikkeaminen voi aiheuttaa. Tietoturvalliseen hallintamalliin tulee myös sisällyttää kaikki viestintä: mitä, milloin, kenelle ja kuka viestii sekä minkälaisia viestintäprosesseja toteutetaan. Tämä koskee sekä sisäistä että ulkoista viestintää. (SFS, 2017.)

Tukitoiminnot sisältävät myös dokumentointiin kohdistuvia määräyksiä. Niihin voivat vaikuttaa organisaation koko ja tuotteiden tai palveluiden tyyppi, prosessien monimutkaisuus ja niiden väliset vuorovaikutukset sekä henkilöiden pätevyys. Periaatteena on, että kaikki tiedon hallinta tulee dokumentoida, dokumenteista tulee näkyä merkintä, kuvaus, tallennusmuoto ja -väline sekä tiedon soveltuvuuden ja riittävyyden varmistaminen. Dokumentoitua tietoa tulee hallita niin, että se on aina saatavilla sopivassa muodossa, se on suojattu vain käyttötarkoitustaan varten, sen säilytys on suunniteltu ennalta määriteltyjen kriteereiden mukaan, muutostenhallinta on käytössä ja miten ja milloin tieto hävitetään. (SFS, 2017.)

Toiminta

Organisaation toimintaosio sisältää kaiken tietoturvan vaatimusten täyttämiseen sisältyvät toiminnot ja niiden ohjauksen sekä tietoturvariskien arvioinnin ja käsittelyn. Toimintoja tulee ohjata ja dokumentoida, sekä hallita muutosta ja arvioida tahattomien muutosten seurauksia ja lieventää mahdollisia haittavaikutuksia. (SFS, 2017.)

Suorituskyvyn arviointi

Organisaation tulee seurata, mitata analysoida ja arvioida tietoturvan tasoa ja hallintajärjestelmän vaikuttavuutta. Sen tulee määrittää mitä seurataan ja mitataan, millä menetelmillä varmistetaan hyväksyttävät tulokset, milloin ne toteutetaan, kenen toimesta, sekä milloin tuloksia analysoidaan ja arvioidaan ja kuka sen toteuttaa. Myös kaikki tämä tulee dokumentoida asianmukaisesti. (SFS, 2017.)

Sisäistä auditointia tulee tehdä suunnitelluin aikavälein, jotta voidaan määrittää, onko tietoturvallisuuden hallintajärjestelmä sekä organisaation omien että standardin vaatimusten mukainen. Auditointiohjelmien suunnittelun tulisi sisältää auditointien taajuus, menetelmät, vastuut, vaatimukset, raportointi, kriteerit, soveltamisala, puolueettomat auditoijat, raportointi johdolle ja auditoinnin dokumentointi. Johdon katselmuksen tulisi tapahtua suunnitelluin aikavälein, jotta hallintamallin voidaan varmistaa olevan organisaatiolle sopiva, asianmukainen ja vaikuttava. Johdon katselmuksesta määrätään yksityiskohtaisesti standardissa

ja sen tulisi parantaa hallintamallia ja tuoda esille mahdolliset muutostarpeet. (SFS, 2017.)

Parantaminen

Parantaminen määrittää poikkeamien ja korjaavien toimenpiteiden hallinnan. Poikkeama tulisi aina katselmoida, selvittää sen syy ja suorittaa mahdolliset toimenpiteet sen korjaamiseksi tarvittaessa. Toimenpiteiden tulisi aina olla tarkoituksenmukaisia poikkeaman vaikutukseen nähden. Tietoturvan hallintajärjestelmää tulisi parantaa niin, että se on koko ajan mahdollisimman sopiva, riittävä ja vaikuttava organisaation käyttöön. (SFS, 2017.)

Vaikka tyypillistä ISO 27001 -käyttöönottoprojektia ei ole, standardointeihin erikoistuneen yrityksen IT Governancen Alice Baker (2017) listaa blogissaan yhdeksänportaisen lähestymistavan:

1. projektin mandaatin hankkiminen johdolta eli sitoutuneisuuden varmistaminen
2. projektin luonti, resurssointi ja hallinnoinnin muodosta päättäminen
3. ISMS:n luonnin aloittaminen
4. tarkemman hallinnon viitekehyksen laatiminen
5. tietoturvan perusasioiden kirjaaminen
6. riskien kartoitus, mikä on standardin sydän – nämä ohjaavat politiikkojen luomista
7. toteutus, mikä tässä tarkoittaa suunnitelmaa siitä, miten riskejä hallitaan
8. mittaa, valvo ja katselmoi, jotta pystyt parantamaan asioita
9. sertifikaatti akkreditoidulta ulkopuoliselta toimijalta.

Hän kertoo myös, että pieni hyvin asioitaan jo dokumentoinut organisaatio saattaa saada hankittua ISO 27001 -sertifikaatin kolmessa kuukaudessa, mutta usein se kestää isommilta organisaatiolta vähintään vuoden. Se vaatii koko organisaation sitoutumista ja työtä ja se on aina uniikki ja räätälöity organisaatiolle. Kahta samanlaista ISMS:ää ei ole.

3.2 Aikaisemmat tutkimukset

Pöyhönen, Lehto ja Lehto (2019) ovat tutkineet terveydenhuollon ja nimenomaan sairaalajärjestelmien turvallisuutta ja toiminnan kehittämistä. Terveydenhuolto nojaa enenevässä määrin teknologiaan ja digitalisoituu siinä missä muutkin alat. Tietoverkot hyödyttävät terveyspalveluja ja varsinkin esineiden internet laajenee nopeasti myös terveydenhuollon käytössä. Tämä aiheuttaa erityistä huolta, sillä tunnetusti IoT-laitteet eivät ole yhtä hyvin suojattuja kuin esimerkiksi yksittäiset

tietokoneet ja palvelimet. Terveydenhuollossa vaaratilanteet voivat johtaa kliinisen hoidon ja potilasturvallisuuden vaarantumiseen. (Pöyhönen et al., 2019.)

Viime vuosina terveydenhuolto on nähnyt useita datamurtoja, tämän tutkimuksen kirjoitushetkellä kohistaan edelleen psykoterapiakeskus Vastaamon tietomurrosta ja kiristyksestä. Tuntematon kiristäjä julkaisi verkossa keskuksen potilaiden arkaluontoisia terapiatietoja ja uhkasi paljastaa lisää tietoja, jos Vastaamo ei maksa lunnaita. Myös yksittäiset potilaat ovat saaneet kiristysviestejä. Valvira, Kyberturvallisuuskeskus ja Keskusrikospoliisi tutkivat tätä maailmanlaajuisestikin poikkeuksellista tapahtumaa. Sen lisäksi suomen valkohattuhakkerit ovat aktivoituneet auttamaan sekä uhreja selvittämään tilannetta että poliisia tutkimuksissa. Esimerkiksi juuri keväällä perustettu KyberVPK on ollut aktiivinen toimija asiassa. (YLE, 2020; Futucast, 2020.)

Pöyhönen et al. (2019) korostavat terveydenhoitoalaan kohdistuvan aivan erityisiä vaatimuksia. Potilastietojen eheys ja saatavuus eivät saisi vaarantua missään vaiheessa, koska ne saattavat estää potilaiden turvallisen hoidon. Tietoja voidaan käyttää myös rikollisiin toimiin, esimerkiksi henkilötietojen kohdalla identiteettivarkauksiin, vaikka hoitoturvallisuus ei vaarantuisikaan. Raportissa mainitaan erittäin luottamuksellisten tietojen käsittelyssä olevan myös erityisiä haasteita: sairaalatietojärjestelmien kehittäminen ja kannettavien hyvinvointilaitteiden lisääntyminen, nopeasti tuotetun tiedon välitön käsittely (jotta hätätilanteessa voidaan reagoida mahdollisimman nopeasti), erilaiset tuotetut tietorakenteet (tekstiä, kuvaa, ääntä, videota) sekä erilaisten tietojen yhdistämisestä johtuva arvonlisäys. (Pöyhönen et al., 2019.)

Vaikka THL ei ole sairaala, se käsittelee paljon sensitiivistä dataa. Kun dataa käytetään tutkimukseen, se anonymisoidaan eli käsitellään niin, ettei sitä pysty johtamaan yksittäiseen henkilöön. Esimerkiksi Infektiotautien torjunta ja rokotukset -yksikössä käytetään useista eri rekistereistä saatavia tietoja THL:n lakisääteisten tehtävien toteuttamiseen. Yksikössä arvioidaan ja seurataan muun muassa tartuntatautien ilmaantuvuutta, kansallisen rokotusohjelman toteutumista sekä rokotusten tehokkuutta ja turvallisuutta. (Elonsalo, 2020.)

Itse ISO 27001 -standardiin perustuvia vapaasti hyödynnettäviä tutkimuksia on hämmentävän vähän. Tatu Suhonen (2019) on huomannut saman tutkiessaan omassa pro gradu -työssään standardiin perustuvien sertifiointien hankintaperusteita ja sertifiointielimien valintaperusteita. Syyt joita hän löysi ovat hyvin yhteneväisiä tämän tutkimuksen kanssa eli sertifiointi parantaa tietoturvaa kokonaisvaltaisesti, helpottaa lainsäädännön kanssa ja auttaa taloudellisissa näkökulmissa lähinnä organisaation luottamuksen lisääntymisenä, myynnin helpottumisena ja säästämällä aikaa ja rahaa. (Suhonen, 2019.)

Valtiovarainministeriö (2020) on julkaissut määritelmän julkisen hallinnon digitaalisesta turvallisuudesta, joka osaltaan tukee kansallisen kyberturvallisuusstrategian 2019 toteuttamista. Sen tarkoituksena on määrittää digitaalisen toimintaympäristön kehittämisen periaatteet ja keskeiset palvelut ja siten suojata yhteiskuntaa kyberuhkilta. Sen mukaan Suomi tunnetaan edelläkävijänä digitaalisten palvelujen tarjoamisessa ja vertailu tehtiin KPMG:n tämän vuoden helmikuussa tuottaman raportin pohjalta. Verrokkimaina olivat Hollanti, Australia,

Ruotsi, Saksa, Iso-Britannia, Venäjä, Israel ja Viro. Näissä kaikissa maissa on jonkinlainen kyberturvallisuusstrategia tai digitalisaatiostrategia, joskin termien kirjava käyttö vaikeutti vertailun tekemistä. Lainsäädäntö on kirjavaa, mutta EU:n tietosuoja-asetus GDPR sekä verkko- ja tietoturvadirektiivi NIS tekevät käytännöistä toivottavasti yhtenäisempiä tulevaisuudessa. Uudistettu EU-viranomainen ENISA (European Union Agency for Cybersecurity) vahvistaa rooliaan kyberturvallisuuden koordinoijana ja neuvonantajana ja se määrittelee sertifiointijärjestelmän prosesseille, palveluille ja tuotteille. Kyseinen sertifiointijärjestelmä on vasta työn alla, mutta se tullee noudattamaan pitkälle ISO 27k -standardiperhettä. Nykyvertailussa huomattiin, että jonkinlainen vaatimus sertifiointiin (joko yksittäisen henkilön tai organisaation) on käytössä monissa maissa. Israel vaatii henkilökohtaista sertifiointia kaikilta, jotka ovat tekemisissä kyberpuolustuksen, tunkeutumistestauksen, tietoturvaloukkausten tutkinnan tai kyberpuolustuksen metodien ja teknologioiden kanssa. (Valtiovarainministeriö, 2020; ENISA, 2019.)

3.3 THL:n nykytila

Terveyden ja hyvinvoinnin laitos (THL) on sosiaali- ja terveysministeriön alaisuudessa toimiva itsenäinen tutkimuslaitos, jota johtaa LT Markku Tervahauta. THL tutkii ja seuraa suomalaisten hyvinvointia, tarjoaa asiantuntemusta ja ratkaisuja hyvinvoinnin edistämiseen ja sidosryhmilleen tutkimukseen ja tietoaineistoihin perustuvaa tietoa heidän päätöksentekonsa tueksi. Suomalaisille yritetään turvata hyvä elämä oikeudenmukaisessa ja uudistuvassa yhteiskunnassa. Sen painopisteitä ovat hyvinvointiyhteiskunnan kestävyys, eriarvoisuuden ja syrjäytymisen vähentäminen, muuttuva sairauksien kirjo, terveysuhkiin varautuminen, palvelujärjestelmän muutos ja valtion sosiaali- ja terveydenhuollon erityispalvelujen ohjaaminen ja järjestäminen (esimerkiksi oikeuslääketieteelliset ruumiinavaukset, mielisairaalat, koulukodit ja lähisuhdeväkivallan auttava tukipuhelin). THL:n tutkimustyöhön kuuluvat lisäksi esimerkiksi yhdenvertaisuusasiat, nuorten ja lasten terveys, hometalot ja rikosseuraamusasiat. Näistä kaikista muodostuu paljon rekistereitä, joten THL käsittelee käytännössä lähes kaikkien suomalaisten tietoja. (THL_a, 2020; Lauren_b, 2020.)

THL on yksi Suomen kansainvälisesti verkottuneimpia tutkimusorganisaatioita ja tukee uudistuvaa kansallista terveydenhuoltoa tekemällä työtä muun muassa sote-uudistuksen ja sosiaali- ja terveydenhuoltojärjestelmän digitalisaation asiantuntijana. Laitoksella on käynnissä noin 70 EU:n rahoittamaa hanketta. THL:n tuottamia artikkeleita julkaistaan tieteellisissä lehdissä vuosittain noin 700, joista puolet on kansainvälisiä yhteisartikkeleita. (THL_a, 2020.)

3.3.1 Strategia, arvot, visio ja hallinto

THL julkisti uusimman strategiansa viime vuonna. Iskulauseekseen he ottivat ”Terveyden ja hyvinvoinnin laitos – jotta me kaikki voisimme hyvin”. THL on miettinyt arvojaan ja haluaa olla ”luottamuksen arvoinen”, ”inhimillinen vuorovaikuttaja” ja ”yhdenvertaisuuden suunnannäyttäjä”. Näitä arvoja se toteuttaa seuraavilla keinoilla: ”osaamme, kokeilemme, uudistamme, arvostamme, kuulemme, keskustelemme, osallistamme, kannustamme, haastamme”. Missionaan se ilmoittaa edistävänsä väestön hyvinvointia, terveyttä ja turvallisuutta, ehkäisevänsä sairauksia ja sosiaalisia ongelmia sekä kehittävänsä hyvinvointiyhteiskuntaa. THL:n visio on olla maailman vaikuttavin terveys- ja hyvinvointialan tutkimuslaitos tekemällä korkeatasoista tutkimus- ja asiantuntijatyötä, sekä kumppaniensa kanssa yhteistyössä parantavansa väestön terveyttä, toimintakykyä ja osallisuutta ja vahvistavansa ihmisten mahdollisuutta pitää huolta omasta ja läheistensä hyvinvoinnista. Se haluaa myös rakentaa tasa-arvoista, yhdenvertaista ja kestävää yhteiskuntaa ja pitää huolta heikommassa asemassa olevista. THL:n strategiset tavoitteet ovat:

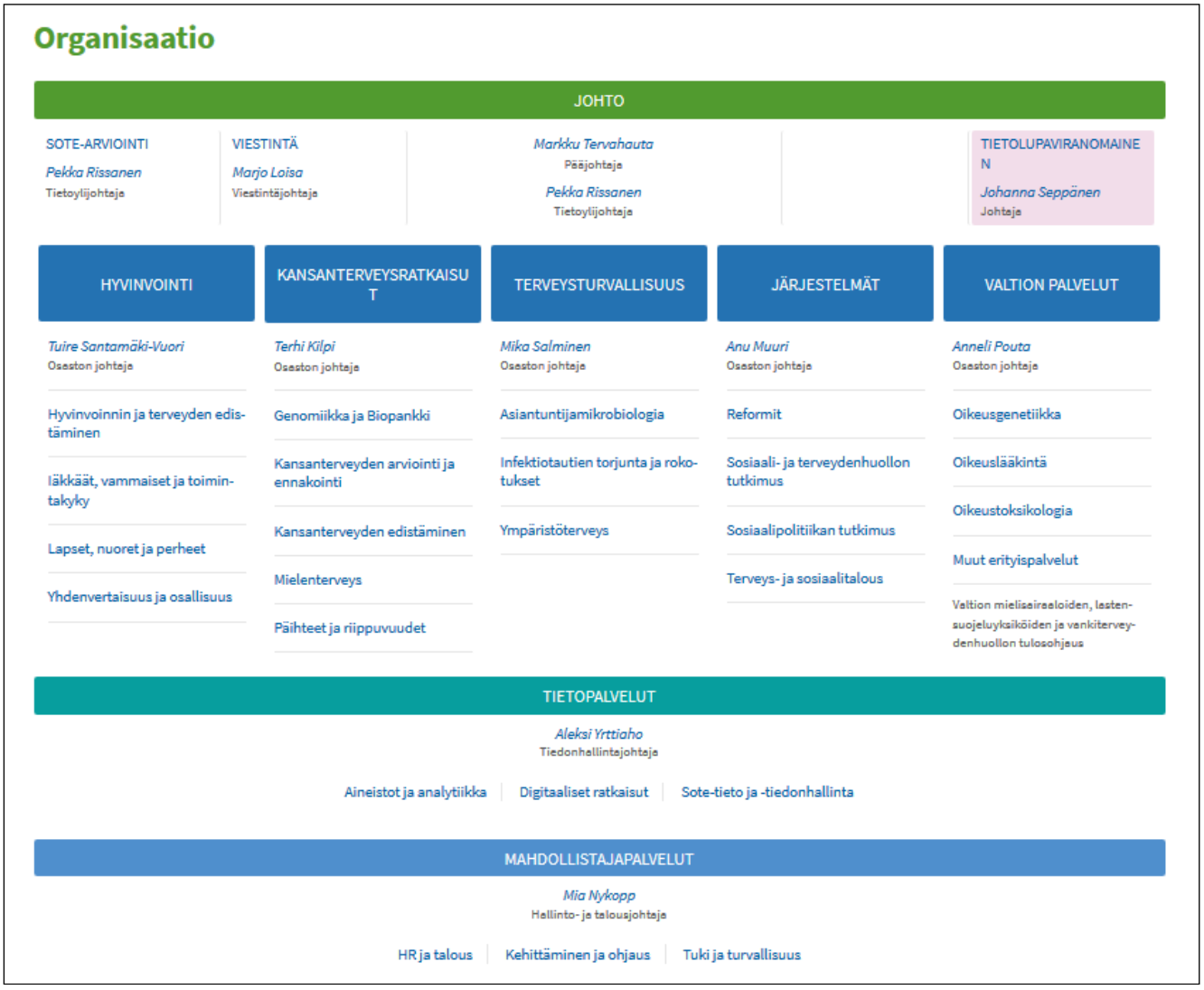
- tieto (vastaamalla tiedon tarpeisiin laadukkaasti ja oikea-aikaisesti, laajentamalla tietotuotantoa katvealueille ja huolehtimalla digitaalisesta turvallisuudesta varautumalla kyberuhkiin)
- tulkinta (ylläpitämällä tilannekuvaa ja ennakoimalla tulevaa sekä kiteyttämällä näkemys muutoksen voimaksi)
- ratkaisut ja tuki (tuottamalla toimintamalleja ja suosituksia sidosryhmien käyttöön, tukemalla sosiaali- ja terveydenhuollon järjestelmäuudistusta ja vauhdittamalla hyvän kasvun kierrettä). (THL_b, 2020.)

THL:n pääjohtajan keskeisin työväline laitoksen johtamisessa on johtoryhmä, missä ylin johto valmistelee tärkeimmät linjaukset ja sitoutuu niihin. Johtoryhmä myös seuraa toiminnan tuloksia ja tehokkuutta, kohdentaa voimavaroja ja linjaa myös henkilöstöä koskevia asioita. Käsittely painottuu tulevaisuuteen, sen haasteisiin ja mahdollisuuksiin. Johtoryhmä on nimenomaan operatiivinen ja asioita käsitellään keskustellen. Johtoryhmään kuuluu pääjohtajan lisäksi eri osastojen ja toimintojen johtajia. Pääjohtajan työtä tukevat myös johtamisfoorumi, johon kuuluvat johtoryhmän jäsenten lisäksi yksiköiden päälliköt ja henkilöstön edustaja. Pääjohtaja antaa henkilöstöinfoja säännöllisesti. (Terho_a, 2019.)

3.3.2 Organisaatio

THL on juuri läpikäymässä vaihetta, jolloin koko sen organisaatio uudistuu. Koska tilanne elää koko ajan, tähän tutkimukseen kuvataan tilanne, mikä on ollut tiedossa lokakuun lopussa. THL:n organisaatio on hieman monimutkainen eikä kaikkia osia ole kuvattu vielä edes intranetissä, joten tutkimuksen tiedot perustuvat sekä julkiseen internetissä olevaan tietoon että turvallisuuspäällikön haastatteluihin.

THL:n organisaatio on matriisiorganisaatio (kuva 1), joka on jaettu viiteen erillisyksikköön: hyvinvointiin, kansanterveysratkaisuihin, terveysturvallisuuteen, järjestelmiin ja valtion palveluihin. Kaikkien näiden läpi toimii kolme erillistä palvelua, jotka toimivat kaikissa yksiköissä. Nämä palvelut ovat johto, tietopalvelut ja mahdollistajapalvelut. (THL_c, 2020, Lauren_d, 2020.)

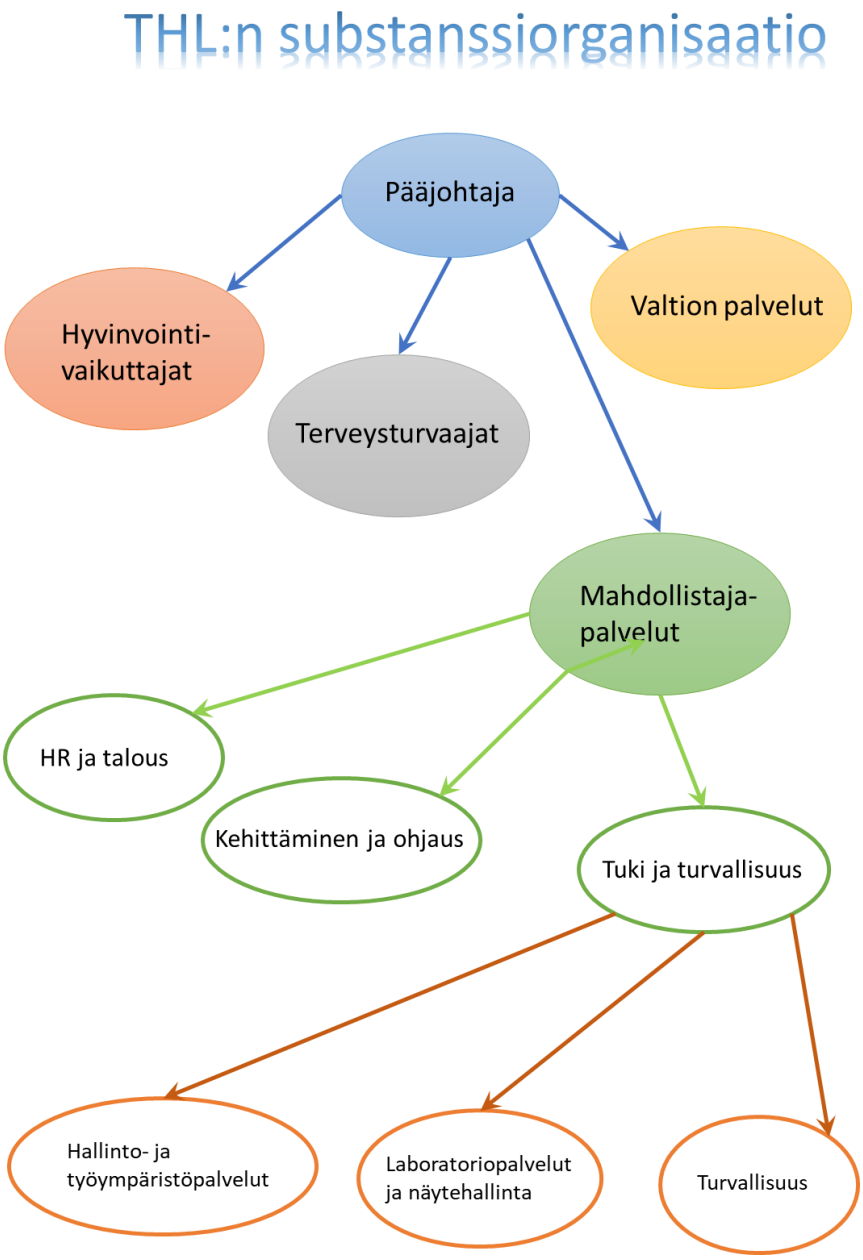


Kuva 1 THL:n organisaatio (THL_c, 2020)

THL käyttää myös substanssiorganisaatiota, jossa tehtävät on jaettu substanssiosaamisen mukaan, eli osa niistä palvelee organisaation kaikkia osia. Kun ajatellaan kyberturvallisuutta, substanssiosaaminen on organisoitu alla olevan kuvan mukaisesti (kuva 2). Mahdollistajapalveluilla on yksi johtaja, joka vastaa kolmesta eri yksiköstä: HR ja talous, kehittäminen ja ohjaus sekä tuki ja turvallisuus. Tuki ja turvallisuus -yksikkö on taas jaettu kolmeen eri tiimiin: laboratoriopalveluihin ja näytteidenhallintaan, hallinto- ja työympäristöpalveluihin ja turvallisuuteen. Turvallisuus-tiimin vastuulle kuuluvat seuraavat asiat:

- riskienhallinta
- jatkuvuudenhallinta
- tietoturva
- tilaturvallisuus
- työsuojelu

ja se palvelee THL:ää konsernina eli kautta koko organisaation. Tietoturvan tila eli kypsyys arvioidaan ja raportoidaan vuosikellon mukaan sekä tarvittaessa. Työjärjestys linjaa annetut vastuut ja johdolle raportoidaan sen mukaan tieto- ja tilaturvallisuudesta sekä työsuojelusta. Nykyinen riskienhallinta on määritetty riskikuvausten kautta. Seuranta ja raportointi tapahtuu tuki- ja turvallisuusyksikön kautta. (Lauren_d, 2020.)



Kuva 2 THL:n substanssiorganisaatio (Lauren_d, 2020)

3.3.3 Tiedon suojaaminen

Terveyden ja hyvinvoinnin laitoksella käsitellään luonnollisesti paljon sekä julkista että salassa pidettävää tietoa ja myös lainsäädäntö lähtee tietoturvan asianmukaisesta suojauksesta. Tietoturvajärjestelyt THL:llä pyrkivät tietojen, tietojärjestelmien ja palvelujen asianmukaiseen suojaamiseen niin, että niiden eheyteen, luottamuksellisuuteen ja käytettävyyteen liittyvät riskit ovat hallinnassa. Tietoturva on myös integroitu osaksi organisaation toiminnan laatua. THL:n tietoturva perustuu muun muassa seuraaviin lakeihin:

- viranomaisten toiminnan julkisuudesta annettu laki (JulkL, 621/1999) ja asetus (1030/1999)
- Terveyden ja hyvinvoinnin laitoksesta annettu laki (668/2008) ja asetus (675/2008)
- EU:n yleinen tietosuoja-asetus GDPR
- GDPR:ää tukeva tietosuojalaki (1050/2018)
- EU:n verkko- ja tietoturvadirektiivi NIS
- laki julkisen hallinnon tiedonhallinnasta (906/2019; yleislaki)
- Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtiohallinnossa (1101/2019)
- rikoslaki (39/1889)
- perustuslaki (mm. yksityisyyden suoja ja julkisuusperiaate)
- laki sähköisen viestinnän palveluista (917/2014)
- sosiaali- ja terveydenhuollon erityislainsäädännöt (esim. THL:n ylläpitämiä rekistereitä ja tilastoja koskevat lait). (Terho_b, 2018; Lauren_c;2020; Kyberturvallisuuskeskus, 2020.)

THL noudattaa myös valtionhallinnon tietoturvallisuutta, jota johtaa Valtiovarainministeriön asettama Valtionhallinnon johtoryhmä eli VAHTI. Sen keskeisin tietoturvaa ja sitä kautta henkilöstöä koskeva säädös on VAHTI 2/2010 ”Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta”, joka on aikaisemmin määritellyt THL:ssä käytettävän ohjeistuksen salassa pidettävästä tiedosta. Tällä hetkellä salassa pidettävien tietojen käsittelyssä noudatetaan julkisuus- ja tiedonhallintalakeja ja turvallisuusluokitteluasetusta tarvittaessa. Viranomaisten toiminnan lähtökohta on avoimuus ja julkisuus, joten tieto on salassa pidettävää vain silloin, kun siitä on erikseen lailla säädetty. Myös tietoaineiston elinkaareen on kiinnitetty huomiota, jotta tutkimusaineistojen ja henkilötietojen luottamuksellisuus, eheys ja käytettävyys säilyisivät kaikissa tilanteissa. Sen lisäksi henkilötietolaki edellyttää tietojen käsittelyn olevan suunniteltua ja sidottua käyttötarkoitukseen. Konkreettisesti tämä tarkoittaa sitä, että jos esimerkiksi henkilötietoja on alun perin kerätty vanhusten liikuntatottumusten selvittämiseen, niitä ei saa myydä terveyspalveluyrityksille markkinointitarkoitukseen. THL suunnitteleekin kaiken salattavaan tietoon liittyvän aineiston elinkaaren aina etukäteen. Tieto arvioidaan ja luokitellaan

suojaustasoihin, joka määrittelee tiedon suojausratkaisun ja menettelyt sen käsittelyyn. Tieto myös anonymisoidaan ja pseudonymisoidaan tutkimusten ja riskien perusteella. Tutkimusta suunniteltaessa mukana on aina myös tutkimuslupamenettely ja eettinen toimikunta, joka arvioi asioita ei vain eettisyyden vaan myös tietosuojan näkökulmasta. IT-infrastruktuurin liittyvät ratkaisut käsitellään tietohallinnossa. Pseudonymisointi tarkoittaa sitä, että tiedosta on poistettu suoran tunnistamisen mahdollisuus, mutta välillisen tunnistamisen mahdollisuus on olemassa (esim. henkilötieto on koodattu ja koodiavaimen selvittämällä henkilön pystyy tunnistamaan). Anonymisointi puolestaan tarkoittaa sitä, että tiedosta on poistettu suoran tunnistamisen lisäksi välillisen tunnistamisen mahdollisuus. (Terho_b, 2018; Lauren_c, 2020.)

Tiedon kerääminen, aineiston säilytys ja käyttö sekä tiedon luovutus, siirtäminen, arkistointi ja hävitys on THL:llä tarkoin määritelty ja ohjeistettu. THL:n työntekijöillä on vaitiolovelvollisuus ja tietojen hyväksikäyttökielto myös työsuhteen päättymisen jälkeen. Työntekijöitä on ohjeistettu olemaan puhumatta työasioista julkisilla paikoilla, esimerkiksi lounasravintolassa tai julkisissa liikennevälineissä. Laitteiden käytöstä, säilytyksestä, hävittämisestä ja salasanoista on myös tarkat ohjeet. Toimitilaturvallisuus käsittää kulunvalvonnan, teknisen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä lähettipalvelujen ja tietoaineistoja sisältävien lähetysten turvallisuuden. Verkkopalvelujen turvallisuudesta, etätyöstä ja etäkäytöstä, ongelmatilanteista ja niiden raportoinnista on niin ikään tarkat ohjeet. (Terho_b, 2018.)

3.3.4 Haavoittuvuuksien hallinta

THL:n haavoittuvuuksien hallintaa varten on oma politiikkansa, jossa on yksityiskohtaiset ohjeet haavoittuvuuksien luokittelusta, riskien arvioinnista, säännöllisten skannausten tekemisestä, vastuista ja seurannasta. Näin organisaatio minimoi riskejä, jotka saattavat vaarantaa THL:n tuottamien ICT-palveluiden tai hallinnoimien tietojen eheyttä, luottamuksellisuutta tai saatavuutta. (Terho_c, 2017.) Myös lokipolitiikka on tarkoin määritelty ja se sisältää ohjeet lokitietojen keräämiselle, kirjausten kohteille, lokitettaville tapahtumille, niiden formaatille, sisällölle, säilytykselle, seurannalle, analysoinnille, raportoinnille, luovutukselle ja tuhoamiselle. Politiikassa on huomioitu edellisten lisäksi järjestelmien toiminnan seuraaminen, ei-toivottujen tilanteiden ennakointi, tapahtuneisiin tilanteisiin reagointi ja toiminnan ja järjestelmän kehittäminen tehtyjen havaintojen perusteella. Tämän lisäksi järjestelmien normaalia käyttöä, vikatilanteita sekä järjestelmänvalvojien ja pääkäyttäjien toimia seurataan ja valvotaan jatkuvasti. (Terho_d, 2017.)

Perusinfrastruktuuria hoitaa Valtion tieto- ja viestintätekniikkakeskus (Valtori) ja siihen sisältyvät myös asiaan kuuluvat tietoturva-asiat. Organisaation perusperiaate on, että vain tarpeellinen ja erikseen hyväksytty liikenne sallitaan, muu liikenne estetään. Verkko on luonnollisesti jaettu aliverkkoihin, joiden välistä liikennettä myös suodatetaan palomuurein. Vastuuhenkilöt ovat THL:n sisällä ja he arvioivat ja hyväksyvät palomuurien sääntömuutokset ja

liityntäpisteet. (Terho_e, 2017; Lauren_c, 2020.) Myös pilvipalveluista löytyy selkeät säännöt, ja turvalliset, harkintaa vaativat ja kokonaan kielletyt pilvipalvelut on selkeästi luetteloitu (Terho_f, 2019; Terho_g, 2019).

THL on valtion laitos, joka käsittelee kaikkien Suomessa asuvien tietoja, joten tietojen suojaaminen on ensiarvoisen tärkeää. THL onkin laatinut laajat ohjeet salassa pidettävien asiakirjojen luokittelusta ja käsittelystä. Vastuut ja rangaistussäännökset on selkeästi esitetty ja perusteltu, samoin suojaustasot ja turvallisuusluokitukset asiakirjojen merkitsemisohjeita myöten. Kaikki asiat on määritelty elinkaaren eri kohdissa koskien tietoaineiston luontia, vastaanottoa, jakelua, siirtoa, sähköistä käsittelyä, säilytystä ja hävittämistä unohtamatta. Myös fyysiset tilat pääkonttorissa Helsingissä on luokiteltu suojaustasoittain. Sähköpostin käytölle on annettu erilliset kattavat ohjeet. (Terho_h, 2020; Terho_i, 2013.)

Roolit ja vastuut ulkopuolisten palveluntarjoajien tietoturva-asiat, tietosuoja, pääsynvalvonta (fyysinen ja sähköinen), viestintäturvallisuus ja henkilöstön rekrytointiin liittyvät asiat on selkeästi määritelty THL:llä. Näistä kaikista löytyy opas intranetistä. Myös hankekohtainen tietoturvaopas on saatavilla intranetistä, samoin ohjeet tietoturvallisesta sovelluskehityksestä. Tietoturvapoikkeamien ja häiriötilanteiden käsittelyyn on oma ohjeensa, kuten myös tietoturvatestauksiin ja tarkastuksiin. Hankintoja varten on oma turvallisuusohjeensa. (Terho_j, 2018; Terho_k, 2017; Terho_l, 2018; Terho_m, 2018; Terho_n, 2019.)

3.3.5 Riskienhallinta

THL on laatinut riskiprofiilin, jossa määritellään laitoksen tiedetyt turvallisuusuhat ja määritellään riskienhallinta. Uhkia ovat muun muassa:

- yksittäiset toimijat (verkkorikolliset, hakkerit, lunnasvaatimukset, petosyritykset tms.)
- rikolliset ryhmittymät (tietomurrot, kohdistetut toimenpiteet)
- aktivistit (yksittäisten tai ryhmittymien tekemät tietomurrot, toiminnan häiriköinti jne.)
- toiset valtiot (tiedonhankinta ja häiriköinti)
- inhimilliset virheet (vahingot, virheet, virheellisen tiedon julkaisu)
- henkilö- ja tutkimusrekistereihin liittyvät tietomurrot.
- tiedustelutoiminta (yksityiset ja valtiolliset) (Terho_o, 2018; Lauren_c, 2020.)

THL jakaa henkilöriskit niin sanottuun perinteiseen insider-toimintaan sekä tahattomaan välikätenä toimimiseen, kun hyökkääjä yrittää päästä käsiksi haluamaansa tietoon. Näitä riskejä pienennetään henkilökunnan ja palveluntuottajien taustojen huolellisella selvittämisellä, koulutuksilla, kulku- ja käyttöoikeuksien tarveperusteisella myöntämisellä ja korostamalla henkilökunnan herkkyyttä reagoida epäilyttävään tai poikkeavaan toimintaan. Laitoksella noudatetaan vähimmän oikeuden eli ns. need-to-know-periaatetta sekä kulkuoikeuksien että tietoresurssien pääsyn kohdalla. Tietoverkkojen tehokkaat valvonta- ja

torjuntatyökalut ovat käytössä, käytäntöjä ja kontrolleja tarkistetaan säännöllisesti ja vahvistetaan tarvittaessa, minkä lisäksi riskialueiden kohdeympäristössä työskentelevien ulkopuolisten palveluntuottajien ja oman henkilökunnan osalta tehdään tarvittaessa turvallisuusselvitys ennen kohteisiin päästämistä. Palveluntarjoajien kohdalla harkitaan joka kerta erikseen turvallisuussopimusten tarpeellisuutta ja työkohteen ollessa erikoistilat tai salaisen tiedon käsittely, koulutukseen ja valvontaan kiinnitetään erityistä huomiota. (Terho_o, 2018.)

THL jakaa tietoturvallisuusriskit useisiin alaryhmiin ja niiden sisällä vielä tarkempiin prosesseissa mahdollisesti esiintyviin riskeihin. Yleistasolla tietoturvariskit on jaettu seuraavasti:

- salassa pidettävät aineistot ja niihin liittyvät riskit
- haavoittuvuudet ja niiden paikkaaminen
- verkkoympäristöihin ja sovelluskehitykseen liittyvät riskit
- haittaohjelmat
- palvelunestohyökkäykset
- verkkopetokset ja huijaukset
- pilvipalveluihin liittyvät riskit
- henkilöriskit
- hankintoihin ja palveluostoihin liittyvät riskit
- some: väärän tiedon levittäminen
- kalasteluviestit. (Terho_o, 2018; Lauren_c, 2020.)

THL:llä on varautumisvelvoite, joka on kirjoitettu yhteiskunnan turvallisuusstrategiaan (Turvallisuuskomitea, 2017) ja se velvoittaa huoltovarmuuskriittisten valtion laitosten varmistamaan mahdollisimman häiriötön tehtävien hoitaminen häiriötilanteissa ja poikkeusoloissa. Jatkuvuussuunnitelma on käytössä monissa yrityksissä ja THL:llä se täyttää tämän velvoitteen. Suunnitelmaa täydennetään valmiuslain perusteella annettavien määräysten perusteella tarvittaessa. Hyvä esimerkki tällaisesta tilanteesta on nykyinen koronapandemia, jolloin poikkeusolot tulivat voimaan Suomessa 16. maaliskuuta ja päättyivät 16. kesäkuuta (Valtioneuvosto, 2020). THL:n jatkuvuudenhallintajärjestelmä perustuu laitoksen jatkuvuudenhallinnan periaatteisiin, valmiussuunnitelmaan ja erityistilanneviestintäsuunnitelmaan. Jatkuvuussuunnitelmat on tehty erikseen toiminto- ja prosessikohtaisesti, toipumissuunnitelma löytyy palvelu- ja tietojärjestelmäkohtaisesti ja palo- ja pelastussuunnitelmat kiinteistökohtaisesti. Jatkuvuudenhallinnan periaatteissa määritetään toiminnan jatkuvuuden hallintajärjestelmä, vastuut ja toimintojen priorisointi. Se määrittelee myös jatkuvuuteen liittyvien asioiden seurannan, raportoinnin ja viestinnän. Jatkuvuussuunnittelussa kuvataan:

- ennaltaehkäisevät toimenpiteet
- toimintaohjeet erityistilanteissa
- ohjeet varamenettelyihin ja -järjestelmiin siirtymisestä
- ohjeet toimintojen hoitamisesta häiriötilanteen ja normaaliin palaamisen välisenä aikana sekä

- ohjeet palaamisesta normaalimenettelyihin ja -järjestelmiin.

Toipumissuunnitelmat on kuvattu palvelu- ja järjestelmäkohtaisesti ja ne sisältävät erityistilanneohjeet, yhteyshenkilöt, vastuutahot, menettelyt varajärjestelmiin siirtymiseksi ja palauttaminen takaisin normaalitoimintaan. Jatkuvuudenhallinnan lähtökohtana on, että laitoksen toiminta on arvioitu, suunniteltu, johdettu ja toteutettu niin, että mahdolliset häiriötilanteet ja poikkeusolot voidaan etukäteen ehkäistä. Jatkuvuussuunnitelmassa on varauduttu seuraaviin erityistilanteisiin yhteiskunnan turvallisuusstrategian mukaan (Turvallisuuskomitea, 2017) seuraavasti:

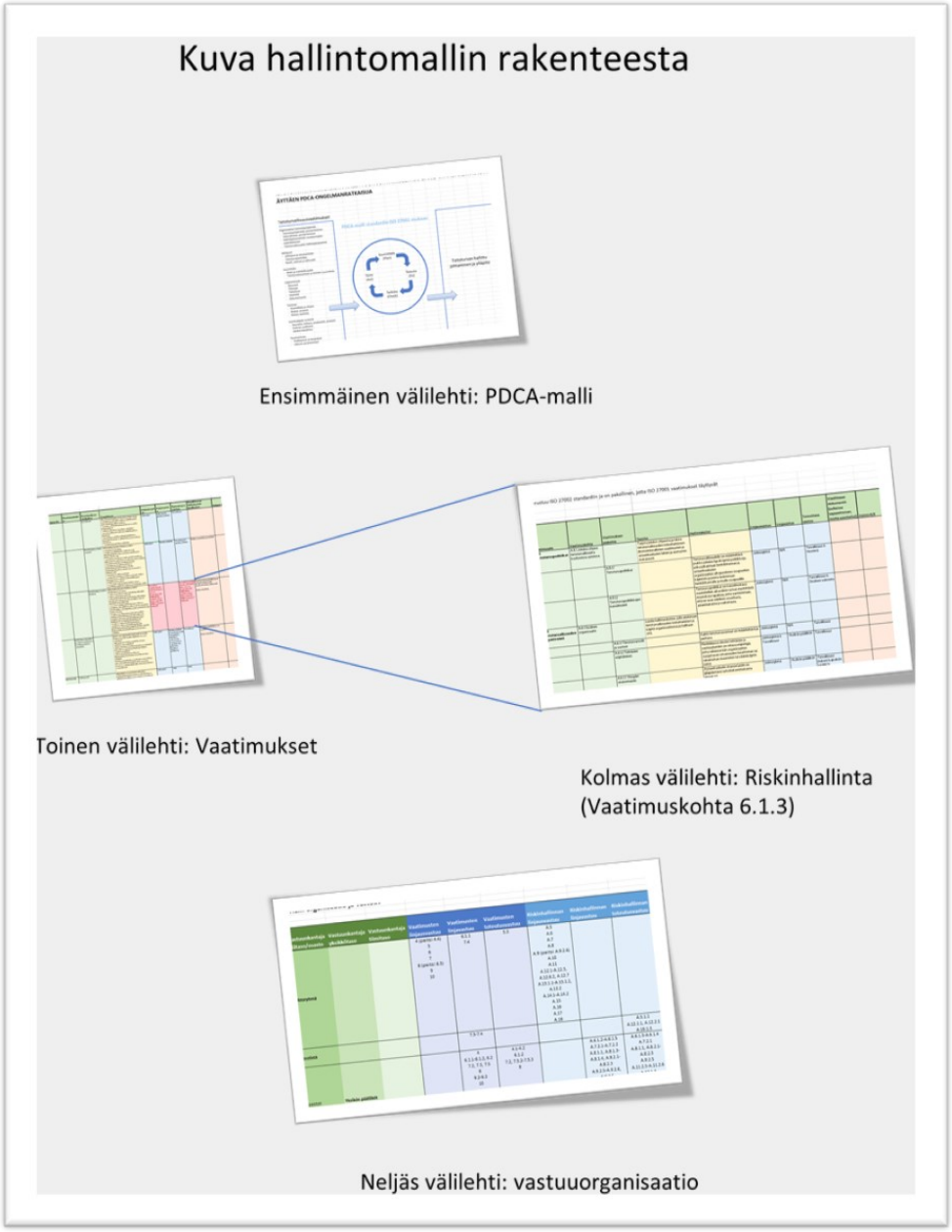
- tulipalot, vesivahingot, voimahuollon tai yhdyskuntatekniikan vakavat häiriöt, onnettomuuden, luonnon ääri-ilmiöt, ympäristöuhkat, terrorismi tai sotilaallinen voimankäyttö estää toimitilojen käytön kokonaan tai merkittävältä osin
- kuljetuslogistiikan vakavat häiriöt, elintarvikehuollon vakavat häiriöt, väestön terveyden ja hyvinvoinnin vakavat häiriöt, suuronnettomuudet, luonnon ääri-ilmiöt, ympäristöuhkat, terrorismi, muu yhteiskuntajärjestystä vaarantava rikollisuus, sotilaallisen voiman käyttö, laajat lakot tai työtaistelutoimet saavat aikaan sen, että merkittävä osa laitoksen henkilöstöstä, ylin johto tai avainhenkilöt eivät ole käytettävissä
- kyberuhkat, voimahuollon tai yhdyskuntatekniikan vakavat häiriöt, onnettomuudet, luonnon ääri-ilmiöt, terrorismi tai sotilaallinen voimankäyttö aiheuttaa tietoliikenteen tai -järjestelmän vakavan häiriön
- rahoitus- ja maksujärjestelmän vakava häiriö, voimahuollon tai yhdyskuntatekniikan vakava häiriö, onnettomuus, luonnon ääri-ilmiö, ympäristöuhka, terrorismi, sotilaallinen voimankäyttö, laaja lakko tai muu työtaistelutoimi aiheuttaa sen, että merkittävä palveluntoimittaja, vastapuoli, sidosryhmä, palvelu tms. ei ole käytettävissä. (Terho_p, 2020; Lauren_c, 2020.)

Jatkuvuussuunnitelma laaditaan aina kriittisen toiminnan näkökulmasta ja se ohjaa jatkuvuussuunnitelman sisältöä (tilaratkaisut, resurssit, reservit, varalaitteet, välineistö, IT). Jatkuvuussuunnitelmat pyritään tekemään yksikkötasolla normaaliolojen häiriötilanteiden varalle. Valmiustoiminnassa on tehty erilliset jatkuvuussuunnitelmat valmiustoiminnan vaatimusten mukaisesti. (Lauren_c, 2020.)

4 Empiirinen tutkimus ja tulokset

Tässä luvussa käsitellään tutkimuskysymysten **”Millainen hallintamalli THL:n tulisi ottaa käyttöön, jotta ISO 27001-sertifikaatin vaatimukset täyttyisivät?”** ja **”Miten tietoturvan vastuut jaetaan tietoturvastandardin mukaan?”** ratkaisuja. Tutkija selvitti ensin standardin sisältöä ja sitten THL:n nykytilaa, joista yhdessä muotoutui Excel-taulukko, joka neljine välilehtineen on ehdotettu standardinmukainen tietoturvajohtamisen hallintamalli eli haluttu lopputuotos.

Ensimmäisellä Excel-välilehdellä on kuva PDCA-ongelmaratkaisusta, jota standardi käyttää. Sitten käsitellään Excelin toinen välilehti Vaatimukset, joka kirjaa kaikki standardin vaatimukset alakohtineen ja tavoitteineen sekä ehdotuksen vastuunkantajista. Seuraavaksi käydään läpi Excelin välilehti Riskinhallinta, sillä vaatimusten kohta 6.1.3 Tietoturvariskien käsittely on laajennettu omaksi taulukokseen. Standardi käsittää riskihallinnan tärkeimmäksi alueeksi, siksi sen ohjeistus on eriytetty. Rakenne on sama kuin Vaatimukset-välilehdellä (lukuun ottamatta ylimääräistä saraketta ”Hallintakeino”). Lopuksi käydään läpi Excel-välilehti Vastuuorganisaatio, johon on koottu kaikkien vastuuryhmien omat vastuualueet standardikohdittain. Kaikki kohdat on numeroitu standardin mukaan, jotta taulukoiden käsittely olisi helpompaa. Kuva 3 selventää hallintamallin rakennetta.



Kuva 3 Luodun hallintamallin rakenne Excel-taulukossa välilehtineen

4.1 Miten hallintamalli luotiin

ISO 27001 -standardi on jaettu kahteen osaan. Ensimmäisessä osassa on lueteltu standardin tietoturvallisuusvaatimukset eli pääkohdat. Nämä ovat:

- 4 Organisaation toimintaympäristö
- 5 Johtajuus
- 6 Suunnittelu
- 7 Tukitoiminnot
- 8 Toiminta

- 9 Suorituskyvyn arviointi
- 10 Parantaminen.

Näillä vaatimuksilla on alakohtia ja alakohdan alakohtia. Kaikilla alakohdilla on kirjatut tavoitteet siitä, mitä vaatimuksella halutaan tavoittaa. Koska näitä kohtia on niin paljon, rakenne tuli selkeimmäksi kirjaamalla kaikki Excel-taulukkoon. Alla kuva 4 esimerkkinä taulukon rakenteesta. Siinä on avattu osa vaatimuskohtaa 6: Suunnittelu.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet
6 Suunnittelu	6.1 Riskien ja mahdollisuuksien käsittely		
		6.1.1 Yleistä	Ottaa huomioon kohdissa 4.1 ja 4.2 mainitut asiat ja vaatimukset ja määrittää riskit ja mahdollisuudet, joiden käsittelyn jälkeen voidaan - varmistaa, että hallintajärjestelmä voi saavuttaa halutut tulokset - estää tai vähentää ei-toivottuja vaikutuksia - parantaa jatkuvasti riskien ja mahdollisuuksien käsittelyä - suunniteltava edellämainittuihin kohdistuvia toimenpiteitä, kuinka ne yhdistetään prosesseihin ja toteutetaan - arvioida toimenpiteiden vaikutusta.
		6.1.2 Tietoturvariskien arviointi	Määritellä ja toteuttaa tietoturvariskien arviointiprosessi, jossa - laaditaan ja ylläpidetään riskikriteerejä (hyväksymiskriteerit ja arvioinnin suorittamista koskevat kriteerit) - varmistetaan toistuvien riskiarviointien tuottavan yhdenmukaisia, päteviä ja verrattavissa olevia tuloksia - tunnistetaan tietoturvariskejä luomalla arviointiprosessi, jolla kartoitetaan hallintajärjestelmään kuuluvan tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit - tunnistetaan riskien omistajat - analysoidaan tietoturvariskit arvioimalla riskien

Kuva 4 Esimerkki hallintamallin luomisesta ISO 27001 -standardin perusteella

Kun kaikki standardin kohdat oli avattu Excel-taulukkoon, siihen lisättiin vastuutahot, jotka jaettiin linjausvastuuseen (ylin vastuu), linjavastuuseen (yksikkötason vastuu) ja toteuttavaan vastuuseen (tiimitason vastuu). Alla esimerkkikuva (kuva 5) samasta kohdasta kuin edellinen kuva lisäyksen jälkeen.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu
6 Suunnittelu	6.1 Riskien ja mahdollisuuksien käsittely					
		6.1.1 Yleistä	Ottaa huomioon kohdissa 4.1 ja 4.2 mainitut asiat ja vaatimukset ja määrittää riskit ja mahdollisuudet, joiden käsittelyn jälkeen voidaan - varmistaa, että hallintajärjestelmä voi saavuttaa halutut tulokset - estää tai vähentää ei-toivottuja vaikutuksia - parantaa jatkuvasti riskien ja mahdollisuuksien käsittelyä - suunniteltava edellämainittuihin kohdistuvia toimenpiteitä, kuinka ne yhdistetään prosesseihin ja toteutetaan - arvioida toimenpiteiden vaikutusta.			

Kuva 5 Esimerkki hallintamallin luomisesta ISO 27001 -standardin perusteella lisättynä vastuutasoilla

Seuraavaksi taulukkoon lisättiin sarake ehdotetuille dokumenteille ja merkinnälle siitä, onko dokumentti jo tehty. Viimeinen sarake lisättiin valmiiksi THL:n työtä varten, eikä sitä ole tarkoitus käyttää tässä tutkimuksessa. Sen sijaan dokumenttiehdotukset-sarake on käytössä. Alla esimerkkikuva siitä, miltä taulukko näiden lisäysten jälkeen näyttää (kuva 6).

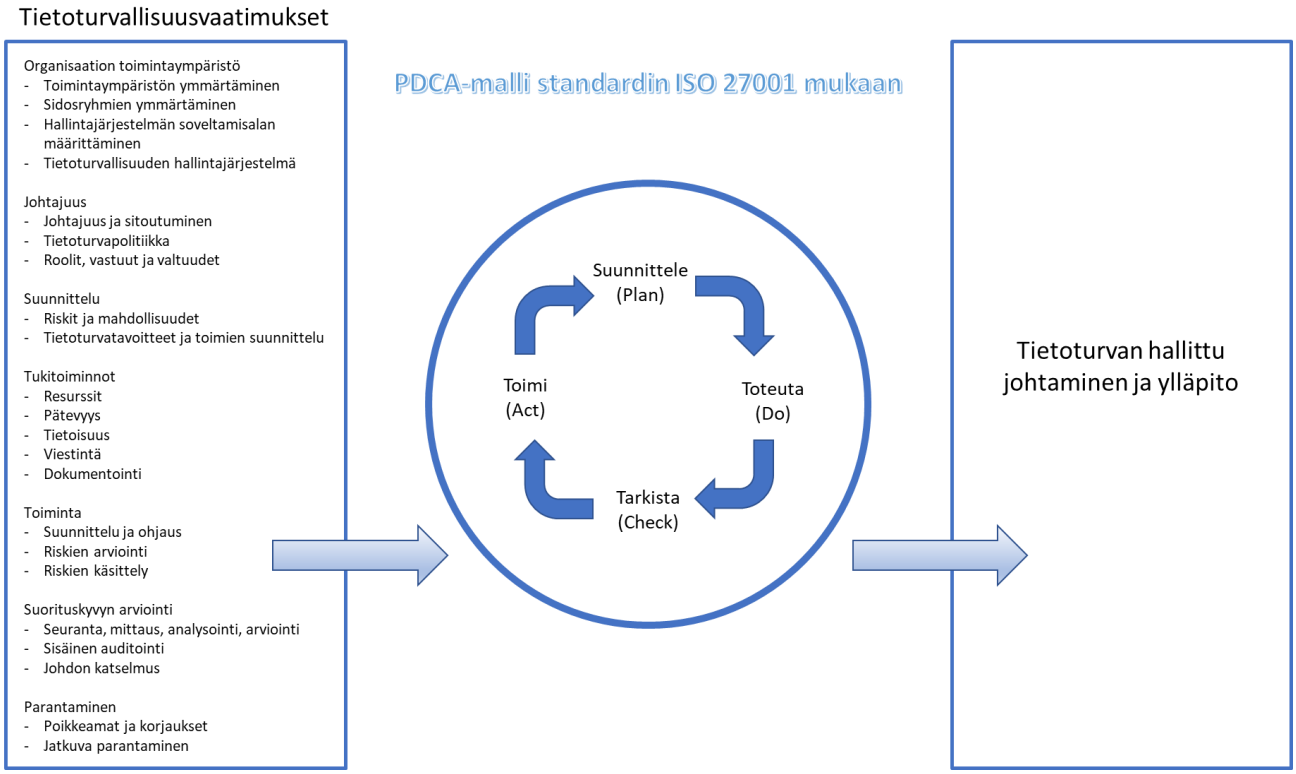
Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
6 Suunnittelu	6.1 Riskien ja mahdollisuuksien käsittely							
		6.1.1 Yleistä	Ottaa huomioon kohdissa 4.1 ja 4.2 mainitut asiat ja vaatimukset ja määrittää riskit ja mahdollisuudet, joiden käsittelyn jälkeen voidaan - varmistaa, että hallintajärjestelmä voi saavuttaa halutut tulokset - estää tai vähentää ei-toivottuja vaikutuksia - parantaa jatkuvasti riskien ja mahdollisuuksien					

Kuva 6 Esimerkki hallintamallin luomisesta ISO 27001 -standardin perusteella lisättynä vastuutasoilla, dokumenttiehdotuksilla ja valmistumissarakkeella

Molemmissa taulukoissa (vaatimukset ja riskinhallinta) käytetään samaa muotoa helppolukuisuuden varmistamiseksi. Vaatimukset on numeroitu 4–10 ja riskinhallinta A.5-A.18 kuten itse standardissa. Osa kohdista on pitkiä, joten ne on saatettu jakaa kahteen tai kolmeen erilliseen kuvaan. Ehdotettujen dokumenttien pohjana on käytetty Adviseran listaa Checklist of mandatory documentation (Advisera, 2020). Koska seuraavissa kohdissa olevien kuvien koko on rajoitettu, eikä tekstistä saa välttämättä selvää, kaikki kuvat on liitetty suurempana liitteeseen 1 samassa järjestyksessä.

4.2 Hallintamalli 1. välilehti: PDCA-malli

ISO 27001 -standardi lähestyy ISMS-hallintamallia käyttämällä yleistä ongelman ratkaisumallia ja kehittämismenetelmää nimeltä PDCA (Plan, Do, Check, Act). Se linjaa tietoturvallisuusvaatimukset, jotka jokainen erikseen suunnitellaan, toteutetaan, tarkistetaan ja tarkistuksen perusteella muutetaan tarvittavia kohtia. Näin saadaan tulokseksi hallittu tietoturvan johtaminen, mikä sisältää ylläpidon. Tämä menetelmä takaa jatkuvan iteroinnin ja hallintamallin parantamisen. Mallin auki piirretty kuva löytyy alta (kuva 7).



Kuva 7 ISO 27001 -standardin mukainen PDCA-malli

4.3 Hallintamalli 2. välilehti: standardin vaatimukset

Kohdassa 4.1 on selitetty se, miten Excel-taulukko on luotu. Tähän kappaleeseen liitetään kaikki standardin vaatimukset, jotka lisättiin taulukkoon. Ne on jaoteltu jokaisen vaatimuskohdan mukaan, jotka on numeroitu standardin mukaan. Ensimmäinen vaatimus on numero 4 ja viimeinen numero 10.

4.3.1 Kohta 4: Organisaation toimintaympäristö

Standardin vaatimusten ensimmäinen kohta on numero 4, organisaation toimintaympäristö (kuva 8). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista (joskin osittain lyhennettyjä) ja kaikille kohdille on mietitty vastuutahot. Organisaation toimintaympäristön ymmärtämiseen sisältyy myös sidosryhmien tarpeiden ja odotusten ymmärtäminen, hallintajärjestelmän sovellusalan määrittäminen ja hallintajärjestelmän luominen. Linjausvastuu on suurimmaksi osaksi johtoryhmällä, linjavastuu yksiköiden päälliköillä ja toteuttajia ovat turvallisuusosasto, yksikön päälliköt ja IT. Kohta vaatii dokumentin ”Soveltamisala” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
4 Organisaation toimintaympäristö	4.1 Organisaation ja sen toimintaympäristön		Määrittää ulkoiset ja sisäiset asiat, jotka ovat olennaisia organisaation tarkoituksen kannalta.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt	Soveltamisala (Scope)	
	4.2 Sidosryhmien tarpeiden ja odotusten ymmärtäminen		Määrittää tietoturvan kannalta olennaiset sidosryhmät ja niiden asettamat vaatimukset.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt		
	4.3 Tietoturvallisuuden hallintajärjestelmän soveltamisalan määrittäminen		Päättää tietoturvan hallintajärjestelmän rajaukset ja soveltamisalat. Otettava huomioon kohdat 4.1, 4.2 ja muut rajapinnat ja riippuvuudet.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		
	4.4 Tietoturvallisuuden hallintajärjestelmä		Luoda, toteuttaa, ylläpitää ja parantaa standardinmukainen tietoturvallisuuden hallintajärjestelmä.	N/A	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 8 ISO 27001 -standardin vaatimus 4 avattuna

4.3.2 Kohta 5: Johtajuus

Standardin seuraava vaatimuskohta on 5, johtajuus (kuva 9). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista (joskin osittain lyhennettyjä) ja kaikille kohdille on mietitty vastuutahot. Johtajuuteen sisältyy johdon sitoutuminen, tietoturvapolitiikan luominen sekä roolien, vastuiden ja valtuuksien jakaminen. Linjausvastuu on johtoryhmällä, linjavastuuta ei ole ja toteuttajia ovat turvallisuusosasto sekä roolien jakamisessa johtoryhmä yhdessä turvallisuusosaston kanssa. Kohta vaatii dokumentin ”Tietoturvapolitiikka ja sen tavoitteet” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
5 Johtajuus	5.1 Johtajuus ja sitoutuminen		Osoittaa ylimmän johdon johtajuutta ja sitoutumista tietoturvallisuuden hallintajärjestelmään: - varmistamalla tietoturvapolitiikan laatiminen, taivoitteiden asettaminen ja yhdenmukaisuus organisaation strategian kanssa - varmistamalla hallintajärjestelmän vaatimusten yhdistäminen prosesseihin - varmistamalla hallintajärjestelmää varten tarvittavat resurssit - viestimällä hallintajärjestelmän vaatimusten noudattamisen tärkeydestä - varmistamalla, että hallintajärjestelmä saavuttaa halutut tulokset - edistämällä sen jatkuvaa parantamista - tukemalla muuta johtoa heidän vastuualueillaan.	Johtoryhmä	N/A	Turvallisuus		
	5.2 Tietoturvapolitiikka		Ylimmän johdon tulee laatia tietoturvapolitiikka, joka - soveltuu organisaation toiminta-ajatukseen - sisältää tietoturvatavoitteet (yhteneväinen kohdan 6.2 kanssa) - sisältää sitoutumisen vaatimusten täyttämiseen ja hallintajärjestelmän jatkuvaan parantamiseen. Politiikan tulee olla dokumentoitu, koko organisaation tiedossa ja tarvittaessa sidosryhmien saatavilla.	Johtoryhmä	N/A	Turvallisuus	Tietoturvapolitiikka ja tarkoitus	
	5.3 Organisaation roolit, vastuut ja valtuudet		Ylimmän johdon tulee varmistaa, että tietoturvan kannalta tärkeiden roolien vastuut ja valtuudet määritellään ja että niistä viestitään, että hallintajärjestelmä on ISO 27001 -standardin vaatimusten mukainen ja että ylintä johtoa pidetään raportein ajan tasalla hallintajärjestelmän suorituskyvystä.	Johtoryhmä	N/A	Johtoryhmä & Turvallisuus		

Kuva 9 ISO 27001 -standardin vaatimus 5 avattuna

4.3.3 Kohta 6: Suunnittelu

Standardin seuraava vaatimuskohta on 6, suunnittelu (kuvat 10 ja 11). Se on jaettu kuvien mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista (joskin osittain lyhennettyjä) ja kaikille kohdille on mietitty vastuutahot. Suunnitteluun sisältyy riskien ja mahdollisuuksien käsittelyn yleiset osat ja riskien arviointi. Linjausvastuu on johtoryhmällä, linjavastuu yksiköiden päälliköillä ja osittain johtoryhmällä ja toteuttajia ovat turvallisuusosasto sekä riskien arvioinnissa yksiköiden päälliköt yhdessä turvallisuusosaston kanssa. Kohta vaatii dokumentit ”Riskien arviointi ja menetelmät”, ”Soveltuvuuslausunto”, ”Riskien käsittely”, Tietoturvapolitiikka ja sen tavoitteet” ja ”Riskien käsittely” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83. Kohta 6.1.3, tietoturvariskien käsittely, ohitetaan tässä vaiheessa, koska se on laajennettu omaksi välilehdekseen ja käsitellään laajennettuna erikseen seuraavassa luvussa 4.4.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
6 Suunnittelu	6.1 Riskien ja mahdollisuuksien käsittely							
		6.1.1 Yleistä	Ottaa huomioon kohdissa 4.1 ja 4.2 mainitut asiat ja vaatimukset ja määrittää riskit ja mahdollisuudet, joiden käsittelyn jälkeen voidaan – varmistaa, että hallintajärjestelmä voi saavuttaa halutut tulokset – estää tai vähentää ei-toivottuja vaikutuksia – parantaa jatkuvasti riskien ja mahdollisuuksien käsittelyä – suunniteltava edellämainittuihin kohdistuvia toimenpiteitä, kuinka ne yhdistetään prosesseihin ja toteutetaan – arvioida toimenpiteiden vaikutusta.	Johtoryhmä	Johtoryhmä & yksikön päälliköt	Turvallisuus		
		6.1.2 Tietoturvariskien arviointi	Määritellä ja toteuttaa tietoturvariskien arviointiprosessi, jossa – laaditaan ja ylläpidetään riskikriteerejä (hyväksymiskriteerit ja arvioinnin suorittamista koskevat kriteerit) – varmistetaan toistuvien riskiarviointien tuottavan yhdenmukaisia, päteviä ja verrattavissa olevia tuloksia – tunnistetaan tietoturvariskejä luomalla arviointiprosessi, jolla kartoitetaan hallintajärjestelmään kuuluvan tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit – tunnistetaan riskien omistajat – analysoidaan tietoturvariskit arvioimalla riskien toteutumisen ja realistinen todennäköisyys ja mahdolliset seuraukset – vertaamalla riskianalyysin tuloksia alussa mainittuihin riskikriteereihin ja priorisoimalla riskit. Dokumentoitu tieto arviointiprosesseista tulee säilyttää.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt	Riskien arviointi ja menetelmät	

Kuva 10 ISO 27001 -standardin vaatimus 6:n alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
		6.1.3 Tietoturvariskien käsittely	Määritellä ja toteuttaa tietoturvariskien käsittelyprosessi, jossa - valitaan soveltuvat riskien käsittelyvaihtoehdot riskien arvioinnin perusteella - määritetään hallintakeinot käsittelyvaihtoehtojen toteuttamiseen (organisaatio voi tehdä ne itse tai yksilöidä muista lähteistä) - verrataan valittuja hallintakeinoja erilliseen taulukkoon, ettei yhtään tarvittavaa keinoa ole jätetty pois (taulukko ei ole täydellinen, joten muitakin keinoja voidaan tarvita) - laaditaan soveltuvuuslausunto, joka sisältää edellämainitut hallintakeinot sekä erillisessä taulukossa olevat perustelut hallintakeinojen käyttämiselle tai käyttämättä jättämiselle - laaditaan riskien käsittelysuunnitelma - hankitaan riskien omistajilta hyväksyntä käsittelysuunnitelmalle ja jäljelle jääville riskeille. Dokumentoitu tieto käsittelyprosesseista tulee säilyttää.	Ks erillinen taulukko toisella välilehdellä (tulee suoraan standardista ISO 27002:2013 ja pakollisia tässä kohtaa, jotta ISO 27001 vaatimukset täyttyvät)		Ks erillinen taulukko toisella välilehdellä (tulee suoraan standardista ISO 27002:2013 ja pakollisia tässä kohtaa, jotta ISO 27001 vaatimukset täyttyvät)	Soveltuvuuslausunto (Statement of Applicability, SoA), standardin tärkein dokumentti Riskien käsittely	
	6.2 Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu		Asettaa asiaankuuluville toiminnoille ja tasoille tietoturvatavoitteet, jotka täyttävät seuraavat vaatimukset - yhdenmukaisia tietoturvapolitiikan kanssa - mitattavia, jos mahdollista - otettava huomioon soveltuvat tietoturvavaatimukset sekä riskien arvioinnin ja käsittelyn tulokset - niistä on viestittävä - niitä on päivitettävä tarvittaessa. Dokumentoitu tieto tietoturvatavoitteista tulee säilyttää. Tietoturvatavoitteiden saavuttamisen suunnittelun tulee määrittää mitä tehdään, mitä resursseja tarvitaan, vastuuhenkilöt, työn aikataulu ja tulosten arviointikeinot.	Johtoryhmä	Yksikön päälliköt (raportointivelvollisuus johdolle, ehdotukset ratkaisuista, resursseista ja rahoituksesta, johto tekee lopulliset päätökset)	Turvallisuus	Tietoturvapolitiikka ja sen tavoitteet Riskien käsittely	

Kuva 11 ISO 27001 -standardin vaatimus 6:n loppuosa avattuna

4.3.4 Kohta 7: Tukitoiminnot

Standardin seuraava vaatimuskohta on 7, tukitoiminnot (kuvat 12 ja 13). Se on jaettu kuvien mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista (joskin osittain lyhennettyjä) ja kaikille kohdille on mietitty vastuutahot. Tukitoimintoihin sisältyvät resurssien ja henkilökunnan pätevyyden listaamisen lisäksi henkilökunnan tietoisuuden kasvattaminen ja tietoturvaviestintä. Tämä kohta sisältää myös ohjeet dokumentoidun tiedon käsittelystä. Linjausvastuu on johtoryhmällä, linjavastuu osittain yksiköiden päälliköillä ja osittain johtoryhmällä ja toteuttajia ovat turvallisuusosasto, johtoryhmä, yksiköiden päälliköt ja viestintäosasto. Kohta vaatii dokumentin ”Luettelo henkilökunnan koulutuksista, taidoista, kokemuksesta ja osaamisesta” ja ei-pakolliset, mutta suositellut dokumentit ”Dokumentoidun tiedon hallintaprosessit” ja ”Dokumettienhallinnan kontrollit” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
7 Tukitoiminnot	7.1 Resurssit		Määrittää ja varata tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen tarvittavat resurssit.	Johtoryhmä	Johto	Johto		
	7.2 Pätevyys		Organisaation on - määritettävä niiden työntekijöiden pätevyysvaatimukset, joiden työ vaikuttaa tietoturvan tasoon - varmistettava pätevyys soveltavan koulutuksen, harjoittelun tai kokemuksen perusteella - hankittava tarvittaessa vaadittava pätevyys ja arvioitava toimenpiteiden vaikuttavuutta - säilytettävä asianmukaista dokumentoitua tietoa pätevyyksistä. Keinoja voivat olla esim. nykyisten työntekijöiden kouluttaminen, mentorointi, siirtäminen toisiin tehtäviin tai pätevien henkilöiden palkkaaminen tai vuokraaminen.	Johtoryhmä	Yksikön päälliköt (osaamisesta ja pätevyyksistä raportoidaan johdolle)	Turvallisuus & yksikön päälliköt (koulutukset ja osaamisarvioinnit)	Luettelo henkilökunnan koulutuksista, taidoista, kokemuksesta ja osaamisesta	
	7.3 Tietoisuus		Organisaation työntekijöiden on oltava tietoisia tietoturvapolitiikasta, miten he voivat osaltaan lisätä tietoturvaa, mitä hyötyä tietoturvan tason parantamisesta on sekä seurauksista noudattamatta jättämisestä.	Johtoryhmä	Yksikön päälliköt (turvallisuudesta vastaavien henkilöiden hyväksyttyjen ohjeiden ja linjausten mukaisesti)	Turvallisuus & Viestintä		
	7.4 Viestintä		Organisaation on määritettävä tietoturvan hallintajärjestelmän kannalta sisäistä ja ulkoista viestintää, esimerkiksi mistä viestitään, milloin, keiden kanssa, ketkä viestivät ja minkälaiset prosessit on toteutettava.	Johtoryhmä	Johtoryhmä	Turvallisuus & Viestintä		

Kuva 12 ISO 27001 -standardin vaatimus 7:n alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	7.5 Dokumentoitu tieto						(Dokumentoidun tiedon hallintaprosessit) (Dokumenttienhallinnan kontrollit)	
		7.5.1 Yleistä	Dokumentoida ISO 27001 -standardissa vaaditut tiedot ja se tieto, jonka organisaatio on määrittänyt tietoturvan hallintajärjestelmän kannalta välttämättömäksi.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & osastojen asiantuntijatahot		
		7.5.2 Dokumentoidun tiedon luominen ja päivittäminen	Varmistaa dokumentoidun tiedon asianmukainen merkintä ja kuvaus, tallennusmuoto, tallennusväline ja soveltuvuuden ja riittävyyden tarkistaminen ja hyväksyminen.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		7.5.3 Dokumentoidun tiedon hallinta	Varmistaa dokumentoidun tiedon saatavuus tarvittaessa sopivassa muodossa sekä sen asianmukainen suojaaminen (esim. ei luvatonta luovutusta, asiaton käyttö estetty, muuttumaton tieto). Dokumenttien hallinnan tulee kattaa jakelu, pääsy tietoihin, esillesaanti, käyttö, varastointi ja säilytys, muutostenhallinta, säilyttäminen ja hävittäminen. (Ulkopuolinen dokumentoitu tieto, joka on tarpeellista tietoturvan hallintajärjestelmän kannalta, on yksilöitävä ja sitä on hallittava myös.)	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		

Kuva 13 ISO 27001 -standardin vaatimus 7:n loppuosa avattuna

4.3.5 Kohta 8: Toiminta

Standardin seuraava vaatimuskohta on toiminta (kuva 14). Se on jaettu kuvien mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista (joskin osittain lyhennettyjä) ja kaikille kohdille on mietitty vastuutahot. Toimintaan suunnittelu ja ohjaus sekä tietoturvariskien arviointi ja käsittely. Linjausvastuu on osittain johtoryhmällä, linjavastuu yksiköiden päälliköillä ja toteuttajia ovat joko turvallisuusosasto tai yksiköiden päälliköt yhdessä turvallisuusosaston kanssa. Kohta vaatii dokumentit ”Riskien arvioinnin raportointi”, ”Riskien käsittely” ja ”Seurannan ja mittausten tulokset” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
8 Toiminta	8.1 Toiminnan suunnittelu ja ohjaus		Suunnitella ja toteuttaa prosessit tietoturvan vaatimusten täyttämiseksi ja kohdan 6.1 määritettyjen toimenpiteiden toteuttamiseksi, sekä ohjata niitä. Suunnitelmat on toteutettava niin, että kohdassa 6.2 määritetyt tietoturvatavoitteet saavutetaan. Dokumentoitu tieto näiden täyttämisestä on säilytettävä. Suunniteltuja muutoksia on hallittava ja arvioitava tahattomien muutosten seurauksia ja pyrittävä lieventämään haittavaikutuksia. Ulkoistetut prosessit on määritettävä ja varmistettava, että niitä valvotaan.	Johtoryhmä	Yksikön päälliköt (raportointi johdolle)	Turvallisuus (tukee) & yksikön päälliköt		
	8.2 Tietoturvariskien arviointi		Tietoturvariskien arviointi suunniteltuin aikavälein tai merkittäviä muutoksia ennen tai muutosten jälkeen. Arvioinnin tulee täyttää kohdan 6.1.2 kriteerit. Nämä on myös dokumentoitava.	Johtoryhmä	Yksikön päälliköt (raportointi johdolle)	Turvallisuus (tukee) & yksikön päälliköt	Riskien arvioinnin ja käsittelyn raportointi	
	8.3 Tietoturvariskien käsittely		Ottaa käyttöön tietoturvariskien käsittelysuunnitelma ja dokumentoida tulokset.	N/A	Yksikön päälliköt (päätökset johdolta)	Turvallisuus (tukee) & yksikön päälliköt	Riskien käsittely Riskien arvioinnin ja käsittelyn raportointi	

Kuva 14 ISO 27001 -standardin vaatimus 8 avattuna

4.3.6 Kohta 9: Suorituskyvyn arviointi

Standardin seuraava vaatimuskohta on 9, suorituskyvyn arviointi (kuvat 15 ja 16). Se on jaettu kuvien mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista (joskin osittain lyhennettyjä) ja kaikille kohdille on mietitty vastuutahot. Suorituskyvyn arviointiin sisältyy seuranta, mittaus, analysointi, arviointi sekä auditoinnit ja johdon katselmus. Linjausvastuu on johtoryhmällä, linjavastuu yksiköiden päälliköillä yhdessä turvallisuusosaston kanssa ja toteuttajia ovat turvallisuusosasto ja joiltain kohdin sisäinen valvonta. Kohta vaatii dokumentit ”Seurannan ja mittausten tulokset”, ”Sisäinen auditoinnin prosessi”, ”Sisäisen auditoinnin tulokset”, ”Johdon katselmukset” ja ei-pakollisen mutta suositellun dokumentin ”Sisäisen auditoinnin työjärjestys” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
9 Suorituskyvyn arviointi	9.1 Seuranta, mittaus, analysointi ja arviointi		Arvioida tietoturvan tasoa ja tietoturvan hallintajärjestelmän vaikuttavuutta ja määrittää - mitä seurataan ja mitataan (ml. tietoturvaprosessit ja hallintakeinot) - millä seuranta-, mittaus-, analysointi- tai arviointimenetelmillä tulos on kelvollinen (valitut menetelmät tulee olla vertailtavia ja toistettavia ollakseen kelvollisia) - milloin seuranta ja mittaus toteutetaan - ketkä toteuttavat - milloin tulokset analysoidaan ja arvioidaan ja kenen toimesta. Todisteena seurannan ja mittaamisen tulokset on dokumentoitava.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus	Seurannan ja mittausten tulokset	
	9.2 Sisäinen auditointi		Suorittaa sisäisiä auditointeja suunnitelluin aikavälein, jotta auditointien perusteella voidaan määrittää - tietoturvan hallintajärjestelmän vaatimuksenmukaisuus ja onko se ISO 27001 -standardin mukainen - onko se toteutettu ja ylläpidetty vaikuttavasti. Organisaation tulee - suunnitella, laatia, toteuttaa ja ylläpitää auditointiohjelmia, jossa määritellään auditointien taajuus, menetelmät, vastuut, suunntteluvaatimukset ja raportointi ottaen huomioon prosessien tärkeys ja edellisten auditointien tulokset - määritellä auditointikriteerit ja soveltamisala - valita auditoijat ja suorittaa auditointiprosessit niin, että objektiivisuus ja puoluettomuus toteutuvat - varmistaa tulosten raportoinnista asiaankuuluville johdon henkilöille - säilyttää dokumentoitua tietoa tuloksista.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Sisäinen valvonta	Sisäisen auditoinnin prosessi Sisäisen auditoinnin tulokset (Sisäisen auditoinnin työjärjestys)	

Kuva 15 ISO 27001 -standardin vaatimus 9:n alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	9.3 Johdon katselmus		Varmistaa suunnitelluin aikavälein tietoturvan hallintajärjestelmän soveltuvuus, asianmukaisuus ja vaikuttavuus. Johdon katselmuksessa tulee ottaa huomioon - aiempien katselmusten määrittämien toimenpiteiden tilanne - olennaisten ulkoisten ja sisäisten asioiden muutokset - tietoturvan tasoa koskeva palaute (sisältäen poikkeamat, korjaavat toimenpiteet, seurannan ja mittauksen tulokset, auditointien tulokset ja tavoitteiden täyttyminen) - sidosryhmien antama palaute - riskiarvioiden tulokset ja riskinkäsittelysuunnitelman tilanne - jatkuvan parantamisen mahdollisuudet. Johdon katselmuksen tuloksiin on sisällyttävä päätökset jatkuvan parantamisen mahdollisuuksista sekä mahdollisista muutostarpeista. Dokumentoitu tieto johdon katselmusten tuloksista tulee säilyttää.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Sisäinen valvonta	Johdon katselmuksen tulokset	

Kuva 16 ISO 27001 -standardin vaatimus 9:n loppuosa avattuna

4.3.7 Kohta 10: Parantaminen

Standardin seuraava vaatimuskohta on 10, parantaminen (kuva 17). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista (joskin osittain lyhennettyjä) ja kaikille kohdille on mietitty vastuutahot. Parantamiseen sisältyy poikkeamat ja korjaavat toimenpiteet sekä jatkuva parantaminen. Linjausvastuu on johtoryhmällä, linjavastuu yksiköiden päälliköillä ja turvallisuusosastolla ja toteuttajia ovat turvallisuusosasto sekä osittain IT. Kohta vaatii dokumentin ”Poikkeamien korjausten tulokset” sekä ei-pakollisen mutta suositellun dokumentin ”Poikkeamien korjausten työjärjestys” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
10 Parantaminen	10.1 Poikkeamat ja korjaavat toimenpiteet		Varmistaa poikkeamien käsitteleminen seuraavasti - poikkeamaan on reagoitava ja ryhdyttävä toimiin sen hallitsemiseksi ja korjaamiseksi sekä käsiteltävä seurauksia - on arvioitava tarvittavat toimenpiteet poikkeaman syiden, toistuvuuden ja muualla esiintyvyyden estämiseksi - toteutettava tarvittavat toimenpiteet ja arvioitava niiden vaikuttavuus - tehtävä muutoksia hallintajärjestelmään, jos tarpeellista. Dokumentoitua tietoa on säilytettävä todisteena poikkeamien luonteesta, niiden johdosta tehdyistä toimenpiteistä ja korjaavien toimenpiteiden tuloksista.	Johtoryhmä	Turvallisuus & yksikön päälliköt (kaikki poikkeamatilanteet raportoidaan johdolle ja pidetään tilannekuvaa yllä)	Turvallisuus & Digitaaliset ratkaisut: IT	Poikkeamien korjausten tulokset (Poikkeamien korjausten työjärjestys)	
	10.2 Jatkuva parantaminen		Parantaa jatkuvasti tietoturvan hallintajärjestelmän soveltuvuutta, riittävyyttä ja vaikuttavuutta.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus		

Kuva 17 ISO 27001 -standardin vaatimus 10 avattuna

4.4 Hallintamalli 3. välilehti: riskinhallinta

Kohdassa 4.1 on selitetty se, miten Excel-taulukko on luotu. Tähän kappaleeseen liitetään kaikki standardin vaatimuksen 6.1.3 eritellyt kohdat, jotka liittyvät riskinhallintaan ja sen taulukkoon. Ne on jaoteltu jokaisen vaatimuskohdan mukaan, jotka on numeroitu standardissa. Ensimmäinen vaatimus on numero A.5 ja viimeinen numero A.18.

4.4.1 Kohta A.5: Tietoturvapolitiikat

Riskinhallinnan ensimmäinen vaatimuskohta on A.5, tietoturvapolitiikat (kuva 18). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Tietoturvapolitiikkoihin sisältyy johdon ohjaus, politiikkojen luominen sekä niiden katselmointi. Linjausvastuu on johtoryhmällä, linjavastuuta ei tässä tapauksessa ole ja toteuttajia ovat turvallisuusosasto sekä osittain viestintä ja sisäinen valvonta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.5 Tietoturvapolitiikat	A.5.1 Johdon ohjaus tietoturvallisuutta koskevissa asioissa		Tarjota johdon ohjausta ja tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti.						
		A.5.1.1 Tietoturvapolitiikat		Tietoturvallisuudelle on määriteltävä joukko johdon hyväksymiä politiikkoja, jotka julkaistaan henkilökunnan ja asiaankuuluvien organisaation ulkopuolisten osapuolten käyttöön ja joista tiedotetaan henkilökunnalle ja muille osapuolille.	Johtoryhmä	N/A	Turvallisuus & Viestintä		
		A.5.1.2 Tietoturvapolitiikkojen katselmointi		Tietoturvapolitiikat on katselmoitava suunniteltuin aikavälein tai kun merkittäviä muutoksia tapahtuu, jotta varmistetaan, että ne ovat edelleen soveltuvia, asianmukaisia ja vaikuttavia.	Johtoryhmä	N/A	Turvallisuus & Sisäinen valvonta		

Kuva 18 ISO 27001 -standardin riskinhallinnan kohta A.5 avattuna

4.4.2 Kohta A.6: Tietoturvallisuuden organisointi

Riskienhallinnan seuraava vaatimuskohta on A.6, tietoturvallisuuden organisointi (kuva 19). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Tietoturvallisuuden organisointiin sisältyvät roolit ja vastuut, tehtävien eriyttäminen, yhteydet viranomaisiin, projektinhallinnan tietoturva sekä mobiililaitteiden käytön ja etätyön politiikat. Linjausvastuu on johtoryhmällä osin turvallisuusosaston tukemana, linjavastuu yksiköiden päälliköillä, turvallisuusosastolla ja IT:llä ja toteuttajia ovat turvallisuusosasto sekä osittain yksiköiden päälliköt. Kohta ei vaadi dokumentteja, mutta suositeltuja dokumentteja

ovat ”Mobiililaitteiden ja etätyön politiikka” sekä ”Omien laitteiden tuomisen politiikka” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.6 Tietoturvallisuuden organisointi	A.6.1 Sisäinen organisaatio		Luoda hallintarakenne, jolla aloitetaan tietoturvallisuuden toteuttaminen ja käyttö organisaatiossa ja hallitaan sitä.						
		A.6.1.1 Tietoturvaroolit ja vastuut		Kaikki tietoturvavastuut on määriteltävä ja jaettava.	Johtoryhmä	N/A	Turvallisuus		
		A.6.1.2 Tehtävien eriyttäminen		Ristiriidassa olevien tehtävien ja vastuualueiden on oltava eriytettyjä, jotta vähennetään organisaation suojattavan omaisuuden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä.	Johtoryhmä & Turvallisuus	Yksikön päälliköt	Turvallisuus		
		A.6.1.3 Yhteydet viranomaisiin		Asiaankuuluviin viranomaisiin on ylläpidettävä tarkoituksenmukaisia yhteyksiä.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		A.6.1.4 Yhteydet osaamisyhteisöihin		Osaamisyhteisöihin tai muihin turvallisuusasiantuntijaryhmiin ja ammatillisiin järjestöihin on ylläpidettävä tarkoituksenmukaisia yhteyksiä.	Johtoryhmä	Yksikön päälliköt	Yksikön päälliköt		
		A.6.1.5 Tietoturvallisuus projektinhallinnassa		Projektinhallinnassa on käsiteltävä tietoturvallisuutta projektin tyypistä riippumatta.	Johtoryhmä	Yksikön päälliköt	Turvallisuus		
	A.6.2 Mobiililaitteet ja etätyö		Varmistaa etätyön ja mobiililaitteiden käytön turvallisuus.						
		A.6.2.1 Mobiililaitteita koskeva politiikka		On otettava käyttöön politiikka ja sitä tukevat turvallisuuskäytännöt, joilla hallitaan mobiililaitteiden käytöstä syntyviä riskejä.	Johtoryhmä & Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Turvallisuus	(Mobiililaitteiden ja etätyön politiikka) (Omien laitteiden tuomisen politiikka)	
		A.6.2.2 Etätyö		On otettava käyttöön politiikka ja sitä tukevat turvallisuuskäytännöt, joilla suojataan etätyöpaikalla käytettyä, käsiteltyä tai säilytettävää tietoa.	Johtoryhmä & Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Turvallisuus		

Kuva 19 ISO 27001 -standardin riskinhallinnan kohta A.6 avattuna

4.4.3 Kohta A.7: Henkilöstöturvallisuus

Riskienhallinnan seuraava vaatimuskohta on A.7, henkilöstöturvallisuus (kuvat 20 ja 21). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Henkilöstöturvallisuuteen sisältyvät turvallisuus ennen työsuhteen alkua, sen aikana ja kun työsuhde päättyy tai muuttuu. Linjausvastuu on johtoryhmällä, linjavastuu osittain yksiköiden päälliköillä, osittain turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla, yksiköiden päälliköillä, ja HR:llä. Kohta vaatii dokumentin ”Turvallisuuden roolien ja vastuiden määrittely” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.7 Henkilöstöturvallisuus	A.7.1 Ennen työsuhteen alkua		Varmistaa, että työntekijät ja vuokratyöntekijät ymmärtävät velvollisuutensa ja ovat sopivia heille harkittuihin tehtäviin.						
		A.7.1.1 Taustatarkistus		Kaikkien työnhakijoiden tausta on tarkastettava asianmukaisten lakien, määräysten ja eettisten normien mukaisesti. Tarkastukset on myös suhteutettava liiketoiminnallisiin vaatimuksiin, käsiteltävän tiedon luokitukseen ja oletettuihin riskeihin.	Johtoryhmä	N/A	Turvallisuus & HR ja talous		
		A.7.1.2 Työsopimuksen ehdot		Työntekijöiden ja vuokratyöntekijöiden kanssa tehdyissä sopimuksissa on eriteltävä työntekijän tai vuokratyöntekijän ja organisaation vastuut tietoturvallisuudesta.	Johtoryhmä	N/A	Turvallisuus & HR ja talous	Turvallisuuden roolien ja vastuiden määrittely	

Kuva 20 ISO 27001 -standardin riskinhallinnan kohdan A.7 alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.7.2 Työsuhteen aikana		Varmistaa, että työntekijät ja vuokratyöntekijät ovat tietoisia tietoturvavastuistaan ja täyttävät ne.						
		A.7.2.1 Johdon vastuut		Johdon on edellytettävä, että kaikki työntekijät ja vuokratyöntekijät toimivat tietoturvallisesti organisaation olemassa olevien politiikkojen ja menettelyjen mukaisesti.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt & HR ja talous		
		A.7.2.2 Tietoturvatietoisuus, -opastus ja -koulutus		Kaikkien organisaation työntekijöiden sekä tarvittaessa vuokratyöntekijöiden on saatava asianmukainen tietoturvatietoisuusopastus ja -koulutus, ja heidän tietojaan organisaation politiikkojen ja menettelyjen muutoksista on päivitettävä säännöllisesti, mikäli se on heidän toimenkuvansa kannalta merkityksellistä.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & HR ja talous		
		A.7.2.3 Kurinpitoprosessi		Organisaatiolla on oltava muodollinen ja tiedossa oleva kurinpitoprosessi, jonka perusteella toimitaan, kun työntekijä on syyllistynyt tietoturvarikkomukseen.	Johtoryhmä	N/A	Turvallisuus & HR ja talous		
	A.7.3 Työsuhteen päättyminen tai muuttuminen		Suojata organisaation etuja osana työsuhteen päättymis- tai muutosprosessia.						
		A.7.3.1 Työsuhteen päättyminen tai vastuiden muuttuminen		On määritettävä tietoturvavastuut ja -velvollisuudet, jotka jäävät voimaan työsuhteen päättymisen tai muuttumisen jälkeen. Niistä on tiedotettava työntekijälle tai vuokratyöntekijälle ja niiden noudattaminen on varmistettava.	Johtoryhmä	N/A	Turvallisuus & HR ja talous		

Kuva 21 ISO 27001 -standardin riskinhallinnan kohdan A.7 loppuosa avattuna

4.4.4 Kohta A.8: Suojattavan omaisuuden hallinta

Riskienhallinnan seuraava vaatimuskohta on A.8, suojattavan omaisuuden hallinta (kuvat 22 ja 23). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Suojattavan omaisuuden hallintaan sisältyvät vastuu omaisuudesta luetteloimalla se, määrittelemällä sille omistajuudet ja hyväksyttävä käyttö, luokittelemalla tiedot ja ohjeistamalla tietovälineiden käytössä. Linjausvastuu on johtoryhmällä, linjavastuu osittain yksiköiden päälliköillä, osittain

turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla ja IT:llä. Kohta vaatii dokumentit ”Suojattavan omaisuuden luettelo” ja ”Suojattavan omaisuuden hyväksyttävä käyttö” sekä ei-pakolliset mutta suositellut dokumentit ”Tietojen luokittelupolitiikka” ja ”Tietovälineiden hyväksymispolitiikka” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.8 Suojattavan omaisuuden hallinta	A.8.1 Vastuu suojattavasta omaisuudesta		Yksilöidä organisaation suojattava omaisuus ja määritellä asianmukaiset suojausvastuut.						
		A.8.1.1 Suojattavan omaisuuden luetteloiminen		Tieto sekä tietoon ja tietojenkäsittelypalveluihin liittyvä suojattava omaisuus on yksilöitävä. Suojattava omaisuus on luetteloitava ja tätä luetteloa on ylläpidettävä.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt & Digitaaliset ratkaisut: IT & HR ja talous	Suojattavan omaisuuden luettelo	
		A.8.1.2 Suojattavan omaisuuden omistajuus		Omaisuusluettelossa olevalla suojattavalla omaisuudella on oltava omistaja.	Johtoryhmä	N/A	Turvallisuus & HR ja talous		
		A.8.1.3 Suojattavan omaisuuden hyväksyttävä käyttö		Tiedon sekä tietoon ja tietojenkäsittelypalveluihin liittyvän suojattavan omaisuuden hyväksyttävän käytön säännöt on yksilöitävä, dokumentoitava ja toteutettava.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Aineistot ja analytiikka & Digitaaliset ratkaisut: IT	Suojattavan omaisuuden hyväksyttävä käyttö	
		A.8.1.4 Suojattavan omaisuuden palauttaminen		Kaikkien työntekijöiden ja organisaation ulkopuolisten käyttäjien on palautettava kaikki hallussaan oleva organisaation suojattava omaisuus työtehtävän, työsuhteen tai sopimuksen päättyessä.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & HR ja talous		

Kuva 22 ISO 27001 -standardin riskinhallinnan kohdan A.8:n alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.8.2 Tietojen luokittelu		Varmistaa, että tiedon suojaustaso on riittävä. Riittävä suojaustaso määräytyy sen perusteella, miten merkittävää tieto on organisaatiolle.					(Tietojen luokittelupolitiikka)	
		A.8.2.1 Tiedon luokittelu		Tieto on luokiteltava lakisääteisten vaatimusten, tiedon arvon ja kriittisyyden sekä sen luvattoman paljastumisen tai muokkaamisen aiheuttamien vaikutusten perusteella.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		A.8.2.2 Tiedon merkintä		Tiedon merkitsemistä koskevat asianmukaiset menettelyt on laadittava ja otettava käyttöön organisaation määrittelemien tiedon luokitteluperiaatteiden mukaisesti.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		A.8.2.3 Suojattavan omaisuuden käsittely		Suojattavan omaisuuden käsittelemistä koskevat menettelyt on laadittava ja otettava käyttöön organisaation määrittelemien tiedon luokitteluperiaatteiden mukaisesti.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt		
	A.8.3 Tietovälineiden käsittely		Estää tietovälineille tallennettujen tietojen luvaton paljastuminen, muuttuminen, poistaminen tai tuhoutuminen.						
		A.8.3.1 Siirrettävien tietovälineiden hallinta		On laadittava siirrettävien tietovälineiden hallintaa koskeva asianmukainen ohjeistus organisaation määrittelemien luokitteluperiaatteiden mukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.8.3.2 Tietovälineiden hävittäminen		Tarpeettomat tietovälineet on hävitettävä turvallisella tavalla muodollisten menettelyjen mukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tietovälineiden hävittämispolitiikka)	
		A.8.3.3 Fyysisten tietovälineiden siirtäminen		Tietoa sisältävät tietovälineet on suojattava luvattomalta pääsyltä, väärinkäytöltä ja turmeltumiselta siirron aikana.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 23 ISO 27001 -standardin riskinhallinnan kohdan A.8 loppuosa avattuna

4.4.5 Kohta A.9: Pääsynhallinta

Riskienhallinnan seuraava vaatimuskohta on A.9, pääsynhallinta (kuvat 24 ja 25). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Pääsynhallintaan sisältyvät pääsynhallintapolitiikka, pääsyoikeuksien hallinta ja käyttäjän vastuut. Linjausvastuu on johtoryhmällä ja osin turvallisuusosastolla, linjavastuu osittain yksiköiden päälliköillä, osittain turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla, yksiköiden päälliköillä ja IT:llä, paitsi tunnisteiden käyttö koko organisaatiolla. Kohta vaatii dokumentin ”Pääsynhallintapolitiikka” ja ei-pakollisen mutta suositeltavan dokumentin ”Salasanapolitiikka” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.9.4 Järjestelmien ja sovellusten pääsynhallinta		Estää luvaton pääsy järjestelmiin ja sovelluksiin.						
		A.9.4.1 Tietoihin pääsyn rajoittaminen		Pääsyä tietoihin ja sovellusjärjestelmien toimintoihin on rajoitettava pääsynhallintapolitiikan mukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.9.4.2 Turvallinen kirjautuminen		Pääsyä järjestelmään ja sovelluksiin on hallittava turvallisella kirjautumismenettelyllä, kun pääsynhallintapolitiikassa niin velvoitetaan.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.9.4.3 Salasanojen hallintajärjestelmä		Salasanojen hallintajärjestelmän on oltava vuorovaikutteinen, ja sen on edellytettävä vahvojen salasanojen käyttöä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Salasanapolitiikka)	
		A.9.4.4 Ylläpito- ja hallintasovellukset		Järjestelmän ja sovellusten hallintakeinot ohittamaan kykenevien apuohjelmien käyttöä on rajoitettava, ja niitä on hallittava tarkasti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.9.4.5 Lähdekoodin suojaaminen pääsynvalvonnalla		Pääsyä ohjelmien lähdekoodeihin on rajoitettava.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT & Kehittäminen ja ohjaus		

Kuva 24 ISO 27001 -standardin riskinhallinnan kohdan A.9 alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.9 Pääsynhallinta	A.9.1 Pääsynhallinnan liiketoiminnalliset vaatimukset		Hallita pääsyä tietoon ja tietojenkäsittelypalveluihin.						
		A.9.1.1 Pääsynhallintapolitiikka		Pääsynhallinnan periaatteet on laadittava, dokumentoitava ja katselmoitava liiketoiminnallisten vaatimusten ja tietoturvavaatimusten perusteella.	Johtoryhmä		Turvallisuus & Digitaaliset ratkaisut: IT	Pääsynhallintapolitiikka	
		A.9.1.2 Pääsy verkkoihin ja verkkopalveluihin		Käyttäjille on sallittava pääsy ainoastaan niihin verkkoihin ja verkkopalveluihin, joihin heille on nimenomaisesti myönnetty pääsyoikeudet.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
	A.9.2 Pääsyoikeuksien hallinta		Varmistaa valtuutettujen käyttäjien pääsy järjestelmiin ja palveluihin sekä estää luvaton pääsy niihin.						
		A.9.2.1 Käyttäjien rekisteröinti ja poistaminen		On toteutettava muodollinen käyttäjien rekisteröinti- ja poistamisprosessi, jonka avulla pääsyoikeudet jaetaan.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Salasanapolitiikka)	
		A.9.2.2 Pääsyoikeuksien jakaminen		On toteutettava muodollinen pääsyoikeuksien jakoprosessi, jonka avulla kyetään antamaan tai kumoamaan pääsyoikeus minkä tahansa tyyppiseltä käyttäjältä mihin tahansa järjestelmään tai palveluun.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Salasanapolitiikka)	
		A.9.2.3 Ylläpito-oikeuksien hallinta		Ylläpito-oikeuksien jakamista ja käyttöä on rajoitettava ja valvottava.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.9.2.4 Käyttäjien tunnistautumistietojen hallinta		Tunnistautumistietojen jakamista on valvottava muodollisen hallintaprosessin avulla.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Salasanapolitiikka)	
		A.9.2.5 Pääsyoikeuksien uudelleenarviointi		Suojattavan omaisuuden omistajien on uudelleenarvioitava pääsyoikeuksia säännöllisin aikavälein.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT & yksikön päälliköt		
		A.9.2.6 Pääsyoikeuksien poistaminen tai muuttaminen		Kaikkien työntekijöiden ja organisaation ulkopuolisten osapuolten käyttäjien pääsyoikeudet tietoon ja tietojenkäsittelypalveluihin on poistettava heidän työtehtävänsä, työsuhteensa tai sopimuksensa päättyessä tai pääsyoikeuksia on muutettava muutosten mukaisesti.	Turvallisuus	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 25 ISO 27001 -standardin riskinhallinnan kohdan A.9 loppuosa avattuna

4.4.6 Kohta A.10: Salaus

Riskienhallinnan seuraava vaatimuskohta on A.10, salaus (kuva 26). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Salaukseen sisältyvät salauksen käytön periaatteet ja salausavainten hallinta. Linjausvastuu on johtoryhmällä, linjavastuu turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla ja IT:llä. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.10 Salaus	A.10.1 Salauksen hallinta		Varmistaa salauksen asianmukainen ja vaikuttava käyttö, jotta tiedon luottamuksellisuutta, aitoutta ja eheyttä kyetään suojaamaan.						
		A.10.1.1 Salauksen käytön periaatteet		On laadittava ja toteutettava politiikka, jota noudatetaan, kun tietoa suojataan salauksen avulla.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.10.1.2 Salausavainten hallinta		Salausavainten käytöstä, suojaamisesta ja käyttöiästä on laadittava politiikka, ja tätä politiikkaa on noudatettava salausavainten koko käyttöiän ajan.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 26 ISO 27001 -standardin riskinhallinnan kohta A.10 avattuna

4.4.7 Kohta A.11: Fyysinen turvallisuus ja ympäristön turvallisuus

Riskienhallinnan seuraava vaatimuskohta on A.11, fyysinen ja ympäristön turvallisuus (kuvat 27 ja 28). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Fyysiseen ja ympäristön turvallisuuteen sisältyvät turva-alueet ja laitteet. Linjausvastuu on johtoryhmällä, linjavastuu turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla, yksiköiden päälliköillä ja IT:llä, paitsi ilman valvontaa jäävät laitteet ja puhtaan pöydän ja näytön periaate koko organisaatiolla. Kohta ei vaadi dokumentteja, mutta ei-pakolliset mutta suositeltavat dokumentit ”Turva-alueilla työskentelyn menettelyohje”, ”Tietovälineiden hävittämispolitiikka” ja ”Puhtaan pöydän ja näytön periaatteen ohje” osoittaisivat standardinmukaisuuden. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.11 Fyysinen turvallisuus ja ympäristön turvallisuus	A.11.1 Turva-alueet		Estää luvaton tunkeutuminen organisaation tietoaineistoihin ja tietojenkäsittelypalveluihin sekä estää niiden vahingoittuminen ja toiminnan häiriintyminen.						
		A.11.1.1 Fyysinen turva-alue		Turva-alueet on määriteltävä ja niitä on noudatettava paikoissa, jotka sisältävät joko arkaluonteisia tai kriittisiä tietoja ja tietojenkäsittelypalveluita.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.11.1.2 Kulunvalvonta		Turva-alueet on suojattava asianmukaisella kulunvalvonnalla, jotta varmistetaan, että vain luvan saaneet henkilöt pääsevät alueelle.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.11.1.3 Toimistojen, tilojen ja laitteistojen suojaus		Toimistojen, tilojen ja laitteistojen fyysinen turvallisuus on suunniteltava ja toteutettava.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.11.1.4 Suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan		On suunniteltava ja toteuttava fyysiset suojakeinot luonnonkatastrofien, vihamielisten hyökkäysten tai onnettomuuksien varalta.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.11.1.5 Turva-alueilla työskentely		On suunniteltava ja toteutettava menettelyt, joiden mukaisesti turva-alueilla työskennellään.	Johtoryhmä	Turvallisuus	Turvallisuus	(Turva-alueilla työskentelyn menettelyohje)	
		A.11.1.6 Toimitus- ja kuormausalueet		Kulkualueita, kuten toimitus- ja kuormausalueita, sekä muita pisteitä, joiden kautta luvattomat henkilöt saattavat päästä tiloihin, on valvottava, ja ne on mahdollisuuksien mukaan eristettävä tietojenkäsittelypalveluista, jotta niihin ei pääse luvatta.	Johtoryhmä	Turvallisuus	Turvallisuus		

Kuva 27 ISO 27001 -standardin riskinhallinnan kohdan A.11 alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.11.2 Laitteet		Estää omaisuuden katoaminen, vahingoittuminen, varastaminen tai vaarantuminen sekä organisaation toimintojen keskeytyminen.						
		A.11.2.1 Laitteiden sijoitus ja suojaus		Laitteistot on sijoitettava ja suojattava siten, että ympäristöuhkien ja luvattoman tunkeutumisen riskejä pienennetään.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.11.2.2 Peruspalvelut		Laitteet on suojattava sähkökatkoilta ja muilta peruspalveluiden vikojen aiheuttamilta häiriöiltä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.11.2.3 Kaapeloinnin turvallisuus		Sähkökaapelointi sekä tietoa siirtävä tai tietotekniikkapalveluita tukeva tietoliikennekaapelointi on suojattava salakuuntelulta, häirinnältä ja vahingoittumiselta.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.11.2.4 Laitteiden huolto		Laitteet on huollettava asianmukaisesti, jotta niiden jatkuva käytettävyys ja eheys voidaan varmistaa.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.11.2.5 Suojattavan omaisuuden poistaminen		Laitteita, tietoaineistoja tai ohjelmistoja ei saa poistaa toimipaikalta ilman ennalta saatua valtuutusta.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & yksikön päälliköt		
		A.11.2.6 Toimitilojen ulkopuolelle vietyjen laitteiden ja suojattavan omaisuuden turvallisuus		Toimitilojen ulkopuolella olevan suojattavan omaisuuden turvallisuus on varmistettava. Tässä on otettava huomioon, että organisaation tilojen ulkopuolella työskentelyyn liittyvät riskit ovat erilaisia.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & yksikön päälliköt		
		A.11.2.7 Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen		Kaikki laitteiden tallennettua tietoa sisältävät osat on tarkistettava, jotta voidaan varmistua siitä, että arkaluonteinen tieto ja tekijänoikeuden suojaamat ohjelmistot on poistettu tai tuhottu turvallisesti ennen laitteen käytöstä poistamista tai kierrättämistä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tietovälineiden hävittämispolitiikka)	
		A.11.2.8 Ilman valvontaa jäävät laitteet		Käyttäjien on varmistettava, että ilman valvontaa jäävät laitteet on suojattu asianmukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & koko		
		A.11.2.9 Puhtaan pöydän ja puhtaan näytön periaate		On otettava käyttöön papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän periaate sekä tietojenkäsittelypalveluja koskeva puhtaan näytön periaate.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & koko organisaatio	(Puhtaan pöydän ja näytön periaatteen ohje)	

Kuva 28 ISO 27001 -standardin riskinhallinnan kohdan A.11 loppuosa avattuna

4.4.8 Kohta A.12: Käyttöturvallisuus

Riskienhallinnan seuraava vaatimuskohta on A.12, käyttöturvallisuus (kuvat 29, 30 ja 31). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Käyttöturvallisuuteen sisältyvät toimintaohjeet ja velvollisuudet, haittaohjelmilta suojautuminen, varmuuskopiointi, kirjaaminen ja seuranta, ohjelmistojen hallinta, teknisten haavoittuvuuksien hallinta ja tietojärjestelmien auditointi. Linjausvastuu on osin johtoryhmällä ja osin turvallisuusosastolla, linjavastuu osittain yksiköiden päälliköillä, osittain turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla, yksiköiden päälliköillä, viestinnällä ja IT:llä. Kohta vaatii dokumentin ”IT:n hallinnoinnin toimintaohjeet” ja ”Käyttäjätapahtumien, poikkeamien ja tietoturvatapahtumien loki” sekä ei-pakolliset mutta suositeltava dokumentti ”Muutoksenhallinnan politiikka” ja ”Varmuuskopiointipolitiikka” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.12 Käyttöturvallisuus	A.12.1 Toimintaohjeet ja velvollisuudet		Varmistaa tietojenkäsittelypalvelujen asianmukainen ja turvallinen toiminta.						
		A.12.1.1 Dokumentoidut toimintaohjeet		Toimintaohjeet on dokumentoitava ja niiden on oltava kaikkien niitä tarvitsevien käyttäjien saatavilla.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Viestintä	IT:n hallinnoinnin toimintaohjeet	
		A.12.1.2 Muutoksenhallinta		Tietoturvallisuuteen vaikuttavia organisaatioon, liiketoimintaprosesseihin ja tietojenkäsittelypalveluihin ja -järjestelmiin tehtäviä muutoksia on hallittava.	Johtoryhmä	Turvallisuus	Turvallisuus	(Muutoksenhallinnan politiikka)	
		A.12.1.3 Kapasiteetinhallinta		Resurssien käyttöä on tarkkailtava ja säädettävä ja on tehtävä ennusteita tulevista kapasiteettivaatimuksista, jotta voidaan varmistaa, että järjestelmän suorituskyky vastaa vaadittua.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT & yksikön päälliköt		
		A.12.1.4 Kehitys-, testaus- ja tuotantoympäristöjen erottaminen		Kehitys-, testaus- ja tuotantoympäristöt on erotettava toisistaan, jotta pienennetään tuotantoympäristön luvattoman käytön tai muuttamisen riskiä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & Kehittäminen ja ohjaus		
	A.12.2 Haittaohjelmilta suojautuminen		Varmistaa, että tiedot ja tietojenkäsittelypalvelut on suojattu haittaohjelmilta.						
		A.12.2.1 Haittaohjelmilta suojautuminen		Haittaohjelmilta suojaavat havaitsemis-, esto- ja palautusmekanismit on toteutettava, ja käyttäjien tietoisuutta haittaohjelmista on ylläpidettävä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & Viestintä		
	A.12.3 Varmuuskopiointi		Suojautua tiedon menettämiseltä.						
		A.12.3.1 Tietojen varmuuskopiointi		Tiedoista, ohjelmistoista ja järjestelmistä on otettava säännöllisesti varmuuskopiot, jotka on testattava sovittujen varmuuskopiointiperiaatteiden mukaisesti.	Johtoryhmä	Turvallisuus	Digitaaliset ratkaisut: IT	(Varmuuskopiopolitiikka)	

Kuva 29 ISO 27001 -standardin riskinhallinnan kohdan A.12 alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.12.4 Kirjaaminen ja seuranta		Tallentaa tapahtumat ja luoda seurantatietoa.						
		A.12.4.1 Tapahtumien kirjaaminen		On luotava tapahtumalokeja, joihin tallennetaan käyttäjien suorittamat toiminnot sekä tapahtuneet poikkeamat, virheet ja tietoturvatapahtumat. Nämä lokit on säilytettävä ja niitä on katselmoitava säännöllisesti.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Käyttäjätapahtumien, poikkeamien ja tietoturvatapahtumien loki	
		A.12.4.2 Lokitietojen suojaaminen		Lokitiedot ja niiden kirjauspalvelut on suojattava peukaloimiselta ja luvaton pääsy niihin on estettävä.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.12.4.3 Pääkäyttäjä- ja operaattorilokit		Järjestelmän pääkäyttäjien ja operaattorien toiminnoista on pidettävä lokia. Nämä lokit on suojattava ja niitä on katselmoitava säännöllisesti.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Käyttäjätapahtumien, poikkeamien ja tietoturvatapahtumien loki	
		A.12.4.4 Kellojen synkronointi		Kaikkien samassa organisaatiossa tai samalla turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on asetettava saman viiteaikalähteen mukaisesti.	N/A	Turvallisuus	Digitaaliset ratkaisut: IT		
	A.12.5 Tuotantokäytössä olevien ohjelmistojen hallinta		Varmistaa tuotantokäytössä olevien järjestelmien eheys.						
		A.12.5.1 Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin		On luotava menettelyt, joilla valvotaan ohjelmistojen asentamista tuotantokäytössä oleviin järjestelmiin.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 30 ISO 27001 -standardin riskinhallinnan kohdan A.12 keskiosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.12.6 Teknisten haavoittuvuuksien hallinta		Estää teknisten haavoittuvuuksien hyväksikäyttö.						
		A.12.6.1 Teknisten haavoittuvuuksien hallinta		Käytettävien tietojärjestelmien teknisistä haavoittuvuuksista on hankittava ajantasaista tietoa. Organisaation altistuminen näille haavoittuvuuksille on arvioitava, ja niihin liittyviin riskeihin on vastattava asianmukaisilla toimenpiteillä.	Turvallisuus	N/A	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.12.6.2 Ohjelmien asentamisen rajoittaminen		On laadittava ja otettava käyttöön käyttäjien suorittamaa ohjelmien asentamista koskevat säännöt.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
	A.12.7 Tietojärjestelmien auditointinäkökohtia		Varmistaa, että auditointitoiminnot vaikuttavat käytössä oleviin järjestelmiin mahdollisimman vähän.						
		A.12.7.1 Tietojärjestelmien auditointimekanismit		Auditointivaatimukset ja -toiminnot, jotka sisältävät tuotantokäytössä olevien järjestelmien todentamisia, on suunniteltava huolellisesti ja hyväksyttävä, jotta liiketoimintaprosesseja häiritään mahdollisimman vähän.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 31 ISO 27001 -standardin riskinhallinnan kohdan A.12 loppuosa avattuna

4.4.9 Kohta A.13: Viestintäturvallisuus

Riskienhallinnan seuraava vaatimuskohta on A.13, viestintäturvallisuus (kuvat 32 ja 33). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Viestintäturvallisuuteen sisältyvät verkon turvallisuuden hallinta ja tietojen siirtäminen. Linjausvastuu on johtoryhmällä, linjavastuu turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla ja IT:llä. Kohta vaatii dokumentin ”Turvallisuuden roolien ja vastuiden määrittely” ja ei-pakollisen mutta suositeltavan dokumentin ”Tiedonsiirtopolitiikka” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.13 Viestintäturvallisuus	A.13.1 Verkon turvallisuuden hallinta		Varmistaa verkossa liikkuvan tiedon ja sen tukena olevien tietojenkäsittelypalveluiden suojaaminen.						
		A.13.1.1 Verkon hallinta		Verkkoja on hallittava ja valvottava, jotta voidaan suojata järjestelmissä ja sovelluksissa oleva tieto.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.13.1.2 Verkkopalvelujen turvaaminen		Kaikkien verkkopalvelujen turvamekanismit, palvelutasot ja hallintavaatimukset on yksilöitävä ja sisällytettävä verkkopalvelusopimuksiin riippumatta siitä, tuotetaanko näitä palveluita organisaation sisällä vai onko ne ulkoistettu.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.13.1.3 Ryhmien eriyttäminen verkossa		Verkoissa olevat tietojenkäsittelypalvelujen, käyttäjien ja tietojärjestelmien ryhmät on eriytettävä toisistaan.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 32 ISO 27001 -standardin riskinhallinnan kohdan A.13 alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.13.2 Tietojen siirtäminen		Ylläpitää organisaation sisällä tai jonkin ulkopuolisen osapuolen kanssa siirretyn tiedon suojausta.						
		A.13.2.1 Tiedonsiirtopolitiikat ja -menettelyt		Kaikentyyppisillä viestintäpalveluilla tapahtuvaa tiedon siirtämistä on suojattava määriteltyjen tiedonsiirtopolitiikan ja tiedonsiirron menettelyiden ja hallintakeinojen avulla.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tiedonsiirtopolitiikka)	
		A.13.2.2 Tiedonsiirtoa koskevat sopimukset		Sopimusten on katettava liiketoimintatietojen turvallinen siirtäminen organisaation ja ulkopuolisten osapuolten välillä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tiedonsiirtopolitiikka)	
		A.13.2.3 Sähköinen viestintä		Sähköisesti viestittyä tietoa on suojattava asianmukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tiedonsiirtopolitiikka)	
		A.13.2.4 Salassapito- ja vaitiolositoumukset		Organisaation tiedonsuojaustarpeita kuvastavat vaatimukset salassapito- ja vaitiolositoumuksille on yksilöitävä, katselmoitava säännöllisesti ja dokumentoitava.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Turvallisuuden roolien ja vastuiden määrittely	

Kuva 33 ISO 27001 -standardin riskinhallinnan kohdan A.13 loppuosa avattuna

4.4.10 Kohta A.14: Järjestelmien hankkiminen, kehittäminen ja ylläpito

Riskienhallinnan seuraava vaatimuskohta on A.13, järjestelmien hankkiminen, kehittäminen ja ylläpito (kuvat 34, 35 ja 36). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Järjestelmien hankkimiseen, kehittämiseen ja ylläpitoon sisältyvät tietojärjestelmiä koskevat turvallisuusvaatimukset, kehitys- ja tukiprosessien turvallisuus ja testiaineisto. Linjausvastuu on osittain johtoryhmällä, linjavastuu osittain kehitysosastolla, osittain turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla, kehitysosastolla ja IT:llä. Kohta vaatii dokumentin ”Turvallisen järjestelmäsuunnittelun periaatteet” ja ei-pakollisen mutta suositeltavan dokumentin ”Muutoksenhallinnan politiikka” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.14 Järjestelmien hankkiminen, kehittäminen ja ylläpito	A.14.1 Tietojärjestelmiä koskevat turvallisuusvaatimukset		Varmistaa, että tietoturvallisuus on olennainen osa tietojärjestelmiä koko niiden elinkaaren ajan. Tähän sisältyvät myös palveluita julkisten verkkojen välityksellä tarjoavia tietojärjestelmiä koskevat turvallisuusvaatimukset.						
		A.14.1.1 Tietoturvavaatimusten analysointi ja määrittely		Tietoturvallisuuteen liittyvät vaatimukset on sisällytettävä uusia tai parannettavia tietojärjestelmiä koskeviin vaatimuksiin.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.14.1.2 Sovelluspalveluiden suojaaminen julkisissa verkoissa		Julkisten verkkojen kautta siirrettävää sovelluspalveluihin kuuluvaa tietoa on suojattava vilpilliseltä ja sopimuksen vastaiselta toiminnalta ja luvattomalta paljastumiselta ja muuttamiselta.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.14.1.3 Sovelluspalvelu-tapahtumien suojaaminen		Sovelluspalvelutapahtumiin liittyvää tietoa on suojattava, jotta estetään niiden epätäydellinen lähetys, väärään paikkaan ohjautuminen, luvaton viestien muuttaminen ja luvaton paljastuminen sekä viestin luvaton kopiointi tai toisto.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 34 ISO 27001 -standardin riskinhallinnan kohdan A.14 alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.14.2 Kehitys- ja tukiprosessien turvallisuus		Varmistaa, että tietoturvallisuutta suunnitellaan ja toteutetaan tietojärjestelmien kehittämisen elinkaaren osana.						
		A.14.2.1 Turvallisen kehittämisen politiikka		Ohjelmien ja järjestelmien kehittämistä koskevat säännöt on laadittava, ja niitä on sovellettava organisaation sisällä toteutettaviin kehitysprojekteihin.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Digitaaliset ratkaisut: IT & Kehittäminen ja ohjaus		
		A.14.2.2 Järjestelmään tehtävien muutosten hallintamenettelyt		Järjestelmiin niiden kehittämisen elinkaaren aikana tehtäviä muutoksia on hallittava muodollisilla muutostenhallintamenettelyillä.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		
		A.14.2.3 Sovellusten tekninen katselmointi käyttöalustan muutosten jälkeen		Liiketoiminnan kannalta kriittiset sovellukset on tarkistettava ja testattava käyttöalustan muutosten yhteydessä, jotta varmistetaan, ettei muutoksilla ole haitallisia vaikutuksia organisaation toimintaan tai turvallisuuteen.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Digitaaliset ratkaisut & Kehittäminen ja ohjaus		
		A.14.2.4 Ohjelmisstopakettien muutoksia koskevat rajoitukset		Ohjelmistopaketteihin tehtäviä muutoksia on vältettävä, ja ne on rajoitettava vain välttämättömiin muutoksiin, minkä lisäksi kaikkia muutoksia on hallittava tarkasti.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus	(Muutoksenhallinnan politiikka)	
		A.14.2.5 Turvallisen järjestelmäsuunnittelun periaatteet		Turvallisten järjestelmien toteuttamisen periaatteet on laadittava ja dokumentoitava. Niitä on ylläpidettävä ja niitä on sovellettava kaikkiin tietojärjestelmien kehitystoimiin.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus	Turvallisen järjesstelmäsuunnittelun periaatteet	

Kuva 35 ISO 27001 -standardin riskinhallinnan kohdan A.14 keskiosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
		A.14.2.6 Turvallinen kehitysympäristö		Organisaatioiden on luotava ja asianmukaisesti suojattava kehitysympäristö, jota hyödynnetään järjestelmän kehittämisessä ja integraatiotoimissa ja joka kattaa järjestelmän koko kehityselinkaaren.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Digitaaliset ratkaisut: IT & Kehittäminen ja ohjaus		
		A.14.2.7 Ulkoistettu kehittäminen		Organisaation on valvottava ja seurattava ulkoistettuja järjestelmän kehitystoimintoja.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		
		A.14.2.8 Järjestelmän turvallisuustestaus		Kehitystyön aikana on testattava turvallisuustoiminnallisuudet.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		
		A.14.2.9 Järjesstelmän hyväksymistestaus		Uusille tietojärjestelmille, päivityksille ja uusille versioille on laadittava hyväksymistestausohjelmat ja niihin liittyvät kriteerit.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		
	A.14.3 Testiaineisto		Varmistaa testaukseen käytettävän tiedon suojaus.						
		A.14.3.1 Testiaineiston suojaaminen		Testiaineistot on valittava huolellisesti ja niitä on suojattava ja hallittava.	N/A	Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		

Kuva 36 ISO 27001 -standardin riskinhallinnan kohdan A.14 loppuosa avattuna

4.4.11 Kohta A.15: Suhteet toimittajiin

Riskienhallinnan seuraava vaatimuskohta on A.15, suhteet toimittajiin (kuva 37). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Suhteet toimittajiin sisältävät tietoturvallisuuden toimittajasuhteissa sekä toimittajien palveluiden hallinnan. Linjausvastuu on johtoryhmällä, linjavastuu osittain yksiköiden päälliköillä, osittain turvallisuusosastolla ja IT:llä sekä toteuttava vastuu

turvallisuusosastolla, yksiköiden päälliköillä ja IT:llä. Kohta vaatii dokumentin ”Toimittajien tietoturvapolitiikka” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A. 15 Suhteet toimittajiin	A. 15.1 Tietoturvallisuus toimittajasuhteissa		Varmistaa, että organisaation toimittajien käytettävissä oleva suojattava omaisuus on suojattu.						
		A. 15.1.1 Toimittajasuhteiden tietoturvapolitiikka		Tietoturvavaatimuksista, joilla vähennetään toimittajan pääsyoikeudesta organisaation suojattavaan omaisuuteen aiheutuvia riskejä, on sovittava yhdessä toimittajan kanssa, ja ne on dokumentoitava.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt	Toimittajien tietoturvapolitiikka	
		A. 15.1.2 Toimittajasopimusten turvallisuus		Kaikki olennaiset tietoturvavaatimukset on laadittava ja hyväksyttävä jokaisen toimittajan kanssa, jolla saattaa olla pääsy organisaation tietoihin tai joka saattaa käsitellä tai viestiä näitä tietoja tai toimittaa niihin liittyviä IT-infrastruktuurin osia.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & yksikön päälliköt & Digitaaliset ratkaisut: IT		
		A. 15.1.3 Tieto- ja viestintäteknikan toimitusketju		Toimittajien kanssa tehtävien sopimusten on sisällettävä vaatimukset, joilla vastataan tieto- ja viestintäteknikkapalveluihin ja tuotteen toimitusketjuihin liittyviin tietoturvariskeihin.	Johtoryhmä	Turvallisuus	Turvallisuus & yksikön päälliköt		
	A. 15.2 Toimittajien palveluiden hallinta		Ylläpitää toimittajasopimusten mukaista sovittua tietoturvatasoa ja palveluiden toimitustasoa.						
		A. 15.2.1 Toimittajien palvelujen seuranta ja katselmointi		Organisaatioiden on säännöllisesti seurattava, katselmoitava ja auditoitava toimittajan palveluiden toimittamista.	Johtoryhmä	Turvallisuus	Turvallisuus & yksikön päälliköt & Digitaaliset ratkaisut: IT		
		A. 15.2.2 Toimittajan palveluihin tulevien muutosten hallinta		Toimittajan palvelun tarjoamista koskevia muutoksia, mukaan lukien olemassa olevan tietoturvapolitiikan, menettelyjen ja hallintakeinojen ylläpitoa ja kehitystä, on hallittava ottaen huomioon kyseisten liiketoimintatietojen, -järjestelmien ja -prosessien kriittisyys ja riskien uudelleenarviointi.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & yksikön päälliköt & Digitaaliset ratkaisut: IT		

Kuva 37 ISO 27001 -standardin riskinhallinnan kohta A.15 avattuna

4.4.12 Kohta A.16: Tietoturvahäiriöiden hallinta

Riskienhallinnan seuraava vaatimuskohta on A.16, tietoturvahäiriöiden hallinta (kuva 38). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Tietoturvahäiriöiden hallintaan sisältyvät vastuut ja menettelyt, raportointi, arviointi ja päätösten tekeminen, niihin vastaaminen, niistä oppiminen ja todisteiden kokoaminen. Linjausvastuu on johtoryhmällä, linjavastuu turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla, viestinnällä ja IT:llä, paitsi tietoturvahäiriöihin vastaaminen koko organisaatiolla. Kohta vaatii dokumentin ”Toimintaohje tietoturvahäiriöissä osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.16 Tietoturvahäiriöiden hallinta	A.16.1 Tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinta		Varmistaa, että tietoturvahäiriöiden hallinnan toimintamalli on johdonmukainen ja vaikuttava ja että siihen sisältyy myös tietoturvatapahtumista ja -heikkouksista viestiminen.						
		A.16.1.1 Vastuut ja menettelyt		On määriteltävä hallintavastuut ja luotava menettelyt, joilla taataan pikainen, tehokas ja järjestelmällinen reagointi tietoturvahäiriöihin.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.16.1.2 Tietoturvatapahtumien raportointi		Tietoturvatapahtumista on raportoitava mahdollisimman nopeasti ja asiaankuuluvaa hallintokanavaa pitkin.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.16.1.3 Tietoturvaheikkouksien raportointi		Organisaation tietojärjestelmiä ja palveluita käyttävien työntekijöiden ja vuokratyöntekijöiden on kiinnitettävä huomiota kaikkiin järjestelmissä tai palveluissa oleviin tai epäiltyihin tietoturvaheikkouksiin ja raportoitava niistä.	Johtoryhmä	Turvallisuus	Turvallisuus & Viestintä		
		A.16.1.4 Tietoturvatapahtumien arviointi ja niitä koskevien päätösten tekeminen		Tietoturvatapahtumat on arvioitava, minkä jälkeen on tehtävä päätös siitä, luokitellaanko ne tietoturvahäiriöiksi.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.16.1.5 Tietoturvahäiriöihin vastaaminen		Tietoturvahäiriöihin on reagoitava menettelyohjeen mukaisesti.	Johtoryhmä	Turvallisuus	Koko organisaatio	Toimintaohje tietoturvahäiriöissä	
		A.16.1.6 Tietoturvahäiriöistä oppiminen		Tietoturvahäiriöiden analysoinnista ja ratkaisemisesta saatua tietämystä on hyödynnettävä tulevien häiriöiden todennäköisyyden vähentämisessä ja niiden vaikutuksen pienentämisessä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.16.1.7 Todisteiden kokoaminen		Organisaation on määriteltävä ja toteutettava menettelyt todistusaineistoksi soveltuvan tiedon yksilöimiseen, keräämiseen, hankkimiseen ja säilyttämiseen.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 38 ISO 27001 -standardin riskinhallinnan kohta A.16 avattuna

4.4.13 Kohta A.17: Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia

Riskienhallinnan seuraava vaatimuskohta on A.17, liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia (kuva 39). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Jatkuvuudenhallintaan sisältyvät sen suunnittelu, toteuttaminen, katselmointi ja arviointi sekä vikasietoisuus. Linjausvastuu on johtoryhmällä, linjavastuu turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla, sisäisellä valvonnalla ja IT:llä. Kohta vaatii dokumentin ”Tietoturvan jatkuvuuden toimintaohjeet” ja ei-pakolliset mutta suositeltavat dokumentti ”Liiketoiminnan keskeytysanalyysi”, ”Tietoturvan harjoittelu- ja testaussuunnitelma”, ”Liiketoiminnan jatkuvuusstrategia” ja ”Tietoturvan katselmointi- ja arviointisuunnitelma” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.17 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia	A.17.1 Tietoturvallisuuden jatkuvuus		Tietoturvallisuuden jatkuvuuden on sisällyttävä organisaation liiketoiminnan jatkuvuuden hallintajärjestelmiin.						
		A.17.1.1 Tietoturvallisuuden jatkuvuuden suunnittelu		Organisaation on määriteltävä tietoturvallisuutta ja sen jatkuvuutta epäsuotuisissa tilanteissa koskevat vaatimukset.	Johtoryhmä	Turvallisuus	Turvallisuus	(Liiketoiminnan keskeytysanalyysi - Business impact analysis)	
		A.17.1.2 Tietoturvallisuuden jatkuvuuden toteuttaminen		Organisaation on laadittava, dokumentoitava, toteutettava ja ylläpidettävä prosesseja, menettelyjä ja hallintamekanismeja, joilla varmistetaan, että tietoturvallisuuden jatkuvuuden vaadittu taso säilyy epäsuotuisissa tilanteissa.	Johtoryhmä	Turvallisuus	Turvallisuus	Tietoturvan jatkuvuuden toimintaohjeet	
		A.17.1.3 Tietoturvallisuuden jatkuvuuden todentaminen, katselmointi ja arviointi		Organisaation on todennettava laaditut ja toteutetut tietoturvallisuuden jatkuvuuden hallintamekanismit säännöllisin aikavälein, jotta voidaan varmistaa, että ne ovat päteviä ja vaikuttavia epäsuotuisissa tilanteissa.	Johtoryhmä	Turvallisuus	Turvallisuus & Sisäinen valvonta	(Tietoturvan harjoittelu ja testaussuunnitelma) (Tietoturvan katselmointi ja	
	A.17.2 Vikasietoisuus		Varmistaa, että tietojenkäsittelypalvelut ovat saatavilla.						
		A.17.2.1 Tietojenkäsittelypalvelu-jen saatavuus		Tietojenkäsittelypalvelut on toteutettava niin vikasietoisina, että saatavuusvaatimukset täyttyvät.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Liiketoiminnan jatkuvuusstrategia)	

Kuva 39 ISO 27001 -standardin riskinhallinnan kohta A.17 avattuna

4.4.14 Kohta A.18: Vaatimustenmukaisuus

Riskienhallinnan viimeinen vaatimuskohta on A.18, vaatimustenmukaisuus (kuvat 40 ja 41). Se on jaettu kuvan mukaisesti alakohtiin ja kohtien tavoitteisiin. Nämä kohdat ovat suoraan standardista ja kaikille kohdille on mietitty vastuutahot. Vaatimustenmukaisuuteen sisältyvät lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen ja tietoturvallisuuden katselmoinnit. Linjausvastuu on johtoryhmällä, linjavastuu osittain yksiköiden päälliköillä, osittain turvallisuusosastolla ja toteuttava vastuu turvallisuusosastolla, yksiköiden päälliköillä ja IT:llä. Kohta vaatii dokumentin ”Lakisääteiset ja sopimukselliset vaatimukset” osoitukseksi standardinmukaisuudesta. Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.18 Vaatimustenmukaisuus	A.18.1 Lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen		Varmistaa aikkien tietoturvallisuuteen liittyvien lakien ja asetusten, säännösten ja sopimusten velvoitteiden sekä mahdollisten turvallisuusvaatimusten noudattaminen.						
		A.18.1.1 Sovellettavien lakisääteisten ja sopimuksellisten vaatimusten yksilöiminen		Kaikki asiaankuuluvat lakien, viranomaisten ja sopimusten asettamat vaatimukset sekä organisaation toimintamalli niiden täyttämistä varten on yksilöitävä yksiselitteisesti ja dokumentoitava sekä pidettävä ajan tasalla kutakin tietojärjestelmää ja organisaatiota varten.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus	Lakisääteiset ja sopimukselliset vaatimukset	
		A.18.1.2 Immateriaalioikeudet		On toteutettava asianmukaiset menettelyt, joilla varmistetaan, että immateriaalioikeuksiin ja tekijänoikeuksilla suojattujen ohjelmistotuotteiden käyttöön liittyviä lakien, viranomaisten ja sopimusten asettamia vaatimuksia noudatetaan.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus		
		A.18.1.3 Tallenteiden suojaaminen		Tallenteet on suojattava katoamiselta, tuhoutumiselta, väärentämiseltä, luvattomalta käytöltä ja luvattomalta levittämiseltä lakien, viranomaisten, sopimusten ja liiketoiminnan asettamien vaatimusten mukaisesti.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.18.1.4 Tietosuoja ja henkilötietojen suojaaminen		Tietosuoja ja henkilötietojen suojaus on varmistettava asiaankuuluvien lakien ja viranomaisten asettamien vaatimusten mukaisesti.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.18.1.5 Salaustekniikan hallintaa koskevat säädökset		Salaustekniikan hallintamekanismeja on käytettävä kaikkien asianmukaisten lakien, viranomaisten ja sopimusten asettamien vaatimusten mukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 40 ISO 27001 -standardin riskinhallinnan kohdan A.18 alkuosa avattuna

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.18.2 Tietoturvallisuuden katselmoinnit		Varmistaa, että tietoturvallisuus on toteutettu ja että sitä noudatetaan organisaation politiikkojen ja menettelyjen mukaisesti.						
		A.18.2.1 Tietoturvallisuuden riippumaton katselmointi		Organisaation tietoturvallisuuden toimintamalli ja sen toteuttaminen (eli tietoturvallisuuteen liittyvät hallintatavoitteet, hallintakeinot, politiikat, prosessit ja menettelyt) on katselmoitava riippumattomasti suunnitelluin aikavälein tai kun tapahtuu merkittäviä muutoksia.	Johtoryhmä	Turvallisuus	Turvallisuus (toimii yhteyshenkilönä, ulkoinen auditointi)		
		A.18.2.2 Turvallisuuspolitiikkojen ja -standardien noudattaminen		Esimiesten on säännöllisesti katselmoitava, ovatko heidän vastuualueellaan olevat tietojenkäsittelymenettelyt ja muut menettelyt tarkoituksenmukaisen turvallisuuspolitiikan ja -standardien sekä muiden mahdollisten turvallisuusvaatimusten mukaisia.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		A.18.2.3 Teknisen vaatimustenmukaisuuden katselmointi		Tietojärjestelmien vaatimustenmukaisuus organisaation tietoturvapolitiikkojen ja -standardien suhteen on katselmoitava säännöllisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Kuva 41 ISO 27001 -standardin riskinhallinnan kohdan A.18 loppuosa avattuna

4.5 Hallintamalli 4. välilehti: vastuuorganisaatio

Tällä neljännellä eli viimeisellä välilehdellä näkyy ensin taulukko, johon on kirjattu kaikki vastuunkantajat (vihreät sarakkeet) ja standardin ne kohdat, joissa kyseisellä ryhmällä on vastuu. Tummansinen tarkoittaa Vaatimukset-välilehteä ja vaaleampi sininen Riskinhallinta-välilehteä (kuvat 42, 43 ja 44). Kaikki suurennetut kuvat löytyvät alkaen sivulta 83.

Vastuunkantaja ylätaso/osasto	Vastuunkantaja yksikkötaso	Vastuunkantaja tiimitaso	Vaatimusten linjausvastuu	Vaatimusten linjavastuu	Vaatimusten toteutusvastuu	Riskinhallinnan linjausvastuu	Riskinhallinnan linjavastuu	Riskinhallinnan toteutusvastuu
Johtoryhmä			4 (paitsi 4.4) 5 6 7 8 (paitsi 8.3) 9 10	6.1.1 7.4	5.3	A.5 A.6 A.7 A.8 A.9 (paitsi A.9.2.6) A.10 A.11 A.12.1-A.12.3, A.12.6.2, A.12.7 A.13.1.1-A.13.1.2, A.13.2 A.14.1-A.14.2 A.15 A.16 A.17 A.18		
Viestintä				7.3-7.4				A.5.1.1 A.12.1.1, A.12.2.1 A.16.1.3
Osastot	Yksikön päälliköt			4 6.1.1-6.1.2, 6.2 7.2, 7.3, 7.5 8 9.2-9.3 10	4.1-4.2 6.1.2 7.2, 7.5.2-7.5.3 8		A.6.1.2-A.6.1.5 A.7.2.1-A.7.2.2 A.8.1.1, A.8.1.3- A.8.1.4, A.8.2.1- A.8.2.3 A.9.2.5-A.9.2.6, A.9.4.5 A.12.1.1, A.12.1.3, A.12.7.1 A.15.1.1, A.15.2.2 A.18.1.1-A.18.1.4, A.18.2.2	A.6.1.3-A.6.1.4 A.7.2.1 A.8.1.1, A.8.2.1- A.8.2.3 A.9.2.5 A.11.2.5-A.11.2.6 A.12.1.3 A.15.1.1-A.15.1.3, A.15.2 A.18.2.2

Kuva 42 ISO 27001 -standardin tietoturvavaatimukset ja riskinhallinta vastuittain, ensimmäinen osa

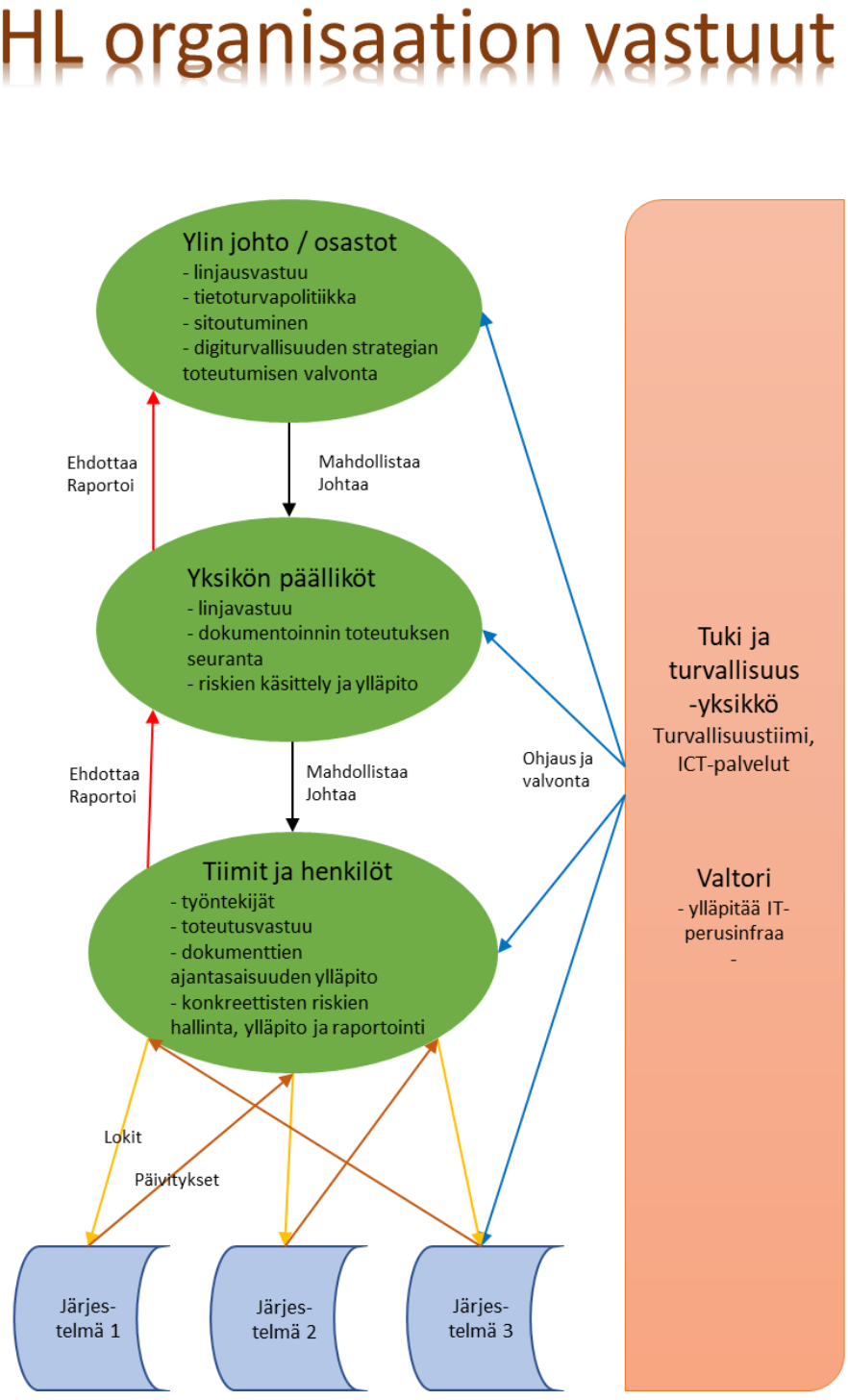
Vastuunkantaja ylätaso/osasto	Vastuunkantaja yksikkötaso	Vastuunkantaja tiimitaso	Vaatimusten linjausvastuu	Vaatimusten linjavastuu	Vaatimusten toteutusvastuu	Riskinhallinnan linjausvastuu	Riskinhallinnan linjavastuu	Riskinhallinnan toteutusvastuu
Tietopalvelut	**Digitaaliset ratkaisut**	IT-infrastruktuuri ja palvelut			4.3, 4.4 10.1		A.6.2	A.8.2.1, A.8.1.3, A.8.3 A.8.1-A.8.2, A.8.4 A.10.1.2 A.11.2 A.12.1.3-A.12.1.4, A.12.2-A.12.7 A.13 A.14.1.2-A.14.1.3, A.14.2.1, A.14.2.3, A.14.2.6 A.15.1.2, A.15.2 A.16.1.1-A.16.1.2, A.16.1.6-A.16.1.7 A.17.2.1 A.18.1.3-A.18.1.5, A.18.2.3
	Aineistot ja analytiikka							A.8.1.3
Mahdollistaja-palvelut	**HR ja talous**							A.7 A.8.1
	Kehittäminen ja ohjaus	Ohjelmistokehitys					A.14.2, A.14.3 A.15.1.2	A.9.4.5 A.12.1.4 A.14.2, A.14.3

Kuva 43 ISO 27001 -standardin tietoturvavaatimukset ja riskinhallinta vastuittain, toinen osa

Vastuunkantaja ylätaso/osasto	Vastuunkantaja yksikkötaso	Vastuunkantaja tiimitaso	Vaatimusten linjausvastuu	Vaatimusten linjavastuu	Vaatimusten toteutusvastuu	Riskinhallinnan linjausvastuu	Riskinhallinnan linjavastuu	Riskinhallinnan toteutusvastuu
	Tuki ja turvallisuus	**Turvallisuus**		9 10	4 5 6.1.1-6.1.2, 6.2 7.2-7.5 8 9 10	A.6.1.2, A.6.2 A.9.2.6 A.12.6.1	A.6.2 A.8.3 A.9.1.2, A.9.2.1- A.9.2.4, A.9.3, A.9.4.1- A.9.4.4 A.10 A.11 A.12.1.2, A.12.1.4, A.12.2-A.12.5, A.12.6.2, A.12.7 A.13 A.14.1.1-A.14.1.2 A.15.1.2-A.15.1.3, A.15.2 A.16 A.17 A.18	A.5.1 A.6.1.1-A.6.1.3, A.6.1.5, A.6.2 A.7 A.8 A.9.1-A.9.2, A.9.4 A.10 A.11 A.12.1-A.12.2, A.12.4- A.12.7 A.13 A.15 A.16.1.1-A.16.1.4, A.16.1.6-A.16.1.7 A.17 A.18
Sisäinen valvonta					9.2-9.3			A.5.1.2 A.17.1.3
Koko organisaatio								A.9.3.1 A.11.2.8-A.11.2.9 A.16.1.5

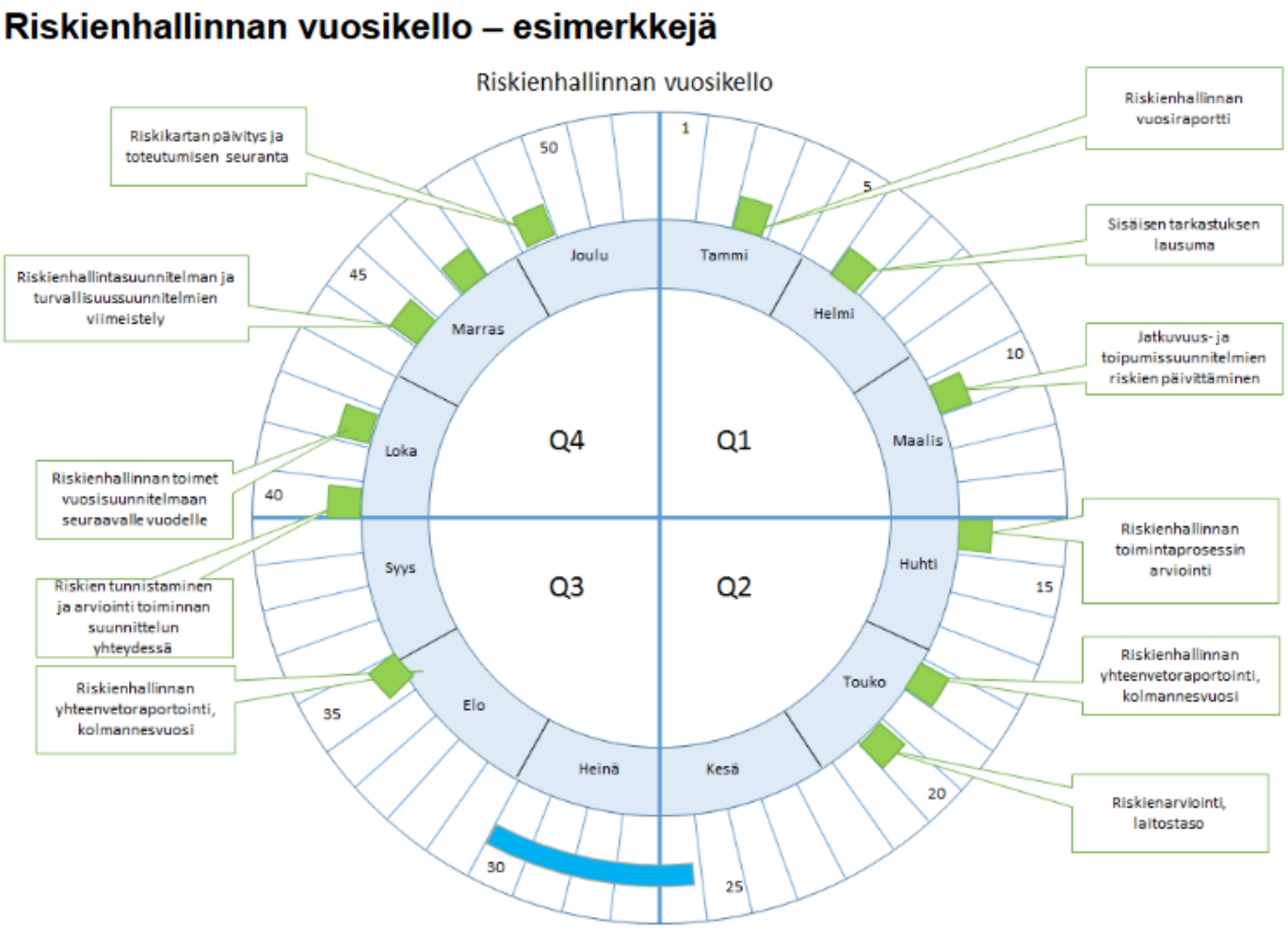
Kuva 44 ISO 27001 -standardin tietoturvavaatimukset ja riskinhallinta vastuittain, kolmas ja viimeinen osa

Välilehdellä seuraavana näkyy kuva 45, johon on kuvattu yhteenvetona kaikki vastuut organisaatiossa, sisältäen tukipalvelut ja prosessit tekijöiden välillä. Kuva on yhteenveto muista välilehdistä ja tarkoitettu hahmottamaan asiaa paremmin.



Kuva 45 THL:n organisaation vastuut kuvana

Välilehdellä viimeisenä on ehdotus tietoturvatapahtumien vuosikelloksi. Ehdotus on poimittu suoraan VAHTI-ohjeistuksen 1/2017 luonnoksesta (kuva 46). Vuosikellon avulla taataan tietoturvan parantaminen vuosi vuodelta.



Kuva 46 Ehdotus vuosikelloksi (Lausuntopalvelu, 2016.)

5 TULOSTEN ANALYSOINTI JA POHDINTAA

Tämä tutkimus alkoi kahdesta tarpeesta: tutkija halusi löytää mahdollisimman mielenkiintoisen aiheen pro graduaan varten ja THL tarvitsi jonkun laittamaan ISO 27001 -sertifioinnin alulle. Molemmat voittivat, sillä tutkija löysi aiheen, joka kiinnosti häntä, hyödyttää häntä taatusti tulevaisuudessa ja mikä parasta, sille oli todellinen tilaus. Ei tarvinnut tehdä ketään kiinnostamatonta työtä vain siksi, että gradu pitää tehdä. THL puolestaan sai näkemyksen siitä, millainen standardi oikein on ja mitä kaikkea vaaditaan sertifikaatin saamiseen. Hallintamalli itsessään antaa myös toivottavasti oivan apuvälineen tietoturvan uudelleenorganisointiin.

5.1 Tutkimusmenetelmä

Tutkimusmenetelmänä käytettiin kvalitatiivista tutkimusta ja strategiana case-tutkimusta. Tämä katsottiin parhaaksi, koska tarkoituksena oli luoda tietoturvan hallintamalli juuri THL:lle, ei luoda yleispätevää mallia. Tutkimusmenetelmä sopi hyvin tapaukseen, eikä tutkija valitsisi toisin, vaikka voisikin aloittaa alusta. ISO 27001 -standardi itsessään oli tärkein asiakirja, ja sen lisäksi tutkittu viitekehys tuki näkemystä siitä, että THL on oikealla polulla. Tapauksen ymmärtäminen omassa kontekstissaan oli tutkimuksen kannalta olennaisin asia ja se toteutui hyvin.

5.2 Käytännön kokemuksia tutkimuksen aikana

Tutkija koki monia yllätyksiä tutkimuksen aikana. Ensinnäkin työ alkoi nopealla aikataululla, mutta sitten iski koronapandemia. Tutkijan suunnitelmat pitkistä päivistä kirjastoissa ja THL:n työtiloissa muuttuivat kotona yksin tekemiseksi. Tokihan työ sielläkin eteni, mutta ympäristön vaihdos silloin tällöin olisi ollut henkisesti kannustavampaa. Tietojen kerääminen vaikeutui myös jonkin verran, koska esimerkiksi pääsy THL:n intranetiin ja myös monet haastattelut piti tehdä internetin yli. Se on joskus haastavaa jopa IT-taustan omaavalle henkilölle kuten tutkijalle toimimattomien tai hitaiden yhteyksien yli.

Toiseksi ISO 27001 -standardi pääsi yllättämään. Tutkija kuvitteli ensisilmäyksellä sen olevan melko yksinkertainen, mutta kun siihen kaivautui syvemmälle, huomasikin sen rakenteen olevan paljon monimutkaisempi. Se teetti kunnolla töitä ennen aukeamistaan ja siitä tulee löytymään yllättäviä asioita vielä pitkälle tulevaisuuteen, arvioi tutkija. Toisaalta sen osaaminen tuskin tulee haittaamaan työelämässä, joten se on ollut vaivan arvoinen.

Sitten kun koronapandemiaan ja jatkuvaan kotonaoloon alkoi tottua, iski psykoterapiakeskus Vastaamon tietomurto. Varastetut tiedot ja niillä kiristäminen oli maailmanlaajuisestikin ainutlaatuinen tapahtuma ja koska se tehtiin

terveydenhoitoalan yritykseen, tutkijan työ alkoi tuntua hänestä itsestään entistä tärkeämmältä, mikä tietenkin toi uutta kannustusta.

Yksi haastavimmista asioista tutkimuksessa oli THL:n organisaation tutkiminen, jotta tietoturvan hallintamallin olisi saanut sulautettua siihen vaivattomasti. Koko THL:n organisaatio ja toiminnat uudistettiin juuri siinä vaiheessa, jolloin työ olisi kaivannut paikallaan pysyvää ja selkeää organisaatiota. Koska organisaatio elää edelleen, piti vain valita jonkin tilanteen kuva ja tutkia hallintamallia sitä vasten. Siksi tutkijasta tuntui, että vastuiden määrittäminen oli hankalaa. Yhteistyö THL:n kanssa sujui todella hyvin ja tietoturvapäällikkö oli aina valmis auttamaan ja ohjaamaan, myös silloin, kun organisaatio muuttui yön yli ja osa tutkimuksesta meni taas uusiksi.

Tutkija koki työnsä mielekkääksi ja tärkeäksi, vaikka välillä tuntui, ettei tietoa tahdo löytyä mistään. Varsinkin aikaisemmat tutkimukset olivat joko maksullisia tai täysin sivuun tämän työn aihepiiristä. Kun materiaalin oli saanut kasaan, kirjoittaminen oli loppujen lopuksi helppoa.

Kaiken kaikkiaan työ ei missään vaiheessa tuntunut ylivoimaiselta, koska tutkija on nopea kirjoittaja, jonka äidinkieli on erittäin hyvää eikä kieliopin kanssa tullut ongelmia. Suurin työ oli hallintamallin eli Excel-taulukon luomisessa, toisaalta se oli myös työn mielenkiintoisin kohta. Koko prosessista jäi tutkijalle käteen hyvä ISO 27001 -standardin osaaminen ja hallintamalli, jota voi itse käyttää hyödyksi tulevaisuudessa, koska vain nimenomaan THL:ään liittyvät osuudet voi helposti muuttaa, muuten malli on periaatteessa yleispätevä standardin suhteen.

5.3 Yhteenveto tutkimuskysymyksistä, tavoitteista ja tuloksista

Tutkimuksen tavoitteen mukainen päätutkimuskysymys oli:

”Millainen hallintamalli THL:n tulisi ottaa käyttöön, jotta ISO 27001 -sertifikaatin vaatimukset täyttyisivät?”

Ja tutkimuksen alakysymys puolestaan:

”Miten tietoturvan vastuut jaetaan tietoturvastandardin mukaan?”

Tutkimuksen alettua hallintamalli alkoi muotoutua luonnollisella tavalla Excel-taulukoksi. Hallintamalli on nelisivuinen taulukko, jossa ensimmäisellä sivulla on ISO 27001 -standardin PDCA-malli eli ongelmanratkaisumalli. Toinen sivu listaa standardin tietoturvavaatimukset ja kolmas yhden vaatimuskohdan eli riskinhallinnan erikseen, koska se standardin mukaan on koko standardin perusajatus ja ansaitsi laajennetun oman taulukkonsa. Neljännellä sivulla listattiin kaikki laitoksen organisaation tietoturvavastuulliset tahot ja ne on lisätty toiseen ja kolmanteen sivuun, neljäs sivu on lähinnä indeksisivu, josta taho voi tarkistaa, mistä kohdista hän on vastuussa. Toiselle ja kolmannelle sivulle lisättiin myös pakolliset ja suositellut asiakirjat, koska aikaa jäi pohtia niitäkin.

Tutkija on tyytyväinen lopputuotokseen eli hallintamalliin. Se on hyvä työkalu, jos ja kun THL alkaa työskennellä ISO 27001 -sertifikaatin hankkimiseksi. Se ei tarkasti kerro, miten asiat toteutetaan, mutta se ei ole standardinkaan tarkoitus. Se antaa yleiset puitteet asioiden kehittämiseksi edelleen ja on hyvä alku. THL:llä näytti olevan iso osa työstä jo periaatteessa tehtynä ja se pitää vain uudelleen järjestää ja nimetä vastuuhenkilöt, joista on jo ehdotukset hallintamallissa.

5.4 Ehdotuksia lisätutkimuksiin

Tämän tutkimuksen lopputulos on hyvä alku ISO 27001 -sertifikaatin hankkimiseksi (Lauren_f, 2020). Toki paljon työtä on vielä tehtävänä. Tutkija kartoitti eri yrityksiä, jotka auttavat maksusta sertifikaatin hankkimisessa tekemällä ensiarvioinnin ja auttamalla koko matkan ajan. Tällainen voi tulla hyvinkin kalliiksi. Tutkija kyseli muutamista yrityksistä jonkinlaista hinta-arviota, mutta hinta riippuu paljon organisaation tilasta ja koosta. Niinkin suurelle yritykselle kuin THL se voi maksaa kymmeniäkin tuhansia. Toisaalta silloin organisaatio tietää tekevänsä oikeita asioita heti ensi kerrasta alkaen.

THL:n kokoisen organisaation, jolla on erikoisen paljon sensitiivistä dataa, voisi kuvitella tarvitsevan kaksi kokopäiväistä henkilöä tekemään töitä sertifikaatin hankkimisen parissa ainakin vuoden. Eri sivustoilta löytyi aika-arviointeja, joissa mainittiin kolme kuukautta hyvin pienelle organisaatiolle, THL:n kokoinen tuntuu arvioinneissa vievän ainakin vuoden. Tietoturvapäällikkö sitä tuskin kykenee hankkimaan oman toimen ohella. Järjestelmän luomiseen kulunee vuoden verran kahdelta henkilöltä ja ylläpitoon todennäköisesti tarvitaan yksi osoitettu henkilö, sillä katselmoinnit, arviot, auditoinnit ja niiden poikimat muutokset varmistavat sen, että tekemistä riittää sertifikaatin uusimisessa ja hallintamallin ylläpidossa.

LÄHTEET

Painetut ja luottamukselliset lähteet

Hirsjärvi, S., Remes, P. & Sajavaara, P. (1997). *Tutki ja kirjoita.* (6. uud. painos). Helsinki: Tammi.

Kananen, J. (2019). *Opinnäytetyön ja pro gradun pikaopas.* Jyväskylä: Jyväskylän ammattikorkeakoulu.

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 2011/1406 (2011). Annettu Helsingissä 22.12.2011. Saatavilla sähköisesti osoitteessa https://www.finlex.fi/fi/laki/alkup/2011/20111406

Ojasalo, K., Moilanen, T., & Ritalahti, J. (2009). *Kehittämistyön menetelmät.* WSOYpro. Helsinki.

Terho_a (2019). *THL:n johtoryhmä.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 2.11.2020.

Terho_b (2018). *Johdanto tietoturvallisuuteen.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_c (2017). *Tietojärjestelmien haavoittuvuuksien hallintapolitiikka.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_d (2017). *Lokipolitiikka THL:ssä.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_e (2017). *Palomuuripolitiikka Terveyden ja hyvinvoinnin laitoksessa.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_f (2019). *Pilvipalvelut.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_g (2019). *Sallitut, erikseen sovitut ja kielletyt pilvipalvelut.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_h (2020). *Salassa pidettävien asiakirjojen luokittelu ja käsittely Terveyden ja hyvinvoinnin laitoksessa.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_i (2013). *Sähköpostin käytön periaatteet Terveyden ja hyvinvoinnin laitoksessa.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_j (2018). *Turvallisuudenhallinnan käsikirja – Security Manual.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 14.9.2020.

Terho_k (2017). *Tietoturvallinen sovelluskehitys.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_l (2018). *Tietoturvapoikkeamat ja häiriötilanteet.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_m (2018). *Tietoturva-testaukset ja tarkastukset.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_n (2019). *Turvallisuussopimusmalli ja hankintavaatimukset.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_o (2018). *Turvallisuusuhat ja -riskit.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 9.6.2020.

Terho_p (2015). *Terveyden ja hyvinvoinnin laitoksen jatkuvuudenhallinnan periaatteet.* Terveyden ja hyvinvoinnin laitoksen intranet. Pääsy vain yrityksen työntekijöiden tunnuksilla. Luettu 2.11.2020.

Elektroniset lähteet

Academic (2020). *ISO 07799.* Luettu 28.5.2020 osoitteesta https://enacademic.com/dic.nsf/enwiki/7042382

Advisera (2020). *Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 Revision).* Luettu 8.11.2020 osoitteesta https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/Checklist_of_ISO_27001_Mandatory_Documentation_EN.pdf

Baker, A. (2017). *Why ISO 27001 is 'the' standard for information security.* Luettu 7.11.2020 osoitteesta https://www.itgovernance.eu/blog/en/why-iso-27001-is-the-standard-for-information-security

BBC (2020). *Police launch homicide inquiry after German hospital hack.* Luettu 6.10. osoitteesta https://www.bbc.com/news/technology-54204356

CIO Wiki (2020). *Enterprise Information Security Architecture (EISA).* Luettu 5.11.2020 osoitteesta https://cio-wiki.org/wiki/Enterprise_Information_Security_Architecture_(EISA)

DigitalGuardian (2020). *What is NIST Compliance?* Luettu 3.11.2020 osoitteesta https://digitalguardian.com/blog/what-nist-compliance

DoD CIO (2020). *DoDAF Wiewpoints and Models.* Luettu 5.11.2020 osoitteesta https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_viewpoints/

Dutton, J. (2019). *What is an ISMS? 9 reasons why you should implement one.* Luettu 7.11.2020 osoitteesta https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one

ENISA (2019). *Standards supporting certification.* Luettu 7.11.2020 osoitteesta https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-ii/at_download/fullReport

Euroopan komissio (2017). *Resilience, Deterrence and Defence: Building strong cybersecurity in Europe.* Luettu 25.3.2020 osoitteesta https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf

Futucast (2020). *Benjamin Särkkä, Vastaamon Tietomurron Jäljillä #130.* Youtube-video katsottu 5.11.2020 osoitteesta https://www.youtube.com/watch?v=nEuIan7JTbQ

GOV.UK (2020). *Guidance: MOD Architecture Framework.* Luettu 5.11.2020 osoitteesta https://www.gov.uk/guidance/mod-architecture-framework

Helsingin yliopisto (2003). *Tietoturvahallinto ja -johtaminen: Suomen VAHTI-ohjeisto.* Luettu 3.11.2020 osoitteesta https://www.cs.helsinki.fi/u/karvi/turvahallinto03/vahti.html

ISACA_a (2020). *About us.* Luettu 22.9.2020 osoitteesta https://www.isaca.org/why-isaca/about-us

ISACA_b (2020). *State of Cybersecurity 2020.* Luettu 22.9.2020 osoitteesta https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc202

IT Governance (2020). *ISO 27001: The facts.* PDF-tiedosto ladattu 23.7.2020 osoitteesta https://www.itgovernance.co.uk/iso27001-factsheet

Koppa, Jyväskylän yliopisto (2015). *Tapaustutkimus.* Luettu 5.3.2020 osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/tapaustutkimus

Krypsys (2020). *What is ISO 27001 and why is it so important for organisations?* Luettu 7.11.2020 osoitteesta https://www.krypsys.com/iso27001/iso-27001-important-organisations/

Kyberturvallisuuskeskus_a (2019). *Luottamuksen lähteillä. Näkökulmia tietoturvan standardointiin ja sertifiointiin.* Luettu 1.11.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

Kyberturvallisuuskeskus_b (2020). *Kyberturvallisuus ja yrityksen hallituksen vastuu.* Luettu 7.11.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Laurea ammattikorkeakoulu (2020). *Katakri-pääauditoijakoulutus.* Luettu 3.11.2020 osoitteesta https://www.laurea.fi/koulutus/taydennyskoulutukset/katakri-paaauditoijakoulutus

Lausuntopalvelu (2016). *VAHTI 1/2017 Ohje riskienhallintaan – Liitteet.* Luonnosversio. Luettu 3.11.2020 osoitteesta https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?attachmentId=1971

Lehto, M., Neittaanmäki, P. (2014). *IT-alan merkitys yhteiskunnassa ja tutkimus- ja innovaatiotoiminnan kehittäminen.* Luettu 30.7.2020 osoitteesta https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/12-2014_it-alan_merkitys_netti.pdf

Magoulas, T., Hadzic, A., Saarikko, T., Pessi, K. (2012). *Alignment in Enterprise Architecture: A Comparatieve Analysis of Four Architectural Approaches.* Academic Conferences and Publishing International Limited, e-Journal of IS Evaluation EJISE, 95. Luettu 5.11.2020 osoitteesta http://www.ejise.com/volume15/issue1/p88

NIST (2015). *About NIST.* Luettu 3.11.2020 osoitteessa https://www.nist.gov/about-nist

Nixu (2017). *Why certify and what is ISO 27001?* Luettu 7.11.2020 osoitteesta https://www.nixu.com/blog/why-certify-and-what-iso-27001

Open Group (2020). *About the TOGAF Standard, Version 9.2.* Luettu 5.11.2020 osoitteesta https://www.opengroup.org/togaf

Pietikäinen, S. (2013). *Tietoturvallisuus – mitä se on?* Luettu 23.3.2020 osoitteesta https://www.vahtiohje.fi/web/guest/691

Pietikäinen, S. (2014). *Viranomaisten tietoturvallisuuden arviointi*. Luettu 23.3.2020 osoitteesta https://www.vahtiohje.fi/web/guest/730

Pro Pilvipalvelut (2020). *Tietoturvan hallinta ja johtaminen ehkäisevät turvallisuusuhkia.* Luettu 7.11.2020 osoitteesta https://www.tietoturva.pro/iso-iec-27001

Puolustusministeriö (2011). *KATAKRI: Kansallinen turvallisuusauditointikriteeristö, versio II.* Luettu 3.11.2020 osoitteesta https://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Pöyhönen, J., Lehto, M. & Lehto, M. (2019). *Kyberturvallisuus sairaalajärjestelmissä: osa2. Toiminnan kehittäminen.* Luettu 22.10.2020 osoitteesta https://www.jyu.fi/it/fi/tutkimus/julkaisut/tekes-raportteja/kyberturvallisuus_sairaalajarjestelmissa_osa_2_toiminnan_kehittaminen.pdf

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). *Triangulaatio.* Luettu 5.3.2020 osoitteesta https://www.fsd.tuni.fi/menetelmaopetus/kvali/L2_3_2_4.html

SABSA Institute (2020). *SABSA Executive Summary: What is SABSA?* Luettu 4.11.2020 osoitteesta https://sabsa.org/sabsa-executive-summary/

SFS-EN ISO/IEC 27001:2017 (2017). *Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.* Ostettu 10.2.2020 osoitteesta https://sales.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/493427.html.stx

Shariati, M., Bahmani, F., Shams, F. (2011). *Enterprise information security, a review of architectures and frameworks from interoperability perspective.* Elsevier, ScienceDirect, 539. Luettu 5.11.2020 osoitteesta https://www.sciencedirect.com/science/article/pii/S1877050910004643/pdf?md5=1819b759f9bfc6f7960b160ac9448d47&pid=1-s2.0-S1877050910004643-main.pdf

Soxlaw (2008). *The Sarbanes-Oxley Act.* Luettu 28.5.2020 osoitteesta http://www.soxlaw.com/

Suhonen, T. (2019). *Pro gradu: ISO/IEC 27001 -sertifioinnin hankintaperusteet ja sertifiointielimen valintaperusteet.* Luettu 7.11.2020 osoitteesta https://jyx.jyu.fi/bitstream/handle/123456789/65721/URN%3ANBN%3Afi%3Ajyu-201910024309.pdf

Suomidigi (2020). *VAHTI-ohjeet.* Luettu 3.11.2020 osoitteesta https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet

TechTarget (2011). *What is information security management system (ISMS).* Luettu 7.11.2020 osoitteesta https://whatis.techtarget.com/definition/information-security-management-system-ISMS

Thales_a (2020). *What are «Common Criteria»?* Luettu 28.5.2020 osoitteesta https://cpl.thalesgroup.com/faq/global-compliance/what-are-common-criteria

Thales_b (2020). *What is ISO 27799:2016?* Luettu 28.5.2020 osoitteesta https://cpl.thalesgroup.com/faq/global-compliance/what-iso-277992016

THL_a (2020). *Mikä on THL?* Luettu 24.10.2020 osoitteesta https://thl.fi/fi/thl/mika-on-thl

THL_b (2020). *Strategia.* Luettu 2.11.2020 osoitteesta https://thl.fi/fi/thl/strategia

THL_c (2020). *Organisaatio.* Luettu 2.10.2020 osoitteesta https://thl.fi/fi/thl/organisaatio

Traficom (2019). *Uusi kriteeristö ohjaa pilvipalveluiden turvalliseen käyttöön.* Luettu 3.11.2020 osoitteesta https://www.traficom.fi/fi/tilastot-ja-julkaisut/blogit/uusi-kriteeristo-ohjaa-pilvipalveluiden-turvalliseen-kayttoon

Turvallisuuskomitea (2017). *Yhteiskunnan turvallisuusstrategia: Valtioneuvoston periaatepäätös.* Luettu 2.11.2020 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Valtioneuvosto (2020). *Valmiuslain mukaisten toimivaltuuksien käytöstä luovutaan – poikkeusolot päättyvät tiistaina 16. kesäkuuta.* Luettu 2.11.2020 osoitteesta https://valtioneuvosto.fi/-/10616/valmiuslain-mukaisten-toimivaltuuksien-kaytosta-luovutaan-poikkeusolot-paattyvat-tiistaina-16-kesakuuta

Valtiovarainministeriö (2020). *Valtiovarainministeriön julkaisuja – 2020:23: Julkisen hallinnon digitaalinen turvallisuus.* Luettu 30.7.2020 osoitteesta http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162169/VM_2020_23.pdf

Wikipedia_a (2020). *Case study.* Luettu 5.3.2020 osoitteesta https://en.wikipedia.org/wiki/Case_study

Wikipedia_b (2020). *Common Criteria.* Luettu 28.5.2020 osoitteesta https://en.wikipedia.org/wiki/Common_Criteria

Wikipedia_c (2019*). Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä.* Luettu 3.11.2020 osoitteesta https://fi.wikipedia.org/wiki/Julkisen_hallinnon_digitaalisen_turvallisuuden_johtoryhm%C3%A4

YLE (2020). *Yle seurasi tietomurtotapausta: Vastaamo on ollut myös Kelan palvelutuottaja, kiristäjän verkkosivu palasi nettiin, HUSin, Tyksin, Taysin ja Kanta-Hämeen keskussairaalan asiakastietoja voinut vuotaa.* Luettu 7.11.2020 osoitteesta https://yle.fi/uutiset/3-11610267

Haastattelut

Elonsalo, Ulpu, ylilääkäri. Terveyden ja hyvinvoinnin laitos (THL), Infektiotautien torjunta ja rokotukset -yksikkö, Helsinki. Puhelinhaastattelu 6.11.2020. Aiheena esimerkki THL:n rekisterien käytöstä. Haastattelijana Tiina Virta.

Lauren_a. Laurén, Andrei, tietoturvapäällikkö. Terveyden ja hyvinvoinnin laitos (THL), Helsinki. Haastattelut THL:llä 9.1.2020, 31.1.2020 ja 9.6.2020. Aiheena aiheesta sopiminen, aiheen tarkentaminen ja ensimmäiset taustatiedot. Haastattelijana Tiina Virta.

Lauren_b. Laurén, Andrei, tietoturvapäällikkö. Terveyden ja hyvinvoinnin laitos (THL), Helsinki. Teams-haastattelu 25.5.2020 ja haastattelu THL:llä 9.6.2020. Aiheena tutkimuksen tausta. Haastattelijana Tiina Virta.

Lauren_c. Laurén, Andrei, tietoturvapäällikkö. Terveyden ja hyvinvoinnin laitos (THL), Helsinki. Teams-haastattelut 15.7.2020 ja 19.8.2020. Aiheena ISO 27001 -standardi ja THL:n nykytila. Haastattelijana Tiina Virta.

Lauren_d. Laurén, Andrei, tietoturvapäällikkö. Terveyden ja hyvinvoinnin laitos (THL), Helsinki. Teams-haastattelu 3.9.2020 ja haastattelu THL:llä 14.9.2020. Aiheena THL:n muuttuva organisaatio ja hallintamallin muoto. Haastattelijana Tiina Virta.

Lauren_e. Laurén, Andrei, tietoturvapäällikkö. Terveyden ja hyvinvoinnin laitos (THL), Helsinki. Teams-haastattelut 5.10.2020, 12.10.2020 ja 19.10.2020. Aiheena hallintamallin luominen. Haastattelijana Tiina Virta.

Lauren_f. Laurén, Andrei, tietoturvapäällikkö. Terveyden ja hyvinvoinnin laitos (THL), Helsinki. Teams-haastattelut 30.10.2020 ja 3.11.2020. Aiheena hallintamallin läpikäynti. Haastattelijana Tiina Virta.

LIITE 1 HALLINTAMALLIN SUURENNETUT KUVAT

Tämä on pro gradu -työn ensimmäinen liite. Varsinaisessa leipätekstissä olevat kuvat ovat niin pieniä, että ne on listattu tähän liitteeseen suurennettuina. Kaikki kuvat löytyvät samassa järjestyksessä tekstistä kuin tässä liitteessä. Kuvat alkavat sivulta 45. Jos joku kuvista on edelleen liian pieni, alkuperäistä Excel-taulukkoa, josta nämä kuvat on otettu, voi pyytää suoraan tutkija Tiina Virralta osoitteesta theena.stream@gmail.com.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
4 Organisaation toimintaympäristö	4.1 Organisaation ja sen toimintaympäristön		Määrittää ulkoiset ja sisäiset asiat, jotka ovat olennaisia organisaation tarkoituksen kannalta.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt	Soveltamisala (Scope)	
	4.2 Sidosryhmien tarpeiden ja odotusten ymmärtäminen		Määrittää tietoturvan kannalta olennaiset sidosryhmät ja niiden asettamat vaatimukset.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt		
	4.3 Tietoturvallisuuden hallintajärjestelmän soveltamisalan määrittäminen		Päättää tietoturvan hallintajärjestelmän rajaukset ja soveltamisalat. Otettava huomioon kohdat 4.1, 4.2 ja muut rajapinnat ja riippuvuudet.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		
	4.4 Tietoturvallisuuden hallintajärjestelmä		Luoda, toteuttaa, ylläpitää ja parantaa standardinmukainen tietoturvallisuuden hallintajärjestelmä.	N/A	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
5 Johtajuus	5.1 Johtajuus ja sitoutuminen		Osoittaa ylimmän johdon johtajuutta ja sitoutumista tietoturvallisuuden hallintajärjestelmään: - varmistamalla tietoturvapolitiikan laatiminen, tavoitteiden asettaminen ja yhdenmukaisuus organisaation strategian kanssa - varmistamalla hallintajärjestelmän vaatimusten yhdistäminen prosesseihin - varmistamalla hallintajärjestelmää varten tarvittavat resurssit - viestimällä hallintajärjestelmän vaatimusten noudattamisen tärkeydestä - varmistamalla, että hallintajärjestelmä saavuttaa halutut tulokset - edistämällä sen jatkuvaa parantamista - tukemalla muuta johtoa heidän vastuualueillaan.	Johtoryhmä	N/A	Turvallisuus		
	5.2 Tietoturvapolitiikka		Ylimmän johdon tulee laatia tietoturvapolitiikka, joka - soveltuu organisaation toiminta-ajatukseen - sisältää tietoturvatavoitteet (yhteneväinen kohdan 6.2 kanssa) - sisältää sitoutumisen vaatimusten täyttämiseen ja hallintajärjestelmän jatkuvaan parantamiseen. Politiikan tulee olla dokumentoitu, koko organisaation tiedossa ja tarvittaessa sidosryhmien saatavilla.	Johtoryhmä	N/A	Turvallisuus	Tietoturvapolitiikka ja tarkoitus	
	5.3 Organisaation roolit, vastuut ja valtuudet		Ylimmän johdon tulee varmistaa, että tietoturvan kannalta tärkeiden roolien vastuut ja valtuudet määritellään ja että niistä viestitään, että hallintajärjestelmä on ISO 27001 -standardin vaatimusten mukainen ja että ylintä johtoa pidetään raportein ajan tasalla hallintajärjestelmän suorituskyvystä.	Johtoryhmä	N/A	Johtoryhmä & Turvallisuus		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
6 Suunnittelu	6.1 Riskien ja mahdollisuuksien käsittely							
		6.1.1 Yleistä	Ottaa huomioon kohdissa 4.1 ja 4.2 mainitut asiat ja vaatimukset ja määrittää riskit ja mahdollisuudet, joiden käsittelyn jälkeen voidaan - varmistaa, että hallintajärjestelmä voi saavuttaa halutut tulokset - estää tai vähentää ei-toivottuja vaikutuksia - parantaa jatkuvasti riskien ja mahdollisuuksien käsittelyä - suunniteltava edellämainittuihin kohdistuvia toimenpiteitä, kuinka ne yhdistetään prosesseihin ja toteutetaan - arvioida toimenpiteiden vaikutusta.	Johtoryhmä	Johtoryhmä & yksikön päälliköt	Turvallisuus		
		6.1.2 Tietoturvariskien arviointi	Määritellä ja toteuttaa tietoturvariskien arviointiprosessi, jossa - laaditaan ja ylläpidetään riskikriteerejä (hyväksymiskriteerit ja arvioinnin suorittamista koskevat kriteerit) - varmistetaan toistuvien riskiarviointien tuottavan yhdenmukaisia, päteviä ja verrattavissa olevia tuloksia - tunnistetaan tietoturvariskejä luomalla arviointiprosessi, jolla kartoitetaan hallintajärjestelmään kuuluvan tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit - tunnistetaan riskien omistajat - analysoidaan tietoturvariskit arvioimalla riskien toteutumisen ja realistinen todennäköisyys ja mahdolliset seuraukset - vertaamalla riskianalyysin tuloksia alussa mainittuihin riskikriteereihin ja prorisoimalla riskit. Dokumentoitu tieto arviointiprosesseista tulee säilyttää.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt	Riskien arviointi ja menetelmät	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
		6.1.3 Tietoturvariskien käsittely	Määritellä ja toteuttaa tietoturvariskien käsittelyprosessi, jossa - valitaan soveltuvat riskien käsittelyvaihtoehdot riskien arvioinnin perusteella - määritetään hallintakeinot käsittelyvaihtoehtojen toteuttamiseen (organisaatio voi tehdä ne itse tai yksilöidä muista lähteistä) - verrataan valittuja hallintakeinoja erilliseen taulukkoon, ettei yhtään tarvittavaa keinoa ole jätetty pois (taulukko ei ole täydellinen, joten muitakin keinoja voidaan tarvita) - laaditaan soveltuvuuslausunto, joka sisältää edellämainitut hallintakeinot sekä erillisessä taulukossa olevat perustelut hallintakeinojen käyttämiselle tai käyttämättä jättämiselle - laaditaan riskien käsittelysuunnitelma - hankitaan riskien omistajilta hyväksyntä käsittelysuunnitelmalle ja jäljelle jääville riskeille. Dokumentoitu tieto käsittelyprosesseista tulee säilyttää.	Ks erillinen taulukko toisella välilehdellä (tulee suoraan standardista ISO 27002:2013 ja pakollisia tässä kohtaa, jotta ISO 27001 vaatimukset täyttyvät)		Ks erillinen taulukko toisella välilehdellä (tulee suoraan standardista ISO 27002:2013 ja pakollisia tässä kohtaa, jotta ISO 27001 vaatimukset täyttyvät)	Soveltuvuuslausunto (Statement of Applicability, SoA), standardin tärkein dokumentti Riskien käsittely	
	6.2 Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu		Asettaa asiaankuuluville toiminnoille ja tasoille tietoturvatavoitteet, jotka täyttävät seuraavat vaatimukset - yhdenmukaisia tietoturvapolitiikan kanssa - mitattavia, jos mahdollista - otettava huomioon soveltuvat tietoturvavaatimukset sekä riskien arvioinnin ja käsittelyn tulokset - niistä on viestittävä - niitä on päivitettävä tarvittaessa. Dokumentoitu tieto tietoturvatavoitteista tulee säilyttää. Tietoturvatavoitteiden saavuttamisen suunnittelun tulee määrittää mitä tehdään, mitä resursseja tarvitaan, vastuuhenkilöt, työn aikataulu ja tulosten arviointikeinot.	Johtoryhmä	Yksikön päälliköt (raportointivelvollisuus johdolle, ehdotukset ratkaisuista, resursseista ja rahoituksesta, johto tekee lopulliset päätökset)	Turvallisuus	Tietoturvapolitiikka ja sen tavoitteet Riskien käsittely	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
7 Tukitoiminnot	7.1 Resurssit		Määrittää ja varata tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen tarvittavat resurssit.	Johtoryhmä	Johto	Johto		
	7.2 Pätevyys		Organisaation on - määritettävä niiden työntekijöiden pätevyysvaatimukset, joiden työ vaikuttaa tietoturvan tasoon - varmistettava pätevyys soveltavan koulutuksen, harjoittelun tai kokemuksen perusteella - hankittava tarvittaessa vaadittava pätevyys ja arvioitava toimenpiteiden vaikuttavuutta - säilytettävä asianmukaista dokumentoitua tietoa pätevyyksistä. Keinoja voivat olla esim. nykyisten työntekijöiden kouluttaminen, mentorointi, siirtäminen toisiin tehtäviin tai pätevien henkilöiden palkkaaminen tai vuokraaminen.	Johtoryhmä	Yksikön päälliköt (osaamisesta ja pätevyyksistä raportoidaan johdolle)	Turvallisuus & yksikön päälliköt (koulutukset ja osaamisarvioinnit)	Luettelo henkilökunnan koulutuksista, taidoista, kokemuksesta ja osaamisesta	
	7.3 Tietoisuus		Organisaation työntekijöiden on oltava tietoisia tietoturvapolitiikasta, miten he voivat osaltaan lisätä tietoturvaa, mitä hyötyä tietoturvan tason parantamisesta on sekä seurauksista noudattamatta jättämisestä.	Johtoryhmä	Yksikön päälliköt (turvallisuudesta vastaavien henkilöiden hyväksyttyjen ohjeiden ja linjausten mukaisesti)	Turvallisuus & Viestintä		
	7.4 Viestintä		Organisaation on määritettävä tietoturvan hallintajärjestelmän kannalta sisäistä ja ulkoista viestintää, esimerkiksi mistä viestitään, milloin, keiden kanssa, ketkä viestivät ja minkälaiset prosessit on toteutettava.	Johtoryhmä	Johtoryhmä	Turvallisuus & Viestintä		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	7.5 Dokumentoitu tieto						(Dokumentoidun tiedon hallintaprosessit) (Dokumenttienhallinnan kontrollit)	
		7.5.1 Yleistä	Dokumentoida ISO 27001 -standardissa vaaditut tiedot ja se tieto, jonka organisaatio on määrittänyt tietoturvan hallintajärjestelmän kannalta välttämättömäksi.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & osastojen asiantuntijatahot		
		7.5.2 Dokumentoidun tiedon luominen ja päivittäminen	Varmistaa dokumentoidun tiedon asianmukainen merkintä ja kuvaus, tallennusmuoto, tallennusväline ja soveltuvuuden ja riittävyyden tarkistaminen ja hyväksyminen.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		7.5.3 Dokumentoidun tiedon hallinta	Varmistaa dokumentoidun tiedon saatavuus tarvittaessa sopivassa muodossa sekä sen asianmukainen suojaaminen (esim. ei luvatonta luovutusta, asiaton käyttö estetty, muuttumaton tieto). Dokumenttien hallinnan tulee kattaa jakelu, pääsy tietoihin, esillesaanti, käyttö, varastointi ja säilytys, muutostenhallinta, säilyttäminen ja hävittäminen. (Ulkopuolinen dokumentoitu tieto, joka on tarpeellista tietoturvan hallintajärjestelmän kannalta, on yksilöitävä ja sitä on hallittava myös.)	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
8 Toiminta	8.1 Toiminnan suunnittelu ja ohjaus		Suunnitella ja toteuttaa prosessit tietoturvan vaatimusten täyttämiseksi ja kohdan 6.1 määritettyjen toimenpiteiden toteuttamiseksi, sekä ohjata niitä. Suunnitelmat on toteutettava niin, että kohdassa 6.2 määritetyt tietoturvatavoitteet saavutetaan. Dokumentoitu tieto näiden täyttämisestä on säilytettävä. Suunniteltuja muutoksia on hallittava ja arvioitava tahattomien muutosten seurauksia ja pyrittävä lieventämään haittavaikutuksia. Ulkoistetut prosessit on määritettävä ja varmistettava, että niitä valvotaan.	Johtoryhmä	Yksikön päälliköt (raportointi johdolle)	Turvallisuus (tukee) & yksikön päälliköt		
	8.2 Tietoturvariskien arviointi		Tietoturvariskien arviointi suunniteltuin aikavälein tai merkittäviä muutoksia ennen tai muutosten jälkeen. Arvioinnin tulee täyttää kohdan 6.1.2 kriteerit. Nämä on myös dokumentoitava.	Johtoryhmä	Yksikön päälliköt (raportointi johdolle)	Turvallisuus (tukee) & yksikön päälliköt	Riskien arvioinnin ja käsittelyn raportointi	
	8.3 Tietoturvariskien käsittely		Ottaa käyttöön tietoturvariskien käsittelysuunnitelma ja dokumentoida tulokset.	N/A	Yksikön päälliköt (päätökset johdolta)	Turvallisuus (tukee) & yksikön päälliköt	Riskien käsittely Riskien arvioinnin ja käsittelyn raportointi	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
9 Suorituskyvyn arviointi	9.1 Seuranta, mittaus, analysointi ja arviointi		Arvioida tietoturvan tasoa ja tietoturvan hallintajärjestelmän vaikuttavuutta ja määrittää - mitä seurataan ja mitataan (ml. tietoturvaprosessit ja hallintakeinot) - millä seuranta-, mittaus-, analysointi- tai arviointimenetelmillä tulos on kelvollinen (valitut menetelmät tulee olla vertailtavia ja toistettavia ollakseen kelvollisia) - milloin seuranta ja mittaus toteutetaan - ketkä toteuttavat - milloin tulokset analysoidaan ja arvioidaan ja kenen toimesta. Todisteena seurannan ja mittaamisen tulokset on dokumentoitava.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus	Seurannan ja mittausten tulokset	
	9.2 Sisäinen auditointi		Suorittaa sisäisiä auditointeja suunnitelluin aikavälein, jotta auditointien perusteella voidaan määrittää - tietoturvan hallintajärjestelmän vaatimuksenmukaisuus ja onko se ISO 27001 -standardin mukainen - onko se toteutettu ja ylläpidetty vaikuttavasti. Organisaation tulee - suunnitella, laatia, toteuttaa ja ylläpitää auditointiohjelmia, jossa määritellään auditointien taajuus, menetelmät, vastuut, suunnteluvaatimukset ja raportointi ottaen huomioon prosessien tärkeys ja edellisten auditointien tulokset - määritellä auditointikriteerit ja soveltamisala - valita auditoijat ja suorittaa auditointiprosessit niin, että objektiivisuus ja puoluettomuus toteutuvat - varmistaa tulosten raportoinnista asiaankuuluville johdon henkilöille - säilyttää dokumentoitua tietoa tuloksista.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Sisäinen valvonta	Sisäisen auditoinnin prosessi Sisäisen auditoinnin tulokset (Sisäisen auditoinnin työjärjestys)	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	9.3 Johdon katselmus		Varmistaa suunnitelluin aikavälein tietoturvan hallintajärjestelmän soveltuvuus, asianmukaisuus ja vaikuttavuus. Johdon katselmuksessa tulee ottaa huomioon - aiempien katselmusten määrittämien toimenpiteiden tilanne - olennaisten ulkoisten ja sisäisten asioiden muutokset - tietoturvan tasoa koskeva palaute (sisältäen poikkeamat, korjaavat toimenpiteet, seurannan ja mittauksen tulokset, auditointien tulokset ja tavoitteiden täyttyminen) - sidosryhmien antama palaute - riskiarvioiden tulokset ja riskinkäsittelysuunnitelman tilanne - jatkuvan parantamisen mahdollisuudet. Johdon katselmuksen tuloksiin on sisällyttävä päätökset jatkuvan parantamisen mahdollisuuksista sekä mahdollisista muutostarpeista. Dokumentoitu tieto johdon katselmusten tuloksista tulee säilyttää.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Sisäinen valvonta	Johdon katselmuksen tulokset	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
10 Parantaminen	10.1 Poikkeamat ja korjaavat toimenpiteet		Varmistaa poikkeamien käsitteleminen seuraavasti - poikkeamaan on reagoitava ja ryhdyttävä toimiin sen hallitsemiseksi ja korjaamiseksi sekä käsiteltävä seurauksia - on arvioitava tarvittavat toimenpiteet poikkeaman syiden, toistuvuuden ja muualla esiintyvyyden estämiseksi - toteutettava tarvittavat toimenpiteet ja arvioitava niiden vaikuttavuus - tehtävä muutoksia hallintajärjestelmään, jos tarpeellista. Dokumentoitua tietoa on säilytettävä todisteena poikkeamien luonteesta, niiden johdosta tehdyistä toimenpiteistä ja korjaavien toimenpiteiden tuloksista.	Johtoryhmä	Turvallisuus & yksikön päälliköt (kaikki poikkeamatilanteet raportoidaan johdolle ja pidetään tilannekuvaa yllä)	Turvallisuus & Digitaaliset ratkaisut: IT	Poikkeamien korjausten tulokset (Poikkeamien korjausten työjärjestys)	
	10.2 Jatkuva parantaminen		Parantaa jatkuvasti tietoturvan hallintajärjestelmän soveltuvuutta, riittävyyttä ja vaikuttavuutta.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.5 Tietoturvapolitiikat	A.5.1 Johdon ohjaus tietoturvallisuutta koskevissa asioissa		Tarjota johdon ohjausta ja tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti.						
		A.5.1.1 Tietoturvapolitiikat		Tietoturvallisuudelle on määriteltävä joukko johdon hyväksymiä politiikkoja, jotka julkaistaan henkilökunnan ja asiaankuuluvien organisaation ulkopuolisten osapuolten käyttöön ja joista tiedotetaan henkilökunnalle ja muille osapuolille.	Johtoryhmä	N/A	Turvallisuus & Viestintä		
		A.5.1.2 Tietoturvapolitiikkojen katselmointi		Tietoturvapolitiikat on katselmoitava suunnitelluin aikavälein tai kun merkittäviä muutoksia tapahtuu, jotta varmistetaan, että ne ovat edelleen soveltuvia, asianmukaisia ja vaikuttavia.	Johtoryhmä	N/A	Turvallisuus & Sisäinen valvonta		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.6 Tietoturvallisuuden organisointi	A.6.1 Sisäinen organisaatio		Luoda hallintarakenne, jolla aloitetaan tietoturvallisuuden toteuttaminen ja käyttö organisaatiossa ja hallitaan sitä.						
		A.6.1.1 Tietoturvaroolit ja vastuut		Kaikki tietoturvavastuut on määriteltävä ja jaettava.	Johtoryhmä	N/A	Turvallisuus		
		A.6.1.2 Tehtävien eriyttäminen		Ristiriidassa olevien tehtävien ja vastuualueiden on oltava eriytettyjä, jotta vähennetään organisaation suojattavan omaisuuden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä.	Johtoryhmä & Turvallisuus	Yksikön päälliköt	Turvallisuus		
		A.6.1.3 Yhteydet viranomaisiin		Asiaankuuluviin viranomaisiin on ylläpidettävä tarkoituksenmukaisia yhteyksiä.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		A.6.1.4 Yhteydet osaamisyhteisöihin		Osaamisyhteisöihin tai muihin turvallisuusasiantuntijaryhmiin ja ammatillisiin järjestöihin on ylläpidettävä tarkoituksenmukaisia yhteyksiä.	Johtoryhmä	Yksikön päälliköt	Yksikön päälliköt		
		A.6.1.5 Tietoturvallisuus projektinhallinnassa		Projektinhallinnassa on käsiteltävä tietoturvallisuutta projektin tyypistä riippumatta.	Johtoryhmä	Yksikön päälliköt	Turvallisuus		
	A.6.2 Mobiililaitteet ja etätyö		Varmistaa etätyön ja mobiililaitteiden käytön turvallisuus.						
		A.6.2.1 Mobiililaitteita koskeva politiikka		On otettava käyttöön politiikka ja sitä tukevat turvallisuuskäytännöt, joilla hallitaan mobiililaitteiden käytöstä syntyviä riskejä.	Johtoryhmä & Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Turvallisuus	(Mobiililaitteiden ja etätyön politiikka) (Omien laitteiden tuomisen politiikka)	
		A.6.2.2 Etätyö		On otettava käyttöön politiikka ja sitä tukevat turvallisuuskäytännöt, joilla suojataan etätyöpaikalla käytettyä, käsiteltyä tai säilytettävää tietoa.	Johtoryhmä & Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Turvallisuus		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.7 Henkilöstöturvallisuus	A.7.1 Ennen työsuhteen alkua		Varmistaa, että työntekijät ja vuokratyöntekijät ymmärtävät velvollisuutensa ja ovat sopivia heille harkittuihin tehtäviin.						
		A.7.1.1 Taustatarkistus		Kaikkien työnhakijoiden tausta on tarkastettava asianmukaisten lakien, määräysten ja eettisten normien mukaisesti. Tarkastukset on myös suhteutettava liiketoiminnallisiin vaatimuksiin, käsiteltävän tiedon luokitukseen ja oletettuihin riskeihin.	Johtoryhmä	N/A	Turvallisuus & HR ja talous		
		A.7.1.2 Työsopimuksen ehdot		Työntekijöiden ja vuokratyöntekijöiden kanssa tehdyissä sopimuksissa on eriteltävä työntekijän tai vuokratyöntekijän ja organisaation vastuut tietoturvallisuudesta.	Johtoryhmä	N/A	Turvallisuus & HR ja talous	Turvallisuuden roolien ja vastuiden määrittely	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.7.2 Työsuhteen aikana		Varmistaa, että työntekijät ja vuokratyöntekijät ovat tietoisia tietoturvavastuistaan ja täyttävät ne.						
		A.7.2.1 Johdon vastuut		Johdon on edellytettävä, että kaikki työntekijät ja vuokratyöntekijät toimivat tietoturvallisesti organisaation olemassa olevien politiikkojen ja menettelyjen mukaisesti.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt & HR ja talous		
		A.7.2.2 Tietoturvatietoisuus, -opastus ja -koulutus		Kaikkien organisaation työntekijöiden sekä tarvittaessa vuokratyöntekijöiden on saatava asianmukainen tietoturvatietoisuusopastus ja -koulutus, ja heidän tietojaan organisaation politiikkojen ja menettelyjen muutoksista on päivitettävä säännöllisesti, mikäli se on heidän toimenkuvansa kannalta merkityksellistä.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & HR ja talous		
		A.7.2.3 Kurinpitoprosessi		Organisaatiolla on oltava muodollinen ja tiedossa oleva kurinpitoprosessi, jonka perusteella toimitaan, kun työntekijä on syyllistynyt tietoturvarikkomukseen.	Johtoryhmä	N/A	Turvallisuus & HR ja talous		
	A.7.3 Työsuhteen päättyminen tai muuttuminen		Suojata organisaation etuja osana työsuhteen päättymis- tai muutosprosessia.						
		A.7.3.1 Työsuhteen päättyminen tai vastuiden muuttuminen		On määritettävä tietoturvavastuut ja -velvollisuudet, jotka jäävät voimaan työsuhteen päättymisen tai muuttumisen jälkeen. Niistä on tiedotettava työntekijälle tai vuokratyöntekijälle ja niiden noudattaminen on varmistettava.	Johtoryhmä	N/A	Turvallisuus & HR ja talous		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.8 Suojattavan omaisuuden hallinta	A.8.1 Vastuu suojattavasta omaisuudesta		Yksilöidä organisaation suojattava omaisuus ja määritellä asianmukaiset suojausvastuut.						
		A.8.1.1 Suojattavan omaisuuden luetteloiminen		Tieto sekä tietoon ja tietojenkäsittelypalveluihin liittyvä suojattava omaisuus on yksilöitävä. Suojattava omaisuus on luetteloitava ja tätä luetteloa on ylläpidettävä.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt & Digitaaliset ratkaisut: IT & HR ja talous	Suojattavan omaisuuden luettelo	
		A.8.1.2 Suojattavan omaisuuden omistajuus		Omaisuusluettelossa olevalla suojattavalla omaisuudella on oltava omistaja.	Johtoryhmä	N/A	Turvallisuus & HR ja talous		
		A.8.1.3 Suojattavan omaisuuden hyväksyttävä käyttö		Tiedon sekä tietoon ja tietojenkäsittelypalveluihin liittyvän suojattavan omaisuuden hyväksyttävän käytön säännöt on yksilöitävä, dokumentoitava ja toteutettava.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Aineistot ja analytiikka & Digitaaliset ratkaisut: IT	Suojattavan omaisuuden hyväksyttävä käyttö	
		A.8.1.4 Suojattavan omaisuuden palauttaminen		Kaikkien työntekijöiden ja organisaation ulkopuolisten käyttäjien on palautettava kaikki hallussaan oleva organisaation suojattava omaisuus työtehtävän, työsuhteen tai sopimuksen päättyessä.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & HR ja talous		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.8.2 Tietojen luokittelu		Varmistaa, että tiedon suojaustaso on riittävä. Riittävä suojaustaso määräytyy sen perusteella, miten merkittävää tieto on organisaatiolle.					(Tietojen luokittelupolitiikka)	
		A.8.2.1 Tiedon luokittelu		Tieto on luokiteltava lakisääteisten vaatimusten, tiedon arvon ja kriittisyyden sekä sen luvattoman paljastumisen tai muokkaamisen aiheuttamien vaikutusten perusteella.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		A.8.2.2 Tiedon merkintä		Tiedon merkitsemistä koskevat asianmukaiset menettelyt on laadittava ja otettava käyttöön organisaation määrittelemien tiedon luokitteluperiaatteiden mukaisesti.	Johtoryhmä	Yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		A.8.2.3 Suojattavan omaisuuden käsittely		Suojattavan omaisuuden käsittelemistä koskevat menettelyt on laadittava ja otettava käyttöön organisaation määrittelemien tiedon luokitteluperiaatteiden mukaisesti.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt		
	A.8.3 Tietovälineiden käsittely		Estää tietovälineille tallennettujen tietojen luvaton paljastuminen, muuttuminen, poistaminen tai tuhoutuminen.						
		A.8.3.1 Siirrettävien tietovälineiden hallinta		On laadittava siirrettävien tietovälineiden hallintaa koskeva asianmukainen ohjeistus organisaation määrittelemien luokitteluperiaatteiden mukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.8.3.2 Tietovälineiden hävittäminen		Tarpeettomat tietovälineet on hävitettävä turvallisella tavalla muodollisten menettelyjen mukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tietovälineiden hävittämispolitiikka)	
		A.8.3.3 Fyysisten tietovälineiden siirtäminen		Tietoa sisältävät tietovälineet on suojattava luvattomalta pääsyltä, väärinkäytöltä ja turmeltumiselta siirron aikana.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.9 Pääsynhallinta	A.9.1 Pääsynhallinnan liiketoiminnalliset vaatimukset		Hallita pääsyä tietoon ja tietojenkäsittelypalveluihin.						
		A.9.1.1 Pääsynhallintapolitiikka		Pääsynhallinnan periaatteet on laadittava, dokumentoitava ja katselmoitava liiketoiminnallisten vaatimusten ja tietoturvavaatimusten perusteella.	Johtoryhmä		Turvallisuus & Digitaaliset ratkaisut: IT	Pääsynhallintapolitiikka	
		A.9.1.2 Pääsy verkkoihin ja verkkopalveluihin		Käyttäjille on sallittava pääsy ainoastaan niihin verkkoihin ja verkkopalveluihin, joihin heille on nimenomaisesti myönnetty pääsyoikeudet.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
	A.9.2 Pääsyoikeuksien hallinta		Varmistaa valtuutettujen käyttäjien pääsy järjestelmiin ja palveluihin sekä estää luvaton pääsy niihin.						
		A.9.2.1 Käyttäjien rekisteröinti ja poistaminen		On toteutettava muodollinen käyttäjien rekisteröinti- ja poistamisprosessi, jonka avulla pääsyoikeudet jaetaan.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Salasanapolitiikka)	
		A.9.2.2 Pääsyoikeuksien jakaminen		On toteutettava muodollinen pääsyoikeuksien jakoprosessi, jonka avulla kyetään antamaan tai kumoamaan pääsyoikeus minkä tahansa tyyppiseltä käyttäjältä mihin tahansa järjestelmään tai palveluun.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Salasanapolitiikka)	
		A.9.2.3 Ylläpito-oikeuksien hallinta		Ylläpito-oikeuksien jakamista ja käyttöä on rajoitettava ja valvottava.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.9.2.4 Käyttäjien tunnistautumistietojen hallinta		Tunnistautumistietojen jakamista on valvottava muodollisen hallintaprosessin avulla.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Salasanapolitiikka)	
		A.9.2.5 Pääsyoikeuksien uudelleenarviointi		Suojattavan omaisuuden omistajien on uudelleenarvioitava pääsyoikeuksia säännöllisin aikavälein.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT & yksikön päälliköt		
		A.9.2.6 Pääsyoikeuksien poistaminen tai muuttaminen		Kaikkien työntekijöiden ja organisaation ulkopuolisten osapuolten käyttäjien pääsyoikeudet tietoon ja tietojenkäsittelypalveluihin on poistettava heidän työtehtävänsä, työsuhteensa tai sopimuksensa päättyessä tai pääsyoikeuksia on muutettava muutosten mukaisesti.	Turvallisuus	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.9.4 Järjestelmien ja sovellusten pääsynhallinta		Estää luvaton pääsy järjestelmiin ja sovelluksiin.						
		A.9.4.1 Tietoihin pääsyn rajoittaminen		Pääsyä tietoihin ja sovellusjärjestelmien toimintoihin on rajoitettava pääsynhallintapolitiikan mukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.9.4.2 Turvallinen kirjautuminen		Pääsyä järjestelmään ja sovelluksiin on hallittava turvallisella kirjautumismenettelyllä, kun pääsynhallintapolitiikassa niin velvoitetaan.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.9.4.3 Salasanojen hallintajärjestelmä		Salasanojen hallintajärjestelmän on oltava vuorovaikutteinen, ja sen on edellytettävä vahvojen salasanojen käyttöä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Salasanapolitiikka)	
		A.9.4.4 Ylläpito- ja hallintasovellukset		Järjestelmän ja sovellusten hallintakeinot ohittamaan kykenevien apuohjelmien käyttöä on rajoitettava, ja niitä on hallittava tarkasti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.9.4.5 Lähdekoodin suojaaminen pääsynvalvonnalla		Pääsyä ohjelmien lähdekoodeihin on rajoitettava.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT & Kehittäminen ja ohjaus		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.10 Salaus	A.10.1 Salauksen hallinta		Varmistaa salauksen asianmukainen ja vaikuttava käyttö, jotta tiedon luottamuksellisuutta, aitoutta ja eheyttä kyetään suojaamaan.						
		A.10.1.1 Salauksen käytön periaatteet		On laadittava ja toteutettava politiikka, jota noudatetaan, kun tietoa suojataan salauksen avulla.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.10.1.2 Salausavainten hallinta		Salausavainten käytöstä, suojaamisesta ja käyttöiästä on laadittava politiikka, ja tätä politiikkaa on noudatettava salausavainten koko käyttöiän ajan.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A. 11 Fyysinen turvallisuus ja ympäristön turvallisuus	A.11.1 Turva-alueet		Estää luvaton tunkeutuminen organisaation tietoaineistoihin ja tietojenkäsittelypalveluihin sekä estää niiden vahingoittuminen ja toiminnan häiriintyminen.						
		A.11.1.1 Fyysinen turva-alue		Turva-alueet on määriteltävä ja niitä on noudatettava paikoissa, jotka sisältävät joko arkaluonteisia tai kriittisiä tietoja ja tietojenkäsittelypalveluita.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.11.1.2 Kulunvalvonta		Turva-alueet on suojattava asianmukaisella kulunvalvonnalla, jotta varmistetaan, että vain luvan saaneet henkilöt pääsevät alueelle.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.11.1.3 Toimistojen, tilojen ja laitteistojen suojaus		Toimistojen, tilojen ja laitteistojen fyysinen turvallisuus on suunniteltava ja toteutettava.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.11.1.4 Suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan		On suunniteltava ja toteuttava fyysiset suojakeinot luonnonkatastrofien, vihamielisten hyökkäysten tai onnettomuuksien varalta.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.11.1.5 Turva-alueilla työskentely		On suunniteltava ja toteutettava menettelyt, joiden mukaisesti turva-alueilla työskennellään.	Johtoryhmä	Turvallisuus	Turvallisuus	(Turva-alueilla työskentelyn menettelyohje)	
		A.11.1.6 Toimitus- ja kuormausalueet		Kulkualueita, kuten toimitus- ja kuormausalueita, sekä muita pisteitä, joiden kautta luvattomat henkilöt saattavat päästä tiloihin, on valvottava, ja ne on mahdollisuuksien mukaan eristettävä tietojenkäsittelypalveluista, jotta niihin ei pääse luvatta.	Johtoryhmä	Turvallisuus	Turvallisuus		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.11.2 Laitteet		Estää omaisuuden katoaminen, vahingoittuminen, varastaminen tai vaarantuminen sekä organisaation toimintojen keskeytyminen.						
		A.11.2.1 Laitteiden sijoitus ja suojaus		Laitteistot on sijoitettava ja suojattava siten, että ympäristöuhkien ja luvattoman tunkeutumisen riskejä pienennetään.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.11.2.2 Peruspalvelut		Laitteet on suojattava sähkökatkoilta ja muilta peruspalveluiden vikojen aiheuttamilta häiriöiltä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.11.2.3 Kaapeloinnin turvallisuus		Sähkökaapelointi sekä tietoa siirtävä tai tietotekniikkapalveluita tukeva tietoliikennekaapelointi on suojattava salakuuntelulta, häirinnältä ja vahingoittumiselta.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.11.2.4 Laitteiden huolto		Laitteet on huollettava asianmukaisesti, jotta niiden jatkuva käytettävyys ja eheys voidaan varmistaa.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.11.2.5 Suojattavan omaisuuden poistaminen		Laitteita, tietoaineistoja tai ohjelmistoja ei saa poistaa toimipaikalta ilman ennalta saatua valtuutusta.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & yksikön päälliköt		
		A.11.2.6 Toimitilojen ulkopuolelle vietyjen laitteiden ja suojattavan omaisuuden turvallisuus		Toimitilojen ulkopuolella olevan suojattavan omaisuuden turvallisuus on varmistettava. Tässä on otettava huomioon, että organisaation tilojen ulkopuolella työskentelyyn liittyvät riskit ovat erilaisia.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & yksikön päälliköt		
		A.11.2.7 Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen		Kaikki laitteiden tallennettua tietoa sisältävät osat on tarkistettava, jotta voidaan varmistua siitä, että arkaluonteinen tieto ja tekijänoikeuden suojaamat ohjelmistot on poistettu tai tuhottu turvallisesti ennen laitteen käytöstä poistamista tai kierrättämistä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tietovälineiden hävittämispolitiikka)	
		A.11.2.8 Ilman valvontaa jäävät laitteet		Käyttäjien on varmistettava, että ilman valvontaa jäävät laitteet on suojattu asianmukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & koko		
		A.11.2.9 Puhtaan pöydän ja puhtaan näytön periaate		On otettava käyttöön papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän periaate sekä tietojenkäsittelypalveluja koskeva puhtaan näytön periaate.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & koko organisaatio	(Puhtaan pöydän ja näytön periaatteen ohje)	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.12 Käyttöturvallisuus	A.12.1 Toimintaohjeet ja velvollisuudet		Varmistaa tietojenkäsittelypalvelujen asianmukainen ja turvallinen toiminta.						
		A.12.1.1 Dokumentoidut toimintaohjeet		Toimintaohjeet on dokumentoitava ja niiden on oltava kaikkien niitä tarvitsevien käyttäjien saatavilla.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Viestintä	IT:n hallinnoinnin toimintaohjeet	
		A.12.1.2 Muutoksenhallinta		Tietoturvallisuuteen vaikuttavia organisaatioon, liiketoimintaprosesseihin ja tietojenkäsittelypalveluihin ja -järjestelmiin tehtäviä muutoksia on hallittava.	Johtoryhmä	Turvallisuus	Turvallisuus	(Muutoksenhallinnan politiikka)	
		A.12.1.3 Kapasiteetinhallinta		Resurssien käyttöä on tarkkailtava ja säädettävä ja on tehtävä ennusteita tulevista kapasiteettivaatimuksista, jotta voidaan varmistaa, että järjestelmän suorituskyky vastaa vaadittua.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT & yksikön päälliköt		
		A.12.1.4 Kehitys-, testaus- ja tuotantoympäristöjen erottaminen		Kehitys-, testaus- ja tuotantoympäristöt on erotettava toisistaan, jotta pienennetään tuotantoympäristön luvattoman käytön tai muuttamisen riskiä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & Kehittäminen ja ohjaus		
	A.12.2 Haittaohjelmilta suojautuminen		Varmistaa, että tiedot ja tietojenkäsittelypalvelut on suojattu haittaohjelmilta.						
		A.12.2.1 Haittaohjelmilta suojautuminen		Haittaohjelmilta suojaavat havaitsemis-, esto- ja palautusmekanismit on toteutettava, ja käyttäjien tietoisuutta haittaohjelmista on ylläpidettävä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT & Viestintä		
	A.12.3 Varmuuskopiointi		Suojautua tiedon menettämiseltä.						
		A.12.3.1 Tietojen varmuuskopiointi		Tiedoista, ohjelmistoista ja järjestelmistä on otettava säännöllisesti varmuuskopiot, jotka on testattava sovittujen varmuuskopiointiperiaatteiden mukaisesti.	Johtoryhmä	Turvallisuus	Digitaaliset ratkaisut: IT	(Varmuuskopiopolitiikka)	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.12.4 Kirjaaminen ja seuranta		Tallentaa tapahtumat ja luoda seurantatietoa.						
		A.12.4.1 Tapahtumien kirjaaminen		On luotava tapahtumalokeja, joihin tallennetaan käyttäjien suorittamat toiminnot sekä tapahtuneet poikkeamat, virheet ja tietoturvatapahtumat. Nämä lokit on säilytettävä ja niitä on katselmoitava säännöllisesti.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Käyttäjätapahtumien, poikkeamien ja tietoturvatapahtumien loki	
		A.12.4.2 Lokitietojen suojaaminen		Lokitiedot ja niiden kirjauspalvelut on suojattava peukaloimiselta ja luvaton pääsy niihin on estettävä.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.12.4.3 Pääkäyttäjä- ja operaattorilokit		Järjestelmän pääkäyttäjien ja operaattorien toiminnoista on pidettävä lokia. Nämä lokit on suojattava ja niitä on katselmoitava säännöllisesti.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Käyttäjätapahtumien, poikkeamien ja tietoturvatapahtumien loki	
		A.12.4.4 Kellojen synkronointi		Kaikkien samassa organisaatiossa tai samalla turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on asetettava saman viiteaikalähteen mukaisesti.	N/A	Turvallisuus	Digitaaliset ratkaisut: IT		
	A.12.5 Tuotantokäytössä olevien ohjelmistojen hallinta		Varmistaa tuotantokäytössä olevien järjestelmien eheys.						
		A.12.5.1 Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin		On luotava menettelyt, joilla valvotaan ohjelmistojen asentamista tuotantokäytössä oleviin järjestelmiin.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.12.6 Teknisten haavoittuvuuksien hallinta		Estää teknisten haavoittuvuuksien hyväksikäyttö.						
		A.12.6.1 Teknisten haavoittuvuuksien hallinta		Käytettävien tietojärjestelmien teknisistä haavoittuvuuksista on hankittava ajantasaista tietoa. Organisaation altistuminen näille haavoittuvuuksille on arvioitava, ja niihin liittyviin riskeihin on vastattava asianmukaisilla toimenpiteillä.	Turvallisuus	N/A	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.12.6.2 Ohjelmien asentamisen rajoittaminen		On laadittava ja otettava käyttöön käyttäjien suorittamaa ohjelmien asentamista koskevat säännöt.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
	A.12.7 Tietojärjestelmien auditointinäkökohtia		Varmistaa, että auditointitoiminnot vaikuttavat käytössä oleviin järjestelmiin mahdollisimman vähän.						
		A.12.7.1 Tietojärjestelmien auditointimekanismit		Auditointivaatimukset ja -toiminnot, jotka sisältävät tuotantokäytössä olevien järjestelmien todentamisia, on suunniteltava huolellisesti ja hyväksyttävä, jotta liiketoimintaprosesseja häiritään mahdollisimman vähän.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.13 Viestintäturvallisuus	A.13.1 Verkon turvallisuuden hallinta		Varmistaa verkossa liikkuvan tiedon ja sen tukena olevien tietojenkäsittelypalveluiden suojaaminen.						
		A.13.1.1 Verkon hallinta		Verkkoja on hallittava ja valvottava, jotta voidaan suojata järjestelmissä ja sovelluksissa oleva tieto.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.13.1.2 Verkkopalvelujen turvaaminen		Kaikkien verkkopalvelujen turvamekanismit, palvelutasot ja hallintavaatimukset on yksilöitävä ja sisällytettävä verkkopalvelusopimuksiin riippumatta siitä, tuotetaanko näitä palveluita organisaation sisällä vai onko ne ulkoistettu.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.13.1.3 Ryhmien eriyttäminen verkossa		Verkoissa olevat tietojenkäsittelypalvelujen, käyttäjien ja tietojärjestelmien ryhmät on eriytettävä toisistaan.	N/A	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.13.2 Tietojen siirtäminen		Ylläpitää organisaation sisällä tai jonkin ulkopuolisen osapuolen kanssa siirretyn tiedon suojausta.						
		A.13.2.1 Tiedonsiirtopolitiikat ja -menettelyt		Kaikentyyppisillä viestintäpalveluilla tapahtuvaa tiedon siirtämistä on suojattava määriteltyjen tiedonsiirtopolitiikan ja tiedonsiirron menettelyiden ja hallintakeinojen avulla.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tiedonsiirtopolitiikka)	
		A.13.2.2 Tiedonsiirtoa koskevat sopimukset		Sopimusten on katettava liiketoimintatietojen turvallinen siirtäminen organisaation ja ulkopuolisten osapuolten välillä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tiedonsiirtopolitiikka)	
		A.13.2.3 Sähköinen viestintä		Sähköisesti viestittyä tietoa on suojattava asianmukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Tiedonsiirtopolitiikka)	
		A.13.2.4 Salassapito- ja vaitiolositoumukset		Organisaation tiedonsuojaustarpeita kuvastavat vaatimukset salassapito- ja vaitiolositoumuksille on yksilöitävä, katselmoitava säännöllisesti ja dokumentoitava.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	Turvallisuuden roolien ja vastuiden määrittely	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.14 Järjestelmien hankkiminen, kehittäminen ja ylläpito	A.14.1 Tietojärjestelmiä koskevat turvallisuusvaatimukset		Varmistaa, että tietoturvallisuus on olennainen osa tietojärjestelmiä koko niiden elinkaaren ajan. Tähän sisältyvät myös palveluita julkisten verkkojen välityksellä tarjoavia tietojärjestelmiä koskevat turvallisuusvaatimukset.						
		A.14.1.1 Tietoturvavaatimusten analysointi ja määrittely		Tietoturvallisuuteen liittyvät vaatimukset on sisällytettävä uusia tai parannettavia tietojärjestelmiä koskeviin vaatimuksiin.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.14.1.2 Sovelluspalveluiden suojaaminen julkisissa verkoissa		Julkisten verkkojen kautta siirrettävää sovelluspalveluihin kuuluvaa tietoa on suojattava vilpilliseltä ja sopimuksen vastaiselta toiminnalta ja luvattomalta paljastumiselta ja muuttamiselta.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.14.1.3 Sovelluspalvelu-tapahtumien suojaaminen		Sovelluspalvelutapahtumiin liittyvää tietoa on suojattava, jotta estetään niiden epätäydellinen lähetys, väärään paikkaan ohjautuminen, luvaton viestien muuttaminen ja luvaton paljastuminen sekä viestin luvaton kopiointi tai toisto.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.14.2 Kehitys- ja tukiprosessien turvallisuus		Varmistaa, että tietoturvallisuutta suunnitellaan ja toteutetaan tietojärjestelmien kehittämisen elinkaaren osana.						
		A.14.2.1 Turvallisen kehittämisen politiikka		Ohjelmien ja järjestelmien kehittämistä koskevat säännöt on laadittava, ja niitä on sovellettava organisaation sisällä toteutettaviin kehitysprojekteihin.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Digitaaliset ratkaisut: IT & Kehittäminen ja ohjaus		
		A.14.2.2 Järjestelmään tehtävien muutosten hallintamenettelyt		Järjestelmiin niiden kehittämisen elinkaaren aikana tehtäviä muutoksia on hallittava muodollisilla muutostenhallintamenettelyillä.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		
		A.14.2.3 Sovellusten tekninen katselmointi käyttöalustan muutosten jälkeen		Liiketoiminnan kannalta kriittiset sovellukset on tarkistettava ja testattava käyttöalustan muutosten yhteydessä, jotta varmistetaan, ettei muutoksilla ole haitallisia vaikutuksia organisaation toimintaan tai turvallisuuteen.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Digitaaliset ratkaisut & Kehittäminen ja ohjaus		
		A.14.2.4 Ohjelmisstopakettien muutoksia koskevat rajoitukset		Ohjelmistopaketteihin tehtäviä muutoksia on vältettävä, ja ne on rajoitettava vain välttämättömiin muutoksiin, minkä lisäksi kaikkia muutoksia on hallittava tarkasti.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus	(Muutoksenhallinnan politiikka)	
		A.14.2.5 Turvallisen järjestelmäsuunnittelun periaatteet		Turvallisten järjestelmien toteuttamisen periaatteet on laadittava ja dokumentoitava. Niitä on ylläpidettävä ja niitä on sovellettava kaikkiin tietojärjestelmien kehitystoimiin.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus	Turvallisen järjesstelmäsuunnittelun periaatteet	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
		A.14.2.6 Turvallinen kehitysympäristö		Organisaatioiden on luotava ja asianmukaisesti suojattava kehitysympäristö, jota hyödynnetään järjestelmän kehittämisessä ja integraatiotoimissa ja joka kattaa järjestelmän koko kehityselinkaaren.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Digitaaliset ratkaisut: IT & Kehittäminen ja ohjaus		
		A.14.2.7 Ulkoistettu kehittäminen		Organisaation on valvottava ja seurattava ulkoistettuja järjestelmän kehitystoimintoja.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		
		A.14.2.8 Järjestelmän turvallisuustestaus		Kehitystyön aikana on testattava turvallisuustoiminnallisuudet.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		
		A.14.2.9 Järjesstelmän hyväksymistestaus		Uusille tietojärjestelmille, päivityksille ja uusille versioille on laadittava hyväksymistestausohjelmat ja niihin liittyvät kriteerit.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		
	A.14.3 Testiaineisto		Varmistaa testaukseen käytettävän tiedon suojaus.						
		A.14.3.1 Testiaineiston suojaaminen		Testiaineistot on valittava huolellisesti ja niitä on suojattava ja hallittava.	N/A	Kehittäminen ja ohjaus	Turvallisuus & Kehittäminen ja ohjaus		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A. 15 Suhteet toimittajiin	A. 15.1 Tietoturvallisuus toimittajasuhteissa		Varmistaa, että organisaation toimittajien käytettävissä oleva suojattava omaisuus on suojattu.						
		A. 15.1.1 Toimittajasuhteiden tietoturvapolitiikka		Tietoturvavaatimuksista, joilla vähennetään toimittajan pääsyoikeudesta organisaation suojattavaan omaisuuteen aiheutuvia riskejä, on sovittava yhdessä toimittajan kanssa, ja ne on dokumentoitava.	Johtoryhmä	Yksikön päälliköt	Turvallisuus & yksikön päälliköt	Toimittajien tietoturvapolitiikka	
		A. 15.1.2 Toimittajasopimusten turvallisuus		Kaikki olennaiset tietoturvavaatimukset on laadittava ja hyväksyttävä jokaisen toimittajan kanssa, jolla saattaa olla pääsy organisaation tietoihin tai joka saattaa käsitellä tai viestiä näitä tietoja tai toimittaa niihin liittyviä IT-infrastruktuurin osia.	Johtoryhmä	Turvallisuus (tukee) & Kehittäminen ja ohjaus	Turvallisuus & yksikön päälliköt & Digitaaliset ratkaisut: IT		
		A. 15.1.3 Tieto- ja viestintätekniikan toimitusketju		Toimittajien kanssa tehtävien sopimusten on sisällettävä vaatimukset, joilla vastataan tieto- ja viestintätekniikkapalveluihin ja tuotteen toimitusketjuihin liittyviin tietoturvariskeihin.	Johtoryhmä	Turvallisuus	Turvallisuus & yksikön päälliköt		
	A. 15.2 Toimittajien palveluiden hallinta		Ylläpitää toimittajasopimusten mukaista sovittua tietoturvatasoa ja palveluiden toimitustasoa.						
		A. 15.2.1 Toimittajien palvelujen seuranta ja katselmointi		Organisaatioiden on säännöllisesti seurattava, katselmoitava ja auditoitava toimittajan palveluiden toimittamista.	Johtoryhmä	Turvallisuus	Turvallisuus & yksikön päälliköt & Digitaaliset ratkaisut: IT		
		A. 15.2.2 Toimittajan palveluihin tulevien muutosten hallinta		Toimittajan palvelun tarjoamista koskevia muutoksia, mukaan lukien olemassa olevan tietoturvapolitiikan, menettelyjen ja hallintakeinojen ylläpitoa ja kehitystä, on hallittava ottaen huomioon kyseisten liiketoimintatietojen, -järjestelmien ja -prosessien kriittisyys ja riskien uudelleenarviointi.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & yksikön päälliköt & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.16 Tietoturvahäiriöiden hallinta	A.16.1 Tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinta		Varmistaa, että tietoturvahäiriöiden hallinnan toimintamalli on johdonmukainen ja vaikuttava ja että siihen sisältyy myös tietoturvatapahtumista ja –heikkouksista viestiminen.						
		A.16.1.1 Vastuut ja menettelyt		On määriteltävä hallintavastuut ja luotava menettelyt, joilla taataan pikainen, tehokas ja järjestelmällinen reagointi tietoturvahäiriöihin.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.16.1.2 Tietoturvatapahtumien raportointi		Tietoturvatapahtumista on raportoitava mahdollisimman nopeasti ja asiaankuuluvaa hallintokanavaa pitkin.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.16.1.3 Tietoturvaheikkouksien raportointi		Organisaation tietojärjestelmiä ja palveluita käyttävien työntekijöiden ja vuokratyöntekijöiden on kiinnitettävä huomiota kaikkiin järjestelmissä tai palveluissa oleviin tai epäiltyihin tietoturvaheikkouksiin ja raportoitava niistä.	Johtoryhmä	Turvallisuus	Turvallisuus & Viestintä		
		A.16.1.4 Tietoturvatapahtumien arviointi ja niitä koskevien päätösten tekeminen		Tietoturvatapahtumat on arvioitava, minkä jälkeen on tehtävä päätös siitä, luokitellaanko ne tietoturvahäiriöiksi.	Johtoryhmä	Turvallisuus	Turvallisuus		
		A.16.1.5 Tietoturvahäiriöihin vastaaminen		Tietoturvahäiriöihin on reagoitava menettelyohjeen mukaisesti.	Johtoryhmä	Turvallisuus	Koko organisaatio	Toimintaohje tietoturvahäiriöissä	
		A.16.1.6 Tietoturvahäiriöistä oppiminen		Tietoturvahäiriöiden analysoinnista ja ratkaisemisesta saatua tietämystä on hyödynnettävä tulevien häiriöiden todennäköisyyden vähentämisessä ja niiden vaikutuksen pienentämisessä.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		
		A.16.1.7 Todisteiden kokoaminen		Organisaation on määriteltävä ja toteutettava menettelyt todistusaineistoksi soveltuvan tiedon yksilöimiseen, keräämiseen, hankkimiseen ja säilyttämiseen.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A.17 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia	A.17.1 Tietoturvallisuuden jatkuvuus		Tietoturvallisuuden jatkuvuuden on sisällyttävä organisaation liiketoiminnan jatkuvuuden hallintajärjestelmiin.						
		A.17.1.1 Tietoturvallisuuden jatkuvuuden suunnittelu		Organisaation on määriteltävä tietoturvallisuutta ja sen jatkuvuutta epäsuotuisissa tilanteissa koskevat vaatimukset.	Johtoryhmä	Turvallisuus	Turvallisuus	(Liiketoiminnan keskeytysanalyysi - Business impact analysis)	
		A.17.1.2 Tietoturvallisuuden jatkuvuuden toteuttaminen		Organisaation on laadittava, dokumentoitava, toteutettava ja ylläpidettävä prosesseja, menettelyjä ja hallintamekanismeja, joilla varmistetaan, että tietoturvallisuuden jatkuvuuden vaadittu taso säilyy epäsuotuisissa tilanteissa.	Johtoryhmä	Turvallisuus	Turvallisuus	Tietoturvan jatkuvuuden toimintaohjeet	
		A.17.1.3 Tietoturvallisuuden jatkuvuuden todentaminen, katselmointi ja arviointi		Organisaation on todennettava laaditut ja toteutetut tietoturvallisuuden jatkuvuuden hallintamekanismit säännöllisin aikavälein, jotta voidaan varmistaa, että ne ovat päteviä ja vaikuttavia epäsuotuisissa tilanteissa.	Johtoryhmä	Turvallisuus	Turvallisuus & Sisäinen valvonta	(Tietoturvan harjoittelu ja testaussuunnitelma) (Tietoturvan katselmointi- ja	
	A.17.2 Vikasietoisuus		Varmistaa, että tietojenkäsittelypalvelut ovat saatavilla.						
		A.17.2.1 Tietojenkäsittelypalvelu-jen saatavuus		Tietojenkäsittelypalvelut on toteutettava niin vikasietoisina, että saatavuusvaatimukset täyttyvät.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT	(Liiketoiminnan jatkuvuusstrategia)	

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
A. 18 Vaatimustenmukaisuus	A. 18. 1 Lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen		Varmistaa aikkien tietoturvallisuuteen liittyvien lakien ja asetusten, säännösten ja sopimusten velvoitteiden sekä mahdollisten turvallisuusvaatimusten noudattaminen.						
		A. 18. 1. 1 Sovellettavien lakisääteisten ja sopimuksellisten vaatimusten yksilöiminen		Kaikki asiaankuuluvat lakien, viranomaisten ja sopimusten asettamat vaatimukset sekä organisaation toimintamalli niiden täyttämistä varten on yksilöitävä yksiselitteisesti ja dokumentoitava sekä pidettävä ajan tasalla kutakin tietojärjestelmää ja organisaatiota varten.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus	Lakisääteiset ja sopimukselliset vaatimukset	
		A. 18. 1. 2 Immateriaalioikeudet		On toteutettava asianmukaiset menettelyt, joilla varmistetaan, että immateriaalioikeuksiin ja tekijänoikeuksilla suojattujen ohjelmistotuotteiden käyttöön liittyviä lakien, viranomaisten ja sopimusten asettamia vaatimuksia noudatetaan.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus		
		A. 18. 1. 3 Tallenteiden suojaaminen		Tallenteet on suojattava katoamiselta, tuhoutumiselta, väärentämiseltä, luvattomalta käytöltä ja luvattomalta levittämiseltä lakien, viranomaisten, sopimusten ja liiketoiminnan asettamien vaatimusten mukaisesti.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		
		A. 18. 1. 4 Tietosuoja ja henkilötietojen suojaaminen		Tietosuoja ja henkilötietojen suojaus on varmistettava asiaankuuluvien lakien ja viranomaisten asettamien vaatimusten mukaisesti.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus & Digitaaliset ratkaisut: IT		
		A. 18. 1. 5 Salaustekniikan hallintaa koskevat säädökset		Salaustekniikan hallintamekanismeja on käytettävä kaikkien asianmukaisten lakien, viranomaisten ja sopimusten asettamien vaatimusten mukaisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoite	Hallintakeino	Linjausvastuu	Linjavastuu	Toteuttava vastuu	Vaadittavat dokumentit (sulkeissa vapaaehtoiset, mutta suositellut)	Valmis K/E
	A.18.2 Tietoturvallisuuden katselmoinnit		Varmistaa, että tietoturvallisuus on toteutettu ja että sitä noudatetaan organisaation politiikkojen ja menettelyjen mukaisesti.						
		A.18.2.1 Tietoturvallisuuden riippumaton katselmointi		Organisaation tietoturvallisuuden toimintamalli ja sen toteuttaminen (eli tietoturvallisuuteen liittyvät hallintatavoitteet, hallintakeinot, politiikat, prosessit ja menettelyt) on katselmoitava riippumattomasti suunnitelluin aikavälein tai kun tapahtuu merkittäviä muutoksia.	Johtoryhmä	Turvallisuus	Turvallisuus (toimii yhteyshenkilönä, ulkoinen auditointi)		
		A.18.2.2 Turvallisuuspolitiikkojen ja -standardien noudattaminen		Esimiesten on säännöllisesti katselmoitava, ovatko heidän vastuualueellaan olevat tietojenkäsittelymenettelyt ja muut menettelyt tarkoituksenmukaisen turvallisuuspolitiikan ja -standardien sekä muiden mahdollisten turvallisuusvaatimusten mukaisia.	Johtoryhmä	Turvallisuus & yksikön päälliköt	Turvallisuus (tukee) & yksikön päälliköt		
		A.18.2.3 Teknisen vaatimustenmukaisuuden katselmointi		Tietojärjestelmien vaatimustenmukaisuus organisaation tietoturvapolitiikkojen ja -standardien suhteen on katselmoitava säännöllisesti.	Johtoryhmä	Turvallisuus	Turvallisuus & Digitaaliset ratkaisut: IT		

Vastuunkantaja ylätaso/osasto	Vastuunkantaja yksikkötaso	Vastuunkantaja tiimitaso	Vaatimusten linjausvastuu	Vaatimusten linjavastuu	Vaatimusten toteutusvastuu	Riskinhallinnan linjausvastuu	Riskinhallinnan linjavastuu	Riskinhallinnan toteutusvastuu
Johtoryhmä			4 (paitsi 4.4) 5 6 7 8 (paitsi 8.3) 9 10	6.1.1 7.4	5.3	A.5 A.6 A.7 A.8 A.9 (paitsi A.9.2.6) A.10 A.11 A.12.1-A.12.3, A.12.6.2, A.12.7 A.13.1.1-A.13.1.2, A.13.2 A.14.1-A.14.2 A.15 A.16 A.17 A.18		
Viestintä				7.3-7.4				A.5.1.1 A.12.1.1, A.12.2.1 A.16.1.3
Osastot	**Yksikön päälliköt**			4 6.1.1-6.1.2, 6.2 7.2, 7.3, 7.5 8 9.2-9.3 10	4.1-4.2 6.1.2 7.2, 7.5.2-7.5.3 8		A.6.1.2-A.6.1.5 A.7.2.1-A.7.2.2 A.8.1.1, A.8.1.3- A.8.1.4, A.8.2.1- A.8.2.3 A.9.2.5-A.9.2.6, A.9.4.5 A.12.1.1, A.12.1.3, A.12.7.1 A.15.1.1, A.15.2.2 A.18.1.1-A.18.1.4, A.18.2.2	A.6.1.3-A.6.1.4 A.7.2.1 A.8.1.1, A.8.2.1- A.8.2.3 A.9.2.5 A.11.2.5-A.11.2.6 A.12.1.3 A.15.1.1-A.15.1.3, A.15.2 A.18.2.2

Vastuunkantaja ylätaso/osasto	Vastuunkantaja yksikkötaso	Vastuunkantaja tiimitaso	Vaatimusten linjausvastuu	Vaatimusten linjavastuu	Vaatimusten toteutusvastuu	Riskinhallinnan linjausvastuu	Riskinhallinnan linjavastuu	Riskinhallinnan toteutusvastuu
Tietopalvelut	**Digitaaliset ratkaisut**	IT-infrastruktuuri ja palvelut			4.3, 4.4 10.1		A.6.2	A.8.2.1, A.8.1.3, A.8.3 A.8.1-A.8.2, A.8.4 A.10.1.2 A.11.2 A.12.1.3-A.12.1.4, A.12.2-A.12.7 A.13 A.14.1.2-A.14.1.3, A.14.2.1, A.14.2.3, A.14.2.6 A.15.1.2, A.15.2 A.16.1.1-A.16.1.2, A.16.1.6-A.16.1.7 A.17.2.1 A.18.1.3-A.18.1.5, A.18.2.3
	Aineistot ja analytiikka							A.8.1.3
Mahdollistaja-palvelut	**HR ja talous**							A.7 A.8.1
	Kehittäminen ja ohjaus	Ohjelmistokehitys					A.14.2, A.14.3 A.15.1.2	A.9.4.5 A.12.1.4 A.14.2, A.14.3

Vastuunkantaja ylätaso/osasto	Vastuunkantaja yksikkötaso	Vastuunkantaja tiimitaso	Vaatimusten linjausvastuu	Vaatimusten linjavastuu	Vaatimusten toteutusvastuu	Riskinhallinnan linjausvastuu	Riskinhallinnan linjavastuu	Riskinhallinnan toteutusvastuu
	Tuki ja turvallisuus	**Turvallisuus**		9 10	4 5 6.1.1-6.1.2, 6.2 7.2-7.5 8 9 10	A.6.1.2, A.6.2 A.9.2.6 A.12.6.1	A.6.2 A.8.3 A.9.1.2, A.9.2.1-A.9.2.4, A.9.3, A.9.4.1-A.9.4.4 A.10 A.11 A.12.1.2, A.12.1.4, A.12.2-A.12.5, A.12.6.2, A.12.7 A.13 A.14.1.1-A.14.1.2 A.15.1.2-A.15.1.3, A.15.2 A.16 A.17 A.18	A.5.1 A.6.1.1-A.6.1.3, A.6.1.5, A.6.2 A.7 A.8 A.9.1-A.9.2, A.9.4 A.10 A.11 A.12.1-A.12.2, A.12.4-A.12.7 A.13 A.15 A.16.1.1-A.16.1.4, A.16.1.6-A.16.1.7 A.17 A.18
Sisäinen valvonta					9.2-9.3			A.5.1.2 A.17.1.3
Koko organisaatio								A.9.3.1 A.11.2.8-A.11.2.9 A.16.1.5