Inhimillisten tekijöiden vaikutus ISO/IEC 27001 -standardin kontrolleihin kyberturvallisuuslain näkökulmasta

Turun yliopisto
Tietotekniikan laitos
Diplomityö
Kyberturvallisuusteknologia
Kesäkuu 2026
Heli Salonen

Tarkastajat:
Jouni Isoaho
Saku Lindroos

TURUN YLIOPISTO
Tietotekniikan laitos

Heli Salonen: Inhimillisten tekijöiden vaikutus
ISO/IEC 27001 -standardin kontrolleihin kyberturvallisuuslain näkökulmasta

Diplomityö, 87 s., 7 liites.
Kyberturvallisuusteknologia
Kesäkuu 2026

Yksi keskeisimmistä EU:n kyberturvallisuussäädöksistä on Kyberturvallisuusdirektiivi NIS2, jonka vaatimukset on siirretty Suomen lainsäädäntöön Kyberturvallisuuslaissa. Laki määrittelee ne yhteiskunnan toimintojen kannalta kriittiset toimijat, joita sen velvoitteet koskevat. Organisaatiot voivat käyttää apuna ISO 27001 -standardia, joka määrittelee vaatimukset tietoturvallisuuden hallintajärjestelmälle. Tämä dokumentti velvoittaa määrittelemään organisaation tietoturvavaatimukset ja niitä uhkaavat riskit sekä riskienkäsittelyprosessit. Näiden toteuttamiseen on valittava tietoturvakontrollit, joita on listattu standardissa.

Edellä kuvatun prosessin toteuttajana on pääasiassa ihminen. Tässä työssä tarkastellaan, mitkä inhimilliset tekijät voivat vaikutta kyberturvallisuusriskeihin ja voivatko nämä inhimilliset tekijät vaikuttaa tietoturvakontrollien toteutumiseen. Lisäksi selvitetään inhimillisten tekijöiden ja kontrollien mahdollinen yhteys ja se, voisiko tämä mahdollinen yhteys tukea kyberturvallisuusriskien hallintaa.

Kirjallisuuskatsauksen perusteella tunnistettiin keskeiset inhimilliset tekijät, jotka voivat vaikuttaa kyberturvallisuusriskien toteutumiseen. ISO 27001 -standardin kontrolleista valittiin ne, joiden toteutumiselle jokin tunnistetuista inhimillisistä tekijöistä voi aiheuttaa riskin. Inhimillisten tekijöiden ja kontrollisen välille saatiin yhteyksiä, jolloin niistä voitiin muodostaa käsitteellinen viitekehys.

Viitekehyksen perusteella kuormitustekijöillä, kuten kiireellä ja stressillä, voitiin todeta olevan laaja-alainen vaikutus kontrollien toteutumiseen ja siten kyberturvallisuusriskien kasvamiseen. Lähes yhtä suuri vaikutus todettiin olevan myös osaamiseen ja riskitekijöihin liittyvillä inhimillisillä tekijöillä. Viitekehyksellä todettiin olevan yhteys kyberturvallisuuslakiin. Viitekehys voi toimia apuna lain velvoitteiden täyttämisessä mahdollistamalla inhimillisten tekijöiden tunnistamisen ennakolta ja huomioimisen riskienhallinnassa.

Asiasanat: inhimillinen tekijä, kyberturvallisuusriskit, ISO 27001, NIS2, Kyberturvallisuuslaki

UNIVERSITY OF TURKU
Department of Computing

Heli Salonen: The Impact of Human Factors on ISO/IEC 27001 Controls from the Perspective of the Cybersecurity Act

Master of Science Thesis, 87 p., 7 app. p.
Cyber Security Engineering
June 2026

One of the key EU cybersecurity regulations is the NIS2 Directive, which have been transposed into Finnish legislation through the Cybersecurity Act. The Cybersecurity Act defines the critical entities essential to the functioning of society to which its obligations apply. Organizations can utilize the ISO 27001 standard, which specifies requirements for an information security management system. This document requires defining the organization's information security requirements and the risks threatening them, as well as the risk management processes. To implement these, information security controls must be selected, which are listed in the standard.

The implementation of the process described above is primarily carried out by humans. This thesis examines which human factors may influence cybersecurity risks and whether these factors can affect the implementation of controls. In addition, the thesis explores the potential relationship between human factors and controls, and whether such a relationship could support the management of cybersecurity risks.

The key human factors that may influence cybersecurity risks were identified through a literature review. The controls chosen for analysis were selected from among the ISO 27001 controls based on whether their implementation could be jeopardized by one or more of the identified human factors. Connections between human factors and controls were identified, enabling the development of a conceptual framework.

Based on this framework, workload-related factors, such as time pressure and stress, have the most extensive impact on the implementation of controls and, consequently, on the increase of cybersecurity risks. Nearly as significant an impact was also attributed to human factors related to competence and risk-related behavior. The framework was found to have a connection to the Cybersecurity Act. The framework can serve as a tool in fulfilling the obligations of the law by enabling the identification of human factors in advance and their consideration in risk management.

Keywords: human factor, cyber security risks, ISO 27001, NIS2, Cyber Security Act

Tekoälyn käyttö

Tässä työssä on käytetty tekoälyä seuraavasti:

- Kirjallisuuskatsauksen artikkelien seulonnan apuna luvussa 5.3.1 kuvatulla tavalla.
- Kuvien ja taulukoiden LaTeX-koodin muodostamisen apuna.
- Viitetietojen LaTeX-muodon muodostamisen ja muokkaamisen apuna.
- Satunnaisista tekstin osista kirjoitusvirheiden etsiminen.
- Tiivistelmän englanniksi kääntämisen apuna.

Käytössä oli Microsoft 365 Copilot ja ChatGPT, jotka perustuvat OpenAI:n GPT-5 -sarjan kielimalleihin.

Tämän työn tekijä on tarkistanut ja muokannut tekoälyn tuottamat vastaukset ennen niiden käyttöä tähän työhön.

Tämän työn tekijä ymmärtää täyden vastuunsa myös yllä luetelluista tekoälyn avulla suoritetuista tehtävistä.

Sisällys

Kuvat

Taulukot

1 Johdanto

Verkko- ja tietojärjestelmistä on muodostunut keskeinen osa nykyaikaista yhteiskunnallista infrastruktuuria. Voimakas digitalisaatio on lisännyt jatkuvasti muuttuvia kyberturvallisuusuhkia. Erityisesti Covid-pandemian aikana etätyö lisääntyi ja samalla organisaatioiden kasvanut digitaalisten palveluiden käyttö lisäsi kyberrikollisten hyökkäyspinta-alaa. Ukrainan sota sekä muut konfliktit ja geopoliittiset jännitteet ovat myös lisänneet kybertoimintaa, kuten häirintää ja vakoilua.

Maailman talousfoorumin tammikuussa 2026 julkaistun raportin mukaan tekoäly on merkittävin kyberturvallisuuteen vaikuttava trendi vuonna 2026 [1]. Tekoäly vaikuttaa kyberturvallisuuteen sekä puolustuksen että hyökkäyksen näkökulmasta. Se voi tehostaa puolustusta automatisoimalla havaitsemista, analysointia ja reagointia, mutta samalla se voi myös tukea rikollisia entistä kehittyneempien hyökkäysten suunnittelussa ja toteuttamisessa. Toisena trendinä raportissa mainitaan geopolitiikka ja siihen liittyvä kriittisen infrastruktuurin häirintä ja vakoilu. Kolmantena trendinä raportti listaa kyberpetokset, jotka lisääntyvät jatkuvasti ja koskevat yhtä lailla niin organisaatioita kuin yksittäisiä kansalaisia.

Euroopan unionin (EU) määritelmän mukaan kyberturvallisuudella tarkoitetaan tietokoneiden, palvelimien, verkkojen, tietojen ja järjestelmien suojelua vihamielisiä hyökkäyksiä, luvatonta pääsyä ja vahingontekoa vastaan [2]. Kyberuhaksi EU määrittelee tarkoituksella haitallisen toiminnan, joka vaarantaa digitaalisten järjestelmien, verkkojen tai tietojen eheyden, luottamuksellisuuden tai saatavuuden [2].

Tietoturva keskittyy pääasiassa tiedon turvaamiseen, joten kyberturvallisuuden voidaan siis ajatella sisältävän tietoturvan lisäksi koko muun digitaalisen ympäristön, kuten verkot ja järjestelmät. Kyberturvallisuudessa riskillä tarkoitetaan mahdollisuutta, että jokin poikkeama aiheuttaa häiriön tai menetyksiä [3]. Riskin suuruus ilmaistaan todennäköisyydellä, joka sisältää sekä poikkeaman toteutumisen mahdollisuuden että häiriön tai menetyksen suuruuden.

EU:n kyberturvallisuusstrategian tavoite on suojella EU:n alueen toimijoita ja yksittäisiä kansalaisia erilaisilta kyberturvallisuusuhilta vahvistamalla kyberhyökkäyksien torjumista ja hyökkäyksistä toipumista [4]. Kyberturvallisuus ja kyberturvallisuusuhat ovat vahvasti mukana myös EU:n lainsäädännössä, joka velvoittaa Suomea EU:n jäsenvaltiona suoraan tai kansalliseen lainsäädäntöön sisällytettynä. Yksi uusimmista säädöksistä on (EU) 2022/2555 Kyberturvallisuusdirektiivi (jäljempänä NIS2), jolla pyritään parantaman yhteiskunnan kriittisten toimialojen, kuten sähkö- ja vesihuollon, kyberturvallisuutta. Direktiivinä NIS2 ei ole suoraan velvoittava, vaan sen vaatimukset on siirretty Suomen lainsäädäntöön Kyberturvallisuuslakiin.

Standardit ovat vaatimuksia, suosituksia ja ominaisuuksia sisältäviä dokumentteja, joita voidaan laatia esimerkiksi tuotteille tai järjestelmille [5]. Standardijärjestelmistä vastaavat kansalliset ja kansainväliset standardoimisorganisaatiot. Standardien laatimisesta vastaavat standardien aihealueiden asiantuntijaryhmät, jotka tekevät työtä vapaaehtoisesti. Pääasiassa standardien noudattaminen on vapaaehtoista, mutta standardia noudattamalla voidaan osoittaa esimerkiksi tuotteen lainsäädännöllinen vaatimustenmukaisuus. ISO/IEC 27000 -standardisarja muodostaa kansainvälisen viitekehyksen kyberturvallisuuden hallinnalle. ISO/IEC 27001 (jäljempänä ISO 27001) kuvaa tietoturvan hallintajärjestelmän (engl. information security management system, ISMS) vaatimukset. ISMS:n riskientunnistamista ja hallintaa varten standardin liitteessä A on lueteltuna 93 tietoturvakontrollia (jäljempänä kontrollit), joiden käyttöönotolla on tarkoitus hallita ja vähentää tunnistettuja kyberturvalli-

suusriskejä. ISO 27001 -standardin noudattaminen on vapaaehtoista, mutta se tarjoaa jäsennellyn viitekehyksen riskienhallintaan ja tietoturvan hallintajärjestelmän rakentamiseen. Nämä tukevat vahvasti NIS2-direktiivin ja siten Kyberturvallisuuslain velvoitteiden täyttymistä.

Teknologian kehityksen myötä yhä useammat prosessit automatisoituvat, mutta ihminen säilyy kuitenkin keskeisenä toimijana monissa tehtävissä. Koneen tai ohjelmiston virhe voidaan usein jäljittää sen käyttäjään tai kehittäjään. Virheiden taustalla on usein inhimillinen tekijä. Keväällä 2024 tapahtuneen Helsingin kaupungin kasvatuksen ja koulutuksen toimialan tietomurron mahdollisti etäyhteyspalvelimen haavoittuvuus, joka oli tiedossa ja johon oli saatavilla korjauspäivitys [6]. Kyseistä palvelinta ei kuitenkaan ollut päivitetty ja jopa 120 000 ihmisen arkaluonteisia tietoja päätyi hyökkääjälle. Voidaan olettaa, että tietohallinnon työntekijä ei tahallaan laiminlyönyt päivitystä, vaan tapahtuneeseen vaikutti inhimillinen tekijä. Kyberturvallisuudessa inhimillisellä tekijällä (engl. human factor) tarkoitetaan ihmisen ominaisuuksia, kuten esimerkiksi tarkkaavaisuutta, stressiä ja tietoisuutta, jotka vaikuttavat kyberturvallisuuteen liittyvien päätösten tekemiseen [7]. Ominaisuudet vaikuttavat ihmisen tapaan arvioida, havaita ja tulkita kyberturvallisuusriskejä, jotka voivat päätöksen myötä joko kasvaa tai pienentyä.

1.1 Tutkimusongelma ja -kysymykset

Kyberturvallisuuslain soveltamisalaan kuuluvat toimijat voivat hyödyntää ISO 27001 -standardia lain velvoitteiden täyttämisessä. Standardi edellyttää riskien tunnistamista ja niihin sopivien kontrollien valitsemista ja toteuttamista. Ihminen on keskeisessä roolissa kontrollien ja siten koko standardin vaatimusten toteuttajana. Inhimilliset tekijät voivat muodostua riskiksi tässä ketjussa. Inhimilliset tekijät pitäisi tunnistaa ja huomioida, jotta voitaisiin ennakoida niiden mahdollisesti aiheuttamat riskit kontrollien, standardin ja lain vaatimusten toteutumiselle.

Edellä olevan pohjalta muodostetaan tämän työn tutkimuskysymykset:

TK1. Mitkä ovat kirjallisuuden perusteella keskeiset inhimilliset tekijät, jotka voivat lisätä kyberturvallisriskejä?

TK2. Mitkä ovat ISO 27001 -standardin keskeiset kontrollit, joiden toteutumista kirjallisuudesta tunnistetut inhimilliset tekijät voivat heikentää?

TK3. Miten tunnistetut inhimilliset tekijät ja valitut ISO 27001 -standardin tietoturvakontrollit voidaan yhdistää viitekehykseksi, joka tukee kyberturvallisuusriskien hallintaa Kyberturvallisuuslain vaatimusten näkökulmasta?

1.2 Työn tavoite ja rakenne

Tämän työn tavoitteena on muodostaa viitekehys, joka yhdistää keskeiset kyberturvallisuuteen vaikuttavat inhimilliset tekijät ja ISO 27001 -standardin kontrollit kyberturvallisuusriskien hallinnan tueksi Kyberturvallisuuslain vaatimusten näkökulmasta. Työn aluksi tutustutaan EU:n kyberturvallisuussääntelyyn ja erityisesti NIS2-direktiiviin. Tarkemmin perehdytään NIS2-direktiivin Suomessa toimeenpanevaan Kyberturvallisuuslakiin.

Viitekehyksen muodostamiseen tarvittavat keskeiset inhimilliset tekijät valitaan kirjallisuuskatsauksen perusteella. ISO 27001 -standardia tarkastellaan sen kontrollien kautta ja valitaan perustellen ne keskeiset kontrollit, joissa inhimillinen tekijä voi olla riski kontrollin toteutumiselle. Määriteltävän uuden viitekehyksen tarkoitus on olla apuväline erityisesti organisaatioille, joita Kyberturvallisuuslaki velvoittaa. Taulukossa 2.2 on lueteltu ne toimialat, joita sekä NIS2 että Kyberturvallisuuslaki velvoittavat. Kyberturvallisuuslain velvoitteiden täyttämisen apuna organisaatio voi käyttää ISO 27001 -standardia. Viitekehyksen avulla organisaatio voi ennakolta varautua ja kiinnittää huomiota tiettyihin kontrolleihin, joissa inhimilliset tekijät voivat heikentää kontrollien toteutumista.

Tämän luvun jälkeen toisessa luvussa keskitytään kyberturvallisuuden lainsää-

däntöön. EU:n lainsäädännöstä esitetään keskeisimmät kyberturvallisuuteen liittyvät asetukset ja direktiivit, joista tutustutaan Kyberturvallisuusdirektiiviin NIS2 ja sen määrittämiin velvoitteisiin. Tämän jälkeen tarkastellaan Suomen kyberturvallisuuteen liittyvää lainsäädäntöä ja erityisesti NIS2-direktiivin määräykset toimeenpanevaa Kyberturvallisuuslakia.

Kolmannessa luvussa keskitytään kyberturvallisuuteen vaikuttaviin inhimillisiin tekijöihin. Käsite määritellään ja selvitetään vaikutukset kyberturvallisuudessa erityisesti riskinä. Neljännessä luvussa selvitetään, mikä on ISO-organisaatio ja mitä ovat organisaation määrittelemät standardit. Tarkemmin esitellään ISO 27000 -standardisarja ja erityisesti ISO 27001 sekä sen kontrollit, joita sovelletaan viitekehyksen muodostamisessa.

Viides luku esittelee, mistä näkökulmasta tätä työtä on tehty ja mitä tutkimusmenetelmiä on käytetty. Kuudennessa luvussa esitellään viitekehykseen valitut keskeiset inhimilliset tekijät ja ISO 27001 -standardin kontrollit, jonka jälkeen esitellään itse viitekehys.

Seitsemännessä luvussa käsitellään, miten muodostetun viitekehyksen kattavuus, johdonmukaisuus ja sovellettavuus arvioitiin. Viimeiseksi kahdeksannessa luvussa esitetään vastaukset tämän työn tutkimuskysymyksiin. Lisäksi pohditaan työn onnistumisia ja haasteita, ja niihin mahdollisesti vaikuttaneita tekijöitä. Myös työn jatkotutkimusmahdollisuudet käsitellään, samoin tulosten mahdolliset ehdot ja rajaukset.

1.3 Työn rajaukset

Tämän työn tärkeänä taustana on lainsäädäntö. Sekä NIS2 että Kyberturvallisuuslaki käyttävät termiä toimija, jolla tarkoitetaan oikeushenkilöä tai luonnollista henkilöä [3]. Termi kattaa siis niin yksityishenkilöt kuin yritykset ja muut organisaatiot, joita säädökset koskevat. Suomessa toimijoita velvoittaa sekä EU:n lainsäädäntö että

kansallinen lainsäädäntö. Tässä työssä esitellään tärkeimmät niin EU:n kuin kansallisen lainsäädännön kyberturvallisuuteen liittyvät säädökset. Erityisesti keskitytään NIS2-direktiiviin ja Kyberturvallisuuslakiin, joka on NIS2-direktiivin Suomen kansallinen toimeenpano. Näistä säädöksistä esitellään keskeisin sisältö. Lisäksi esitellään toimijat, joita nämä säädökset koskevat. Nämä toimijat on määritelty Kyberturvallisuuslaissa ja muodostavat kohderyhmän, joihin tässä työssä tarkasteltavat vaatimukset kohdistuvat. Toimijat muodostavat myös kehitettävän viitekehyksen soveltamiskohteen.

ISO 27001 standardi on tässä työssä väline, jota voidaan käyttää Kyberturvallisuuslain velvoitteiden täyttämisen apuna. Standardissa ei käytetä termiä toimija, vaan organisaatio (engl. organization). Standardin analysointi keskittyy tässä työssä sen kontrolleihin.

Tämä työ rajoittuu Suomessa toimiviin tai Suomessa palveluja tarjoaviin toimijatason toimijoihin, joihin sovelletaan Kyberturvallisuuslakia. Kyberturvallisuuslain 1 luku 3 § määrittelee nämä toimijat ja ne on tiivistetysti esitetty myöhemmin tämän työn taulukossa 2.2. Inhimillisten tekijöiden osalta tämä työ rajoittuu tarkastelemaan niitä tekijöitä, jotka suoritettavan kirjallisuuskatsauksen mukaan ovat yleisimpiä lisäämään kyberturvallisuusriskejä. ISO 27001 -standardin osalta tarkempi tarkastelu rajoittuu niihin standardin kontrolleihin, joiden toteutumiseen kirjallisuuskatsauksen perusteella valitut inhimilliset tekijät voivat vaikuttaa ja jotka liittyvät päivittäiseen tekemiseen.

Tässä työssä ei ole huomioitu NIS2-direktiivin määrittelemiä DNS-palveluntarjoajien, aluetunnusrekisterien, verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien sekä verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien erityisvelvoitteita.

2 Kyberturvallisuuden sääntely

Tässä luvussa käsitellään kyberturvallisuuteen liittyvää keskeisintä lainsäädäntöä EU:ssa ja Suomessa. Erityisesti keskitytään tämän työn kannalta tärkeimpiin säädöksiin: EU:n kyberturvallisuusdirektiiviin ja sen velvoitteet toimeenpanevaan Suomen kansallisen lainsäädännön Kyberturvallisuuslakiin.

2.1 EU:n lainsäädäntö

EU:n lainsäädäntö koostuu eri tyyppisistä säädöksistä. Tässä luvussa käsiteltävät EU-säädökset ovat joko asetuksia tai direktiivejä. Asetukset ovat sellaisenaan kaikilta osiltaan suoraan sitovia ja velvoittavia säädöksiä eli niillä on lainvoimainen asema kaikissa EU:n jäsenvaltioissa [8]. EU-asetuksen sisältö on vähimmäisvaatimus, joten jäsenvaltion oma lainsäädäntö voi määritellä tiukemmat vaatimukset. Direktiivit sen sijaan määrittelevät velvoittavia minimitavoitteita [8]. Ne eivät sellaisenaan ole lainvoimaisia vaan jäsenvaltioiden on siirrettävä direktiivin vaatimukset omaan lainsäädäntöönsä. Velvoitteet on täytettävä, mutta jäsenvaltio voi lainsäädäntöönsä itse määritellä, miten ne saavutetaan.

EU:n kyberturvallisuuspolitiikassa keskeisimpiä säädöksiä ovat Kyberturvallisuusasetus (engl. Cyber Security Act, CSA) Kyberturvallisuusdirektiivi (engl. Network and Information Security Directive, NIS2), Kyberkestävyyssäädös (engl. Cyber Resilience Act, CRA) ja Kybersolidaarisuussäädös (engl. Cyber Solidarity Act) [9]. Näiden lisäksi on lukuisia eri toimijasektoreita velvoittavia säädöksiä, kuten Asetus

finanssialan digitaalisesta häiriönsietokyvystä (engl. Digital Operational Resiliency Act, DORA) ja Direktiivi kriittisten toimijoiden häiriönsietokyvystä (engl. Critical Entities Resilience Directive, CER). Kaikkien edellä mainittujen säädösten lyhenteet, nimet ja säädösnumerot on esitetty taulukossa 2.1. Taulukon päiväys on säädöksen voimaantulopäivä, joka on 20. päivä siitä, kun säädös on julkaistu Euroopan unionin virallisessa lehdessä.

Taulukko 2.1: Kyberturvallisuuteen liittyviä EU-säädöksiä.

lyhenne	**nro**	**nimi**	**voimaan**
CSA	(EU) 2019/881	Kyberturvallisuusasetus	26.6.2019
NIS2	(EU) 2022/2555	Kyberturvallisuusdirektiivi	15.1.2023
CRA	(EU) 2024/2847	Kyberkestävyyssäädös	9.12.2024
-	(EU) 2025/38	Kybersolidaarisuussäädös	3.2.2025
DORA	(EU) 2022/2554	Asetus finanssialan digitaalisesta häiriönsietokyvystä	15.1.2023
CER	(EU) 2022/2557	Direktiivi kriittisten toimijoiden häiriönsietokyvystä	15.1.2023

CSA on asetus, joka määrittelee Euroopan unionin kyberturvallisuusviraston (engl. European Union Agency for Cybersecurity, ENISA) tavoitteet, tehtävät ja organisaation [10]. Se tuli voimaan 26.6.2019, mutta osa vaatimuksista tuli sovellettavaksi vasta 28.6.2021. ENISA oli toiminnassa jo ennen tätä asetusta määräaikaisina toimeksiantoina vuodesta 2004 alkaen, mutta tämä asetus määrittelee sen pysyvän perustamisen. Lisäksi asetus määrää eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän perustamisesta.

NIS2-direktiiviä käsitellään tarkemmin seuraavassa luvussa 2.2 ja direktiivin toimeenpanevaa Suomen kansallista Kyberturvallisuuslakia käsitellään luvussa 2.4.

CRA määrittelee verkkoon liitettävien digitaalisten laitteiden kyberturvallisuus-

vaatimusten vähimmäistason [11]. Asetus tulee asteittain sovellettavaksi 11.9.2026 alkaen ja kokonaisuudessaan sitä sovelletaan 11.12.2027 alkaen. Asetuksen tavoitteena on saada digitaalisten laitteiden valmistajat ymmärtämään kyberturvallisuuden tärkeys, ja että kyberturvallisuus huomioidaan tuotteiden suunnittelusta alkaen tuotteen koko elinkaaren ajan. Asetus määrittelee myös valmistajan vastuut laitteiden ilmaisten päivitysten jakamisesta.

Kybersolidaarisuussäädös on asetus, joka määrittelee toimenpiteet kyberturvallisuusuhkiin ja -poikkeamiin varautumiseen, hallintaan, ja reagointiin [12]. Se tuli sovellettavaksi kokonaisuudessaan 3.2.2025. Tämä asetus määrittelee myös kansalliset ja vähintään kolmen valtion yhdessä muodostamat kyberkeskittymät, jotka muodostavat eurooppalaisen kyberturvallisuuden hälytysjärjestelmän. Kyberkeskittymiin liittyminen on jäsenmaille vapaaehtoista. Lisäksi asetus säätää kyberturvallisuuden hätämekanismin perustamisesta. Tavoitteena on pystyä paremmin varautumaan ja reagoimaan merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin ja -hyökkäyksiin. Tällaisia ovat esimerkiksi sähkö- tai tietoliikenneverkkoon kohdistuva laajamittaisen häiriön aiheuttava hyökkäys, joka aiheuttaa taloudellisia tappioita [12].

DORA koskee finanssialaa ja määrittelee toimijoiden tieto- ja viestintätekniikan häiriöiden ja kyberuhkien ennaltaehkäisemisen vaatimukset [13]. Tavoitteena on alan toimijoiden häiriönsietokyvyn pysyminen korkealla tasolla. Asetuksen liitteessä lueteltuja finanssialan toimijoita ovat esimerkiksi pankit sekä vakuutus- ja rahoituslaitokset.

CER-direktiivin toimenpiteitä on pitänyt soveltaa jäsenvaltioiden lainsäädännön kautta 18.10.2024 alkaen [14]. Suomen lainsäädännön Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (jäljempänä CER-laki) tuli kuitenkin voimaan vasta 1.7.2025 [15]. Direktiivin liitteessä luetellaan yhteiskunnan kriittisten toimialojen toimijat. Direktiivi määrää näiden toimi-

joiden riskiarvioinnista, häiriönsietokyvyn varmistamisesta ja suunnitelmasta sekä poikkeamien ilmoittamisesta. CER-lain sisällöstä kerrotaan enemmän luvussa 2.3.

2.2 Kyberturvallisuusdirektiivi NIS2

NIS2-direktiivin ensisijainen tarkoitus on kyberturvallisuuden korkean tason saavuttaminen koko EU:n alueella. Direktiivin velvoitteita on pitänyt soveltaa jäsenvaltioissa 18.10.2024 alkaen. Suomen lainsäädäntöön se tuotiin kuitenkin vasta 8.4.2025, jolloin Kyberturvallisuuslaki astui voimaan. Myöhästymisen takia Suomi sai 22 muun valtion kanssa virallisen ilmoituksen Euroopan komissiolta rikkomusmenettelyn alkamisesta 28.11.2024 [16]. Valtiot saivat kaksi kuukautta aikaa saattaa direktiivi osaksi kansallista lainsäädäntöä. Tästäkin aikataulusta Suomi myöhästyi, ja sai vielä 7.5.2025 komissiolta lausunnon, koska Suomi ei ollut ilmoittanut komissiolle direktiivin täysimääräisestä saattamisesta osaksi kansallista lainsäädäntöään [17].

2.2.1 Valtiotason velvoitteet

NIS2-direktiivi määrittelee valtiotasolle erilaisia valvonta- ja raportointivelvoitteita. Valtioilla on velvollisuus tehdä kyberturvallisuusstrategia sekä perustaa ja nimetä toimivaltaisia viranomaisia ja organisaatioita kyberturvallisuuteen liittyviin valvontatehtäviin, poikkeamiin ja kriisinhallintaan. Kyberturvallisuusstrategiassa on määriteltävä valtion kyberturvallisuuden strategiset tavoitteet ja toimet niiden saavuttamiseksi. Strategia on päivitettävä säännöllisesti ja annettava tiedoksi Euroopan komissiolle. Jokaisella valtiolla on oltava keskitetty yhteyspiste, joka vastaa kyberturvallisuuteen liittyvästä yhteydenpidosta valtion sisällä ja EU:n toimielimiin. Kyberturvallisuuspoikkeamien varalle on laadittava suunnitelma, ja valtioiden on valvottava, että toimijat ilmoittavat poikkeamista viranomaisille. Tietoturvaloukkauksiin reagoimaan ja niitä tutkimaan on perustettava CSIRT-yksikkö (engl. Compu-

ter Security Incident Response Team). Suomessa tämä tehtävä kuuluu Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle.

Valtioiden on listattava keskeiset ja tärkeät toimijat, joita direktiivin velvoitteet koskevat. Toimijoiden perustiedoista ja kokonaislukumäärästä on pidettävä kirjaa, ja listaus on lähetettävä tiedoksi Euroopan komissiolle. Toimijoiden hallintoelinten toimintaa on valvottava ja varmistettava mm. vaadittujen kyberturvallisuustoimenpiteiden ja koulutusten toteutuminen. Direktiivi määrittelee rikkomuksista ja seuraamuksista, jos toimija ei noudata direktiivin määrittelemiä velvoitteita.

NIS2 painottaa monissa kohdissa yhteistyötä. Sitä velvoitetaan jäsenvaltion kyberturvallisuuteen liittyvien viranomaisten ja yksiköiden sisällä ja välillä. Lisäksi mainitaan velvoitteita yhteistyöhön jäsenvaltioiden kesken sekä jäsenvaltion ja unionin eri toimielinten kesken. Direktiivi huomioi myös toimijat, jotka eivät kuulu direktiivin määrittelemiin toimijoihin. Heille on tarjottava ohjausta ja tukea, jotta myös näiden toimijoiden kyberturvallisuustaso saadaan mahdollisimman korkeaksi vahvistamalla toimijoiden kyberresilienssiä ja kyberhygieniaa. Kyberresilienssillä tarkoitetaan varautumista kyberuhkiin sekä kykyä toimia ja palautua normaalitilaan kyberuhan toteutuessa. Kyberhygienia tarkoittaa jatkuvia rutiininomaisia toimia, joilla ylläpidetään kyberturvallisuutta.

2.2.2 Toimijatason velvoitteet

Toimijatason velvoitteet koskevat NIS2-direktiivin liitteissä listattujen erittäin kriittisten ja muiden kriittisten toimialojen julkisia ja yksityisiä toimijoita. Nämä on esitetty tiivistetysti taulukossa 2.2. Listaus ei täysin riitä määrittelemään, koskeeko NIS2 tiettyä toimijaa. Direktiivin liitteet määrittelevät vielä tarkemmin toimialojen toimijatyypit, joita direktiivi velvoittaa. Lisäksi tähänkin toimijoiden rajaukseen on useita lisäyksiä ja poikkeuksia. Esimerkiksi kansallisen turvallisuuden ja puolustuksen toimijoita direktiivi ei koske.

Taulukko 2.2: Toimialat, joita NIS2:n toimijatason velvoitteet koskevat. [18]

erittäin kriittiset toimialat	**valvova viranomainen**
energia: sähkö, kaukolämmitys ja -jäähdytys, öljy, kaasu, vety	Energiavirasto tai Tukes
liikenne: ilma-, raide-, vesi- tai tieliikenne	Traficom
pankkitoiminta	Finanssivalvonta
finanssimarkkinoiden infrastruktuuri	Finanssivalvonta
terveys	Fimea tai Lupa- ja valvontavirasto
juomavesi	Elinvoimakeskus
jätevesi	Elinvoimakeskus
digitaalinen infrastruktuuri	Traficom
tieto- ja viestintätekniikan palvelujen hallinta (yritysten välinen)	Traficom
julkishallinto	Traficom
avaruus	Traficom
Muut kriittiset toimialat	**Valvova viranomainen**
posti- ja kuriiripalvelut	Traficom
jätehuolto	Lupa- ja valvontavirasto
kemikaalien valmistus, tuotanto ja jakelu	Tukes
elintarvikkeiden tuotanto, jalostus ja jakelu	Ruokavirasto
valmistus: lääkinnälliset laitteet, in vitro -diagnostiikkaan tarkoitetut lääkinnälliset laitteet, tietokoneet sekä elektroniset ja optiset tuotteet ja sähkölaitteet, muut koneet ja laitteet, moottoriajoneuvot, perävaunut ja puoliperävaunut, muut kulkuneuvot	Fimea, Traficom tai Tukes
digitaalisen palvelun tarjoajat	Traficom
tutkimustoiminta	Traficom

Toimijoille on asetettu kokoraja, joten aivan pienimpiä toimijoita velvoitteet eivät myöskään koske, ellei toimijan katsota olevan erityisen tärkeä yhteiskunnan kriittisten toimintojen kannalta. Direktiivi velvoittaa myös niitä yksittäisiä toimijoita, jotka jäsenvaltio on nimennyt CER-direktiivin mukaisiksi kriittisiksi toimijoiksi. Kun toimijan todetaan kuuluvan direktiivin soveltamisalaan, se luokitellaan vielä joko keskeiseksi toimijaksi tai tärkeäksi toimijaksi NIS-direktiivin 1 luvun 3 artiklan mukaisesti. Jako perustuu siihen, kuinka tärkeäksi toimija koetaan yhteiskunnan toiminnan kannalta.

Toimijoiden on ilmoitettava viranomaisille nimensä, yhteystietonsa, direktiivin liitteiden mukaisen toimialansa ja ne jäsenvaltiot, joiden alueilla tarjoavat palvelujaan. Toimijalla on velvollisuus ylläpitää ilmoitettuja tietoja, ja muutoksista on ilmoitettava kahden viikon kuluessa.

Toimijoiden hallintoelinten on toteutettava hallintatoimenpiteet verkko- ja tietojärjestelmien turvallisuusriskien minimoimiseksi. Toimenpiteissä on huomioitava seuraavat asiat:

- riskianalyysit ja tietojärjestelmien turvallisuutta koskevat politiikat
- poikkeamien käsittely ja toiminnan jatkuvuuden hallinta
- toimitusketjun turvallisuus
- verkko- ja tietojärjestelmien koko elinkaaren turvallisuus
- hallintatoimenpiteiden tehokkuuden arviointi
- kyberhygieniakäytännöt, kyberturvallisuuskoulutus
- kryptografian ja salauksen käytön periaatteet
- henkilöstöturvallisuus, pääsynhallinta, omaisuudenhallinta
- monivaiheisen ja jatkuvan todennuksen ratkaisut, suojatun viestinnän käyttö

Joidenkin toimialojen toimijoille on asetettu tarkempia alakohtaisia teknisiä vaatimuksia hallintatoimenpiteiden toteuttamiseksi. Hallintoelinten jäsenten on osallistuttava säännöllisesti koulutuksiin ja tarjottava koulutusta kaikille työntekijöilleen.

Toimijoiden on viipymättä ilmoitettava merkittävistä poikkeamista CSIRT-yksikölle sekä palvelujensa vastaanottajille, joihin uhka voi vaikuttaa. Digi-infran toimijoille on erillinen Euroopan komission NIS2-täytäntöönpanoasetus, joka määrittelee näitä toimijoita koskevan merkittävän poikkeaman. Ensimmäinen ilmoitus, ennakkovaroitus, on tehtävä CSIRT-yksikölle 24 tunnin kuluessa siitä, kun toimija on saanut tiedon poikkeamasta. Toinen ilmoitus, varsinainen poikkeamailmoitus, on tehtävä 72 tunnin kuluessa. Kolmas ilmoitus, lopullinen raportti, on toimitettava viimeistään kuukauden kuluttua. Jos poikkeama on edelleen kesken, toimitetaan edistymisraportti, ja lopullinen raportti kuukauden kuluessa siitä, kun poikkeama on loppuun käsitelty. Poikkeama määritellään merkittäväksi, jos se voi aiheuttaa toimijan tarjoamiin palveluihin vakavan toimintahäiriön tai taloudellisia tappioita. Merkittäväksi katsotaan myös poikkeama, joka aiheuttaa huomattavaa aineellista tai aineetonta vahinkoa kenelle tahansa luonnolliselle tai oikeushenkilölle.

Kuten luvussa 2.1 mainittiin, direktiivit eivät suoraan velvoita vaan ne on siirrettävä jäsenvaltion lainsäädäntöön. Edellä käsiteltiin tiivistetysti NIS2 -direktiivin sisältöä. Jo siitä voidaan todeta, että direktiivi sisältää paljon hyvinkin tarkkoja määritelmiä, vaikka ne direktiivinä määrittävät vain minimitason. Esimerkiksi poikkeamista ilmoittamisen prosessi on kuvattu jo direktiivissä hyvin tarkkaan aikamääreineen. Näitä määrityksiä jäsenvaltiot voivat vain tiukentaa.

2.3 Suomen lainsäädäntö

Suomen lainsäädännön keskeisin kyberturvallisuuteen liittyvä säädös on Kyberturvallisuuslaki, joka siirtää NIS2-direktiivin vaatimukset Suomen kansalliseen lainsäädäntöön. CER-direktiivin vaatimukset Suomen lainsäädäntöön siirtää CER-laki. Nä-

mä kaksi lakia muodostavat vahvan perustan kyberturvallisuuden sääntelylle Suomessa. Edellä mainitut ja muut tässä luvussa myöhemmin esiteltävät Suomen lainsäädännön säädökset on esitelty kootusti taulukossa 2.3.

Taulukko 2.3: Kyberturvallisuuteen liittyvät tärkeimmät säädökset Suomen kansallisessa lainsäädännössä.

nro	**nimi**	**perustuu**	**voimaan**
124/2025	Kyberturvallisuuslaki	NIS2	8.4.2025
125/2025	Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta	NIS2	8.4.2025
310/2025	Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta	CER	1.7.2025
917/2014	Laki sähköisen viestinnän palveluista		1.1.2015

Kyberturvallisuuslakia käsitellään seuraavassa luvussa 2.4. Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta tuli voimaan yhtäaikaisesti Kyberturvallisuuslain kanssa 8.4.2025. Alkuperäiseen Lakiin julkisen hallinnon tiedonhallinnasta verrattuna uusi laki on päivitetty NIS2-vaatimusten mukaiseksi. Tämän lain toimijoita ovat julkisen hallinnon keskeiset toimijat (NIS2 Liite I kohta 10), joiden kyberturvallisuuteen liittyvät NIS2-velvoitteet on lisätty lakiin uutena lain lukuna 4a [19].

CER-laki koskee CER-direktiivin liitteessä lueteltuja yhteiskunnan kriittisten toimialojen toimijoita. Laki määrää näiden toimijoiden riskiarvioinnista, häiriönsietokyvyn varmistamisesta ja suunnitelmasta sekä poikkeamien ilmoittamisesta [15]. Kriittisiksi toimialoiksi on määritelty mm. energia, liikenne, pankkiala ja terveys, joista valtion on nimettävä yksittäiset organisaatiot kriittisiksi toimijoiksi. Lisäksi laissa määritetään toimivaltaiset viranomaiset sekä eri alojen valvovat viranomaiset ja heidän tehtävänsä. Viranomaisten tehtäviksi määrätään mm. kansallisen riskiar-

vioinnin ja valtakunnallisen suunnitelman tekeminen.

Traficomin säädöslistauksessa kyberturvallisuuteen on liitetty myös Laki sähköisen viestinnän palveluista, joka on ollut voimassa vuoden 2015 alusta alkaen [20]. Lakia on päivitetty useita kertoja ja tällä hetkellä siihen on vireillä useita hallituksen esityksiä, joilla mm. päivitetään lainsäädäntöä syksyllä 2026 voimaantulevan CRA:n vaatimusten mukaisiksi [21]. Lain tarkoitus on mm. varmistaa viestintäpalvelujen saatavuus ja radiotaajuuksien häiriötön käyttö koko maassa [22]. Verkkopalvelut liittyvät vahvasti sekä viestintäpalveluihin että radiotaajuuksiin, ja laissa mainitaan esimerkiksi viestintäverkkojen ja -palvelujen tietoturva. Laki myös kieltää viestintälaitteiden käytön viestintäverkon kriittisissä osissa kansallisen turvallisuuden, kuten ulkomaisen tiedustelutoiminnan epäilyn, vuoksi. Lain mukaan viestintäverkkojen turvallisuutta seuraa Valtioneuvoston asettama verkkoturvallisuuden neuvottelukunta.

2.4 Kyberturvallisuuslaki

NIS2 on monilta osin kirjoitettu hyvin yksityiskohtaisesti todennäköisesti siksi, että jäsenmaiden kansalliset säädökset olisivat mahdollisimman yhdenmukaisia. Suomen Kyberturvallisuuslaki on sisällöltään pääasiassa hyvin NIS2-direktiivin määrittelemän minimitason mukainen. Verrattaessa toimijaluetteloita NIS2-direktiivin liitteissä 1 ja 2 Kyberturvallisuusdirektiivin liitteisiin 1 ja 2, ovat ne lähes identtisiä sisällöltään. Kyberturvallisuuslain liitteisiin toimijat on jaoteltu hieman eri tavalla, ja kuvauksiin on lisätty viitteitä Suomen kansalliseen lainsäädäntöön. Kuten aiemmin mainittiin, NIS2-direktiivin Liitteen 1 kohta 10 (julkisen hallinnon keskeiset toimijat) on Suomen lainsäädännössä siirretty Lakiin julkisen hallinnon tiedonhallinnasta, joka on ajantasaistettu.

Riskienhallinnan osalta Kyberturvallisuuslaissa on määritelty toimijoille toimenpiteet, joilla on varmistettava toimijan palveluntarjontaan liittyvien verkkojen ja

tietojärjestelmien turvallisuus. Kaikki vaaratekijät on tiedostettava ja minimoitava, poikkeuksiin varauduttava ja suunnitelmat on pidettävä ajantasaisina. Luvussa 2.2.2 listattiin NIS2-direktiivin IV luvun 21 artiklan määrittelemät toimenpiteet turvallisuusriskien minimoimiseksi. Vastaava listaus on myös Kyberturvallisuuslaissa 2 luvun 9 §:ssä [3]. Listoja vertailtaessa havaitaan niiden sisällön olevan hyvin samanlainen, mutta asiat on sanoitettu eri tavalla. Toimijan johdolla on oltava perehtyneisyys kyberturvallisuuteen, koska johto vastaa toimijan riskienhallinnasta kokonaisuudessaan [3]. Johdon vastuu on määritelty laissa omassa pykälässään, joka osaltaan voi kertoa johdon vastuun korostamisesta.

Poikkeamailmoitusten prosessi on Kyberturvallisuuslaissa aivan sama kuin NIS2-direktiivissä. Prosessiin kuuluu samat kolme ilmoitusta: ensi-ilmoitus, jatkoilmoitus ja loppuraportti. Laki määrittää poikkeamailmoitusten sisällöstä direktiiviä tarkemmin sekä valvovan viranomaisen mahdollisuudesta antaa valvomilleen toimijoille tarkempia vaatimuksia sisältöön liittyen.

Kuten luvussa 2.2.1 mainittiin yhteistyöstä ja sen positiivisesta merkityksestä NIS2-direktiivin valtiollisten toimijoiden välillä, myös Kyberturvallisuuslaissa kehotetaan yhteistyöhön ja vapaaehtoiseen kyberturvallisuustietojen jakamiseen [3]. Tähän CSIRT-yksikön koordinoimaan yhteistyöhön voivat osallistua sekä lain soveltamisalaan kuuluvat toimijat että myös sellaiset toimijat, joilla ei ole lain vaatimia velvoitteita. Laissa mainitaan myös mahdollisuudesta vapaaehtoisesti tehdä poikkeamailmoituksia valvovalle viranomaiselle myös muista kuin laissa velvoitetuista tapahtumista. Vaikka laissa säädetään kyberturvallisuutta koskevien riskien hallinnasta tietyillä yhteiskunnan tärkeillä toimialoilla, laki selvästi myös kannustaa laajempaan kuin lain velvoittamaan yhteistyöhön.

Kyberturvallisuuslaki määrittää, että keskitettynä yhteyspisteenä Suomessa toimii Kyberturvallisuuskeskus [3]. Sen tehtävä on toimia yhteistyön koordinoijana valvovien viranomaisten välillä ja raportoida Suomen tietoturvapoikkeamista ja kybe-

ruhkista ENISA:lle kolmen kuukauden välein. Laki määrää CSIRT-yksikön tehtävät ja että yksikkö toimii Suomessa Liikenne- ja viestintäviraston alaisuudessa.

Kyberturvallisuuslaki määrää suoraan valvovat viranomaistahot kaikille lain velvoittamille toimialoille, jotka on listattu luvussa 2.2.2 esitellyssä taulukossa 2.2. Valvovat viranomaiset ylläpitävät listaa kaikista valvonta-alansa toimijoista ja välittävät listan keskitetylle yhteyspisteelle. Se taas huolehtii listan lähettämisestä EU:n nimetyille toimielimille, kuten ENISA:lle. Valvovien viranomaisten tehtävä on valvoa lain noudattamista ja niillä on siksi oikeus saada valvonnan kannalta tarpeelliset tiedot toimijoilta tietojen luovuttamiseen liittyvistä rajoituksista huolimatta. Valvovilla viranomaisilla on myös oikeus tehdä tarkastuksia ja ryhtyä lain määrittämiin toimiin, jos valvonnassa huomataan puutteita lain noudattamisessa.

Valtioneuvoston tehtäväksi Kyberturvallisuuslaki määrää kansallisen kyberturvallisuusstrategian hyväksymisen ja päivittämisen vähintään viiden vuoden välein [3]. Liikenne- ja viestintäministeriön tehtäväksi määrätään laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelman laatiminen, ja Kyberturvallisuuskeskus määrätään koordinaattoriksi hallinnoimaan mahdollisia laajamittaisia kyberturvallisuuspoikkeamia ja -kriisejä. Viranomaisten kohdalla palataan myös yhteistyö-teemaan: Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava yhteistyössä keskenään sekä tarvittaessa myös muiden viranomaistahojen, kuten poliisin, kanssa. Yhteistyöllä päästään paremmin ja laajemmin NIS2:n ja siten Kyberturvallisuuslain tärkeimpään tavoitteeseen eli parempaan kyberturvallisuuteen EU:n jäsenvaltioissa ja niiden välillä.

3 Inhimillinen tekijä kyberturvallisuudessa

Tässä luvussa määritetään, mitä inhimillisellä tekijällä tarkoitetaan. Tämän jälkeen selvitetään esimerkein, miten se esiintyy kyberturvallisuusriskien yhteydessä.

3.1 Inhimillisen tekijän määritelmä

Englanninkielinen termi human factors engineering, HFE, on määritelty jo 1920-luvulla [23]. Termi on vaikea suomentaa, mutta käytännössä se tarkoittaa psykologian, insinööritaitojen ja suunnitteluperiaatteiden yhdistelmää. Tämän monialaisen suunnittelun tarkoituksena on parantaa käyttäjien tehokkuutta, turvallisuutta ja tuottavuutta. Tavoitteena on siis suunnitella laitteet ihmistä varten, jotta ihmisen ja suunniteltujen laitteiden yhteistyö ja vuorovaikutus olisivat paremmat. Alkujaan termi oli hyvin lähellä ergonomiaa, joka tarkoittaa ihmisen ja järjestelmien välistä vuorovaikutusta.

Viimeisen kahden vuosikymmenen aikana human factor, inhimillinen tekijä, on tullut yhä enemmän osaksi kyberturvallisuutta ja sen tutkimusta. Kyberturvallisuuteen liittyvissä tutkimuksissa alettiin ottaa mukaan inhimillinen tekijä tarkoituksena auttaa organisaatioita suhtautumaan myönteisemmin kyberturvallisuuteen. Lisäksi alettiin tutkia ihmisen tiedonkäsittelyä ja päätöksentekoa, sekä niiden yhteyttä kyberturvallisuusriskeihin. Tutkimuksissa havaittiin myös, että inhimillisillä tekijöillä,

kuten luonteenpiirteillä ja käyttäytymisellä, voi olla yhteys kyberturvallisuuteen joko positiivisesti tai negatiivisesti. [23], [24], [25]

Tämän päivän inhimillisen tekijän määritelmillä kyberturvallisuudessa on edelleen yhteys HFE:n vanhaan määritelmään. Inhimillinen tekijä tarkoittaa ihmisen ominaisuutta, joka kyberturvallisuudessa jollakin tavalla liittyy ihmisen ja teknologian väliseen vuorovaikutukseen. Inhimilliset tekijät ovat niitä ihmisen ominaisuuksia ja käyttäytymiseen liittyviä näkökohtia, jotka vaikuttavat ihmisen tekemiin kyberturvallisuuteen liittyviin päätöksiin [7]. Tällaisia ihmisen ominaisuuksia ovat esimerkiksi tietoisuus, ymmärrys ja ajattelutavat. Ne vaikuttavat ihmisen tapaan arvioida, havaita ja tulkita kyberturvallisuusriskejä. Näiden riskien ymmärrys ja tietoisuus vaikuttavat ihmisen ajattelu- ja toimintatapoihin, jotka muokkaavat organisaation turvallisuuskulttuuria. Vahva turvallisuuskulttuuri sisältää käsityksen, että tietoturvakäytännöt ymmärretään ja asetetaan etusijalle kaikessa toiminnassa [26]. Positiivisella turvallisuuskulttuurilla on suora vaikutus inhimillisiin tekijöihin, jotka lisäävät halukkuutta noudattaa turvallisuuteen liittyviä käytänteitä.

3.2 Inhimillinen tekijä kyberturvallisuusriskinä

Inhimillinen tekijä tuo kyberturvallisuuteen sekä riskejä että selviytymiskykyä tavoilla, joita ei pystytä hallitsemaan pelkillä teknologioilla, kuten palomuureilla ja salauksella [27]. Jo turvallisen järjestelmän kehittäminen ja valmistaminen on vaatinut ihmisen toiminnalta onnistumista. Inhimillinen tekijä on mukana järjestelmien käytössä, kun niiden toiminnasta vastaa ihminen yksilönä tai ryhmässä. Tarkkuudella ja ohjeita noudattamalla ihminen voi pitää järjestelmän turvallisena tai huolimattomalla toiminnalla johtaa riskin toteutumiseen. Inhimillinen tekijä on tullut mukaan kyberturvallisuuden tutimukseen, koska tekniset ratkaisut eivät yksin riitä kyberturvallisuusriskien estämisessä [23].

Kyberturvallisuuteen vaikuttavien inhimillisten tekijöiden keskiössä ovat psyko-

logiset ominaisuudet, kuten erilaiset arviointikykyyn vaikuttavat ajattelun vääristymät tai vinoumat [7]. Tällaisia ovat esimerkiksi optimismiharha, joka saa ihmisen uskomaan, että vaara on todellisuutta pienempi. Vahvistusharha taas saa ihmisen tulkitsemaan ja uskomaan uutta tietoa siten, että se tukee olemassa olevia jo vääristyneitä uskomuksia. Tällä tavalla ajattelun kokonaisharha kasvaa, joka voi johtaa aliarvioimaan kyberturvallisuusriskejä ja tekemään vääriä päätöksiä riskien suhteen.

Ihmisen käyttäytymiseen liittyy monia erilaisia inhimillisiä tekijöitä, jotka voivat lisätä virheitä kyberturvallisuusriskien yhteydessä [7]. Ihmisen tekemät virheet voivat johtua esimerkiksi mukavuudenhalusta, tietämättömyydestä tai liiallisesta luottamisesta. Virheiden seuraus voi olla esimerkiksi liian helpot tai turvattomasti säilytetyt salasanat tai ohjelmistopäivitysten ohittaminen.

Ihmisen sosiokulttuuriseen ajatteluun vaikuttavat ympäristö- ja kulttuuritekijät sekä olosuhteet. Sosiokulttuuriset tekijät vaikuttavat kyberturvallisuudessa tietoisuuden ja käytäntöjen muodostumiseen [7]. Niillä on vahva vaikutus asenteisiin turvallisuutta ja yksityisyyttä kohtaan. Kun yksityisyys on kulttuurisesti vahva arvo, vaikuttaa se suoraan vähempään yksityisten tietojen jakamiseen ja vahvempaan kyberturvallisuusajatteluun, joka voi näkyä niin yksityis- kuin organisaatiotasollakin. Organisaation vahvan kyberturvallisuuskulttuurin syntyyn vaikuttaa esimerkiksi se, että kaikilta vaaditaan kyberturvallisuuskäytänteiden noudattamista.

Inhimilliset tekijät on huomioitava kyberturvallisuuden johtamisessa, jotta organisaatiolla on mahdollisuus menestyä [28]. Johtajuuden lisäksi yhdenmukaisilla käytännöillä ja organisaatiokulttuurilla on merkittävä vaikutus kyberturvallisuuden vaatimustenmukaisuuteen [29]. Kyberturvallisuuteen on suhtauduttava vakavasti eikä sitä saa pitää pelkkänä kulueränä organisaatiolle [25]. Yksinkertaisemmat prosessit ja korkea organisaation sisäinen luottamus ovat tärkeä osa strategiaa, ja joilla voidaan vähentää kyberturvallisuusväsymystä ja parantaa tietoturvasääntöjen noudattamista.

Inhimillisten tekijöiden keskeinen rooli kyberturvallisuudessa on kasvanut, ja niillä on todettu olevan vaikutusta sekä haavoittuvuuksiin että resilienssin muodostumiseen [29]. Pelkät teknologiset ratkaisut eivät riitä, vaan inhimillisten tekijöiden ymmärtäminen ja huomioiminen on välttämätöntä kehitettäessä kyberturvallisuusstrategioita. Teknologia voidaan kiertää hyökkäämällä ihmisen heikkouksiin, jolloin kyberturvallisuusriskit voivat toteutua. Erityisen riskialttiissa teollisuuden ympäristöissä inhimillinen tekijä on tunnistettu merkittäväksi syyksi teknisten järjestelmien vikoihin [29].

Liian vähäinen ymmärrys inhimillisten tekijöiden vaikutuksesta kyberturvallisuuteen voi johtaa sosiaalisen manipuloinnin, kuten tietojenkalasteluhyökkäysten, lisääntymiseen sekä tietomurtoihin [23]. Sosiaalinen manipulointi (engl. social engineering) tarkoittaa yksilön manipulointia siten, että yksilö tulee antaneeksi hyökkääjälle luvattoman pääsyn järjestelmiin tai tietoihin [30]. Hyökkääjä voi kerätä tietoa kohteensa verkkotoiminnasta, jonka jälkeen hän pyrkii luomaan suhteen kohteeseen. Hyökkääjä manipuloi kohteensa luottamusta tarkoituksenaan saada kohde esimerkiksi paljastamaan arkaluonteisia tietoja ja antamaan pääsyoikeus hyökkääjälle luvattomiin tietoihin. Sosiaalisen manipuloinnin hyökkäyksiä tehdään sekä yksilöitä että organisaatioita kohtaan. Arkaluontoisen tiedon vuotaminen voi tarkoittaa organisaatiolle myös merkittävää taloudellista menetystä [31]. Luonteeltaan luottavaisten ja sosiaalisten henkilöiden on todettu olevan erityisen alttiita sosiaalisen manipuloinnin hyökkäyksille [24].

Tietojenkalasteluhyökkäys (engl. phishing) on yksi tehokkaimmista ja laajimmin käytetyistä sosiaalisen manipuloinnin muodoista [32]. Tietojenkalastelussa hyökkääjä esiintyy luotettavana tahona tarkoituksenaan hankkia arkaluonteista tietoa, kuten kirjautumistietoja [33]. Tietojenkalasteluhyökkäykset ovat mahdollisia, kun yksilöt eivät tunnista riskejä eivätkä tiedosta omia haavoittuvuuksiaan. Kiireinen työympäristö ja stressi ovat esimerkkejä inhimillisistä tekijöistä, jotka altistavat tietojenkalas-

teluhyökkäyksille. Lisäksi verkossa jaettu henkilökohtainen tieto auttaa hyökkääjää tiedonkeruussa ja mahdollisten hyökkäysten kohteiden profiloinnissa. Tietojenkalastteluun liittyy yleensä jokin viesti, esimerkiksi sähköposti tai tekstiviesti, ja nykyään usein myös puhelinsoitto, joka on tehty hyvin aidoksi, vaikuttaa olevan luotettavalta lähteeltä ja vaatii yleensä kiireellistä reagointia. Tekstiviestin välityksellä tapahtuvalle tietojenkalastelulle on olemassa myös oma englanninkielinen termi smishing (sms phishing) ja puhelinsoiton välityksellä tapahtuvalle termi vishing (voice phishing). Jos viestin saaja ei kyseenalaista viestin alkuperää tai sisältöä, hän voi päätyä esimerkiksi viestin linkkien kautta antamaan pankkitunnuksensa väärennetyllä sivustolla. Hyökkääjä onnistuu näin saamaan pääsyn pankkitilille ja varastamaan sieltä rahat.

Inhimilliset tekijät luovat haavoittuvuuksia, joihin tietojenkalastelujen tekijät kohdistavat hyökkäyksensä. Tieto auttaa tunnistamaan tietojenkalasteluviestejä ja tietoisuus huomaamaan pieniäkin merkkejä, kuten vääriä URL-osoitteita, viestin epäaitoudesta [33]. Omaa oppimista voi testata ja lisätä erilaisilla koulutustarkoitukseen suunnitelluilla peleillä ja simulaatioilla, jotka opettavat tunnistamaan erilaisia tietojenkalastelumuotoja [32]. Myös totutut tavat klikkailla huolettomasti linkkejä tai aliarvioida omaa mahdollisuutta tulla huijatuksi, hyödyttävät hyökkääjiä. Inhimillisten tekijöiden tueksi tarvitaan koulutusta ja teknologioita, kuten sähköpostisuodattimia, jotka auttavat hyökkäysten torjumisessa. Käyttäjien on myös osattava järjestelmien turvallinen käyttö ja turvallisuusohjeistusten noudattaminen.

4 ISO 27001 kyberturvallisuuden viitekehyksenä

Tässä luvussa käsitellään, mitä ISO-standardit ovat ja miten niistä voi hyötyä lainsäädäntövaatimusten täyttämisessä. Käsittely keskittyy tämän työn kannalta oleelliseen standardiin ISO 27001, josta esitellään myös myöhemmin viitekehyksen muodostamiseen tarvittavat kontrollit.

4.1 ISO-organisaatio

Vuonna 1946 alkujaan 25 valtion organisaatioiden yhteistyönä perustettu The International Organization of Standardization, ISO, on maailmanlaajuinen eri alojen standardeja ja oppaita julkaiseva organisaatio [34]. Sen jäseniä ovat kansalliset standardisoimisesta vastaavat organisaatiot, joita on mukana jo 175 eri maasta, yksi organisaatio kustakin maasta. Suomen jäsenenä ja edustajana ISO:ssa on Suomen Standardisoimisliitto, SFS. Se on vuonna 1924 perustettu yhdistys, ja se vastaa myös Suomen kansallisten standardien eli SFS-standardien laatimisesta.

ISO:lla on yli 250 kansainvälistä teknistä komiteaa, joiden jäsenet ovat komitean aihealueen asiantuntijoita [34]. Komiteat vastaavat ISO-standardien laatimisesta ja päivittämisestä. Standardin laatiminen on kuitenkin yhteistyötä ja siihen osallistuu usein myös standardin tulevia käyttäjiä sekä mahdollisesti kuluttaja- ja kansalaisjärjestöjä. Uuden ISO-standardin laatiminen kestää kokonaisuudessaan noin kolme

vuotta ja hyväksyminen tapahtuu äänestämällä.

4.2 ISO-standardien asema ja merkitys

ISO-standardit ovat vapaaehtoisia suosituksia, mutta kansainvälisesti tunnustettu tapa osoittaa, että prosessit, tuotteet tai palvelut ovat laadukkaita, turvallisia ja yhteensopivia keskenään [34]. ISO-standardeja voi siis vapaasti halutessaan noudattaa ja siten osoittaa toimivansa tiettyjen yhteisten menettelytapojen mukaisesti. ISO-standardi voi myös olla sisällöltään tietyn säädöksen kaltainen. Tällöin vapaaehtoisen standardin noudattaminen tukee lainsäädäntövaatimusten täyttämistä. Kyberturvallisuusriskien hallinnassa standardin toteuttaminen tuo tekemiseen systemaattisuutta ja samalla voidaan osoittaa tekemisen olevan tiettyjen vaatimusten mukaista.

Lähtökohtaisesti standardi kertoo, mitä pitää tehdä, mutta standardia noudattavan on itse määriteltävä, miten standardin vaatimukset täytetään. Jos halutaan varmistaa ja osoittaa, että noudatetaan tietyn standardin vaatimuksia, suoritetaan sisäisiä auditointeja. Tällöin sisäinen asiantunteva henkilö määrätään tekemään järjestelmällinen selvitys siitä, että standardin määrittelemiä prosesseja ja toimintatapoja noudatetaan toiminnassa. Puutteet kirjataan ja niiden korjaamiseksi suunnitellaan toimenpiteet. Sisäisten auditointien lisäksi voidaan suorittaa ulkoisia auditointeja, jolloin puolueeton, ulkopuolinen kyseisen standardin ammattilainen suorittaa auditoinnin. Jos ulkoisen auditoinnin suorittaa kyseisen standardin akkreditoitu eli päteväksi todettu auditoija ja kaikki standardin vaatimukset täyttyvät, voidaan myöntää sertifikaatti. Suomessa auditoijan akkreditoinnin myöntää Suomen akkreditointipalvelu FINAS, joka on Työ- ja elinkeinoministeriön alaisuudessa toimiva itsenäinen ja riippumaton yksikkö [35]. Sertifikaatti osoittaa, että tietyn ISO-standardin vaatimukset täyttyvät, mutta se on kuitenkin täysin erillinen ISO-organisaatiosta, joka itse ei myönnä sertifikaatteja.

4.3 ISO 27001

ISO 27001 kuuluu laajaan tietoturvallisuuden, kyberturvallisuuden ja tietosuojan ISO 27000 -standardisarjaan. ISO/IEC 27000 esittelee tietoturvallisuuden hallintajärjestelmän (engl. information security management system, ISMS), sekä siinä käytettyä sanastoa ja määritelmiä [36]. Nämä perustiedot auttavat ymmärtämään standardia ISO 27001, joka määrittelee vaatimukset ISMS:lle lausekkein ja kontrollein. ISO/IEC 27002:2022 (jäljempänä ISO 27002) sisältää ohjeet, miten kontrolleja voidaan toteuttaa ISMS:n yhteydessä [36]. Tässä työssä keskitytään standardiin ISO 27001, mutta standardia ISO 27002 käytetään apuna kontrollien valinnassa.

Ensimmäinen ISO 27001 -standardin versio julkaistiin vuonna 2005, ja viimeisin versio on vuodelta 2022 [36]. Tässä työssä käytetään standardin SFS-EN ISO/IEC 27001:2023 englanninkielistä versiota, joka perustuu mainittuun viimeisimpään kansainväliseen versioon ISO/IEC 27001:2022.

ISO 27001 määrittelee, miten organisaation on luotava, toteutettava, ylläpidettävä ja jatkuvasti parannettava ISMS:ä [37]. Lisäksi standardi määrittelee tietoturvariskien arvioinnin ja käsittelyn vaatimukset. Standardi sopii käytettäväksi erilaisissa organisaatioissa toimialasta ja organisaation koosta riippumatta. Seuraavaksi luvuissa 4.3.1 ja 4.3.2 käsitellään standardin mukaista ISMS:n toteutusta ja ylläpitoa. Luvussa 4.3.3 perehdytään siihen, kenellä on vastuu ISMS:stä ja luvussa 4.3.4 käsitellään tämän työn kannalta tärkeitä standardin kontrolleja.

4.3.1 ISMS:n suunnittelu ja toteutus

Standardia noudattavan organisaation on itse määritettävä ja dokumentoitava oman ISMS:nsä laajuus. Rajoja varten on määritettävä ne sisäiset ja ulkoiset tekijät sekä sidosryhmät, jotka ovat merkityksellisiä tietoturvan kannalta ja vaikuttavat ISMS:n vaatimusten saavuttamiseen. Jokaisen sidosryhmän kohdalla määritetään erikseen, mitkä sidosryhmään liittyvät tietoturvavaatimukset kirjataan ISMS:än ja hallitaan

sen avulla.

Kun ISMS:lle on määritetty rajat ja tietoturvavaatimukset, pitää määritellä vaatimuksia uhkaavat riskit. Tämän jälkeen on arvioitava riskien mahdolliset seuraukset ja suunniteltava toimenpiteet riskien toteutumisen varalle. Tässä kohtaa tarvitaan kontrolleja, joihin palataan luvussa 4.3.4. Riskien lisäksi on määriteltävä tietoturvatavoitteet, jotka huomioivat suunnitellun tietoturvapolitiikan ja -vaatimukset.

4.3.2 ISMS:n ylläpito ja jatkuva parantaminen

Kun ISMS on otettu käyttöön, työ jatkuu hallintajärjestelmän ylläpidolla ja jatkuvalla parantamisella. Poikkeamien kohdalla tämä tarkoittaa, että poikkeaman käsittelyn lisäksi analysoidaan syyt poikkeaman taustalla ja opitaan niistä. Samanlaisten tai vastaavien poikkeamien ehkäisemiseksi on suunniteltava toimenpiteet ja mahdollisesti tehtävä muutoksia ISMS:än.

Prosessien jatkuvasta seurannasta ja mahdollisista mittauksista on myös huolehdittava. Näiden tarkoituksena on varmistaa, että ISMS:ssä määritellyt prosessit ovat tehokkaita ja suorituskykyisiä. Organisaation johdon vastuulla on järjestää tarkastuksia, kuten säännöllisiä johdon katselmuksia ja sisäisiä auditointeja. Johdon katselmuksissa on pohdittava jatkuvan parantamisen mahdollisuuksia ja mahdollisia muutostarpeita ISMS:än. Kaikki tarkastukset on dokumentoitava.

4.3.3 Vastuut ja resurssit

Standardia noudattavan organisaation ylimmällä johdolla on aina vastuu ISMS:sta ja tietoturvapolitiikasta suunnitteluvaiheesta alkaen. Ylin johto vastaa tarvittavien vastuiden ja valtuuksien jakamisesta, sekä riittävistä resursseista, riittävästä viestinnästä ja vaaditusta dokumentoinnista. Valtuutetuilla henkilöillä on oltava riittävä koulutus ja osaaminen tehtävään, ja näitä taitoja on ylläpidettävä ja tarvittaessa tarjottava lisäkoulutusta. Viestinnän osalta on oltava suunnitelma sisäiselle ja ul-

koiselle viestinnälle, ja määritettävä, mitä, milloin, miten ja kenelle viestitään. Dokumentointi on erittäin tärkeää joka vaiheessa, ja esimerkiksi kaikki suunnitelmat, tapahtumat ja muutokset on dokumentoitava. Dokumentaatiot on oltava helposti saatavilla, mutta kuitenkin riittävän suojatusti tallennettuina.

Organisaation ylimmän johdon vastuulla on tietoturvavaatimusten integroiminen kaikkiin organisaation prosesseihin [37]. Tästäkin syystä koko henkilöstön on oltava tietoinen tietoturvapolitiikan ja ISMS:n sisällöstä. Jokaisen on ymmärrettävä vastuunsa ja velvoitteensa, sekä oltava tietoinen niistä seurauksista, joita voi aiheutua, jos ISMS:n vaatimuksia ei noudateta.

4.3.4 Kontrollit

Jotta ISMS:ssä määritelty tietoturvataso voidaan saavuttaa, on sitä varten suunnitteluvaiheessa tunnistettava, arvioitava ja käsiteltävä mahdolliset tietoturvariskit [37]. Riskiarvioinnin perusteella jokaiselle riskille määritellään käsittelyprosessi ja sen toteuttamiseen tarvittavat kontrollit. Standardissa on listattuna yhteensä 93 kontrollia, jotka on käytävä läpi jokaisen riskin kohdalla. Muitakin kuin liitteessä mainittuja kontrolleja saa käyttää. Standardi vaatii jokaisen kontrollin kohdalla dokumentoidut perustelut, miksi kontrolli valittiin tai jätettiin valitsematta. Kontrollien valinnat ja poisjättämiset perusteluineen dokumentoidaan sovellettavuuslausuntoon (engl. Statement of Applicability, SoA). Jokaisen valitun kontrollin kohdalle merkitään myös sen edellyttämät toimenpiteet ja onko ne jo toteutettu. SoA:a ylläpidetään jatkuvasti osana ISMS:n hallintaa.

Standardissa kontrollit on jaettu neljään ryhmään: organisaatioon liittyviin, ihmisiin liittyviin, fyysisiin ja teknologisiin kontrolleihin. Ryhmittely kattaa organisaation tietoturvan hallinnolliset, henkilöstöön liittyvät, fyysiset ja tekniset osa-alueet.

Organisaatioon liittyvät kontrollit (engl. organizational controls, kontrollit 5.1-5.37) käsittelevät organisaation hallintoa, tietoturvakäytäntöjä ja riskienhallintaa.

Kuten Kyberturvallisuuslaki, myös ISO 27001 määrittelee, että korkein vastuu kyberturvallisuudesta on organisaation (laissa toimijan) johdolla. Standardin kontrolleja noudattamalla johto voi varmistaa vastuullisuutensa ja osallistumisensa toteutumisen.

Ihmisiin liittyviin kontrolleihin (engl. people controls, kontrollit 6.1-6.8) on koottu organisaation henkilöstöön liittyvät keskeiset kyberturvallisuuteen liittyvät asiat työsuhteen alusta loppuun. Kontrolleilla määritellään esimerkiksi ennen työsuhdetta tehtävästä taustojen tarkistuksesta. Työsuhteen aikana kontrolleilla määritellään esimerkiksi käyttöoikeuksien hallinnasta ja etätyökäytänteistä. Työsuhteen päättymisen kohdalla kontrollit määrittelevät esimerkiksi organisaation omistuksessa olevien laitteiden palautuksesta.

Fyysiset kontrollit (engl. physical controls, kontrollit 7.1-7.14) määrittelevät pääasiassa fyysisen turvallisuuden suojaamisesta, kuten kulunvalvonnasta ja organisaation omistamien laitteiden suojaamisesta organisaation tiloissa ja niiden ulkopuolella.

Teknologiset kontrollit (engl. technological controls, kontrollit 8.1-8.34) liittyvät digitaalisen infrastruktuurin suojaamiseen. Tällaisia teknologioita ovat esimerkiksi palomuurit, virustorjuntaohjelmistot, pääsynhallintajärjestelmät ja verkkojen turvallisuus.

5 Tutkimusmenetelmät

Tämä luku esittelee tämän työn tutkimusnäkökulman ja -otteen. Lisäksi esitellään inhimillisten tekijöiden ja ISO 27001 -kontrollien valintaan käytetyt tutkimusmenetelmät ja niiden päävaiheet. Viimeisenä käsitellään viitekehyksen muodostamisen ja arvioinnin lähestymistavat.

5.1 Tutkimusparadigma

Paradigma tarkoittaa tutkimukseen liittyvien oletusten ja tutkimusmenetelmien yhdistelmää. Valittu paradigma ohjaa tutkimusta ja määrittelee, miten tietoa hankitaan [38]. Se vaikuttaa myös esimerkiksi tutkimuskysymysten asettelussa ja tulosten tulkinnassa.

Tämä työ tehtiin näkökulmasta, joka parhaiten vastaa pragmatismia. Tässä työssä tieto ei ole täysin objektiivista, koska siihen sisältyy tekijän tulkintaa. Työn tuloksena tavoiteltiin kuitenkin käytännöllistä mallia. Pragmatismissa keskitytään käytännön ongelman ratkaisuun ja hyödyllisen, toimivan tuloksen tuottamiseen [39]. Pragmatismi suhtautuu tietoon välineenä, ja tiedon arvo määräytyy suoraan saavutetun tuloksen toimivuuden perusteella. Tässä työssä tämä tarkoittaa sitä, että kirjallisuuskatsauksen ja kvalitatiivisen analyysin tulokset toimivat rakennusaineina, joilla pyrittiin muodostamaan käytännöllinen ja toimiva viitekehys.

5.2 Tutkimusote

Tässä työssä ongelmaa lähestyttiin ja tutkimusta rakennettiin tieteellisen suunnittelututkimuksen näkökulmasta. Tällaisen tutkimuksen tarkoituksena on kehittää todelliseen ongelmaan ratkaisu, esimerkiksi prosessi tai työkalu, joka aidosti parantaa alkuperäistä tilannetta ymmärrettävällä tavalla [40]. Tässä työssä esitellään ja arvioidaan viitekehys, jonka avulla voidaan minimoida keskeisten inhimillisten tekijöiden aiheuttamat riskit valittujen ISO 27001 -kontrollien toteutumiselle ja samalla kyberturvallisuuslain noudattamiselle.

5.3 Kirjallisuuskatsaus

Kirjallisuuskatsauksella tarkoitetaan tutkittavan aiheen olemassa olevan kirjallisen tiedon keräämistä [40]. Kerättyyn aineistoon tutustumalla voidaan esimerkiksi tunnistaa paremmin tutkimuksessa olevia aukkoja ja näin saada suuntaa tulevalle tutkimukselle. Systemaattinen kirjallisuuskatsaus on laaja toistettavissa oleva prosessi, jonka tarkoituksena on muodostaa yhteenveto olemassa olevasta tiedosta vastaamaan asetettuihin tutkimuskysymyksiin [40], [41]. Tässä työssä kirjallisuuskatsaus tehtiin kevennetysti systemaattisen kirjallisuuskatsauksen periaatteiden mukaisesti tavoitteena vastata ensimmäiseen työlle asetettuun tutkimuskysymykseen.

5.3.1 Toteutus

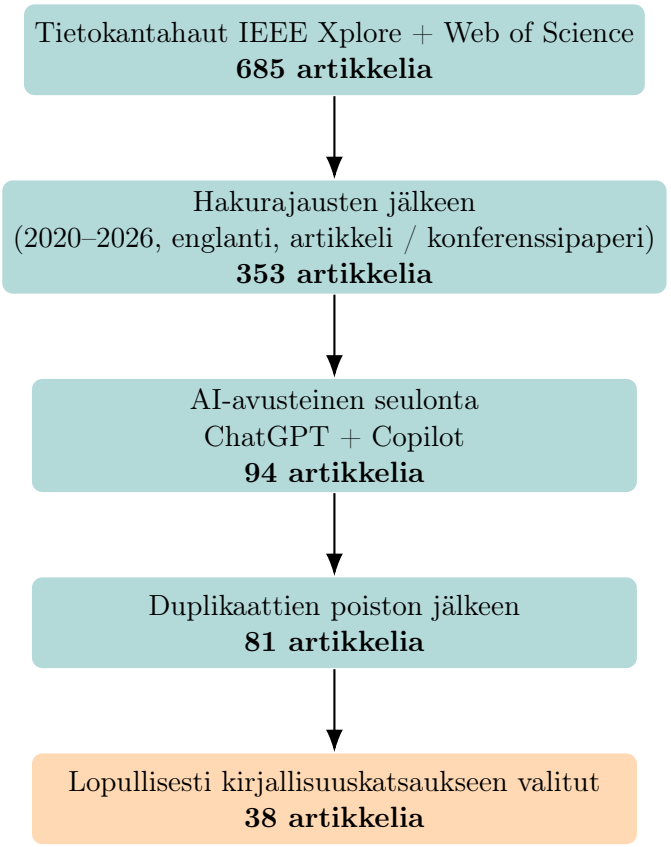
Kirjallisuuskatsaus suoritettiin samoin kriteerein kahdessa tietokannassa: IEEE Xplore (IEEE) ja Web of Science (WOS). Jotta tieto olisi ajankohtaista, tehtiin aikarajaus vuosille 2020-2026. Dokumenttityypeiksi rajattiin tieteellisissä aikakauslehdissä julkaistut artikkelit sekä konferenssipaperit, ja artikkelien kieleksi valittiin englanti. Käytetyt hakulauseet on esitetty taulukossa 5.1. Samaan taulukkoon on kirjattu hakulauseiden jälkeen molempien tietokantojen tuottamat artikkelimäärät. Ensim-

mäinen luku on artikkelien määrä pelkällä hakulauseella ja toinen luku artikkelien määrä kuvattujen hakurajausten tekemisen jälkeen.

Taulukko 5.1: Kirjallisuushakujen tulosten lukumäärät (aluksi | rajauksen jälkeen | valitut).

hakulause	**IEEE**			**WOS**		
"human factor*"AND risk AND "cyber security"	62	32	11	166	69	15
"human factor*"AND risk AND cybersecurity	176	111	34	250	139	33
"human factor*"AND 27001	3	2	0	20	1	1
"human factor*"AND "iso27001"AND control*	4	0	0	4	0	0

Hakurajausten tekemisen jälkeen taulukon 5.1 kahden ylimmän haun artikkelien seulonnassa käytettiin apuna kahta tekoälyä, ChatGPT ja Copilot. Molemmille syötettiin yksi artikkelien viitetietolistaus kerrallaan sekä ohje "Analysoi viitteiden artikkelit siten, että ehdotat, mistä artikkeleista on hyötyä vastattaessa kysymykseen: Mitkä ovat kirjallisuuden perusteella keskeiset inhimilliset tekijät, jotka ovat riski kyberturvallisuudelle?"Tekoälyjen antamat artikkelilistat poikkesivat toisistaan, joten kahden tekoälyn käyttö osoittautui perustelluksi. Joka haussa tekoälyt olivat valinneet noin kolmanneksen eri artikkeleja, ja kokonaisuudessaan Copilot valitsi hieman enemmän artikkeleja listalleen. Tekoälyjen valinnat käytiin läpi, myös niiden poisjättämät artikkelit, joista muutama valittiin mukaan. Näin saatiin kokoon valitut artikkelit, joiden lukumäärät ovat kolmantena taulukossa 5.1. Seulonnan jälkeen artikkeleita oli 94, joista duplikaattien poiston jälkeen valittiin 81. Nämä artikkelit käytiin vielä tarkemmin läpi, jonka jälkeen kirjallisuuskatsaukseen valikoitui mukaan 38 artikkelia. Valintaprosessi ja artikkelimäärät on esitetty kuvassa 5.1.



Kuva 5.1: Kirjallisuuskatsauksen artikkelien valintaprosessi.

5.4 Kvalitatiivinen tutkimus

Kvalitatiivinen eli laadullinen tutkimus on menetelmä, jonka avulla pyritään ymmärtämään ongelmia ja löytämään uusia näkökulmia [42]. Temaattinen analyysi on laadullinen tutkimusmenetelmä, jota voidaan käyttää tutkimusaineiston teemojen tunnistamiseen ja ryhmittelyyn [43]. Tällä tavalla aineistoa on helpompi edelleen analysoida ja etsiä siitä tutkimuksen kannalta merkityksellisiä tuloksia.

Tässä työssä temaattista analyysia käytettiin keskeisenä menetelmänä kirjallisuuskatsauksessa havaittujen inhimillisten tekijöiden sekä valittujen ISO 27001 -standardin kontrollien ryhmittelyssä. Inhimillisiin tekijöihin sovellettiin induktiivista päättelyä ja kontrolleihin abduktiivista päättelyä.

5.4.1 Induktiivinen päättely

Induktiivisella päättelyllä yhdistetään yksittäisiä havaintoja suuremman kokonaiskuvan luomiseksi [40]. Päättely ei takaa lopputuloksen oikeellisuutta vaan ainoastaan todennäköisyyden.

Kirjallisuuskatsauksessa tunnistetut alkuperäiset englanninkieliset inhimilliset tekijät taulukoitiin, ja samat tai samankaltaiset käsitteet yhdistettiin ryhmäksi. Jokaiselle ryhmälle valittiin mahdollisimman kattava ja kuvaava suomenkielinen vastine. Tässä vaiheessa hylättiin ne suomenkieliset tekijät, joihin kuului yksi tai kaksi englanninkielistä tekijää, jotta analyysi voitiin keskittää useammin esiintyviin ilmiöihin. Yhtä tai kahta esiintymää ei katsottu riittävän edustetuiksi valitussa kirjallisuudessa. Suomenkielisten tekijöiden ryhmittelyä jatkettiin käyttäen apuna kirjallisuuskatsauksen artikkelien aihepiirejä. Monet artikkeleista keskittyivät tietynlaisiin inhimillisiin tekijöihin, kuten kognitiivisiin [32], [33], emotionaalisiin [44] ja sosiaalisiin tekijöihin [30], [45]. Suomenkielisten tekijöiden ryhmittelyä jatkettiin, kunnes jäljellä oli kuusi ryhmää. Näiden rakenne ja määrä todettiin sopivaksi, joten ryhmittely lopetettiin. Näitä kuutta ryhmää käytettiin viitekehyksen muodostamiseen.

5.4.2 Abduktiivinen päättely

Abduktiivisessa päättelyssä olemassa olevaan teoriaan yhdistetään epätäydelliset havainnot, ja tuloksena saadaan ymmärrystä ja päätöksentekoa auttavia hypoteeseja [40]. Tällaisella prosessilla voi saada aikaiseksi uusia ideoita.

Tässä työssä abduktiivista päättelyä käytettiin kontrollien valinnassa. Kontrollit toimivat olemassa olevana teoriana ja inhimillisten tekijöiden ryhmät epätäydellisinä havaintoina. Näillä muodostettiin hypoteesi siitä, mihin kontrolleihin inhimillisillä tekijöillä voi olla vaikutusta. Standardin 93 kontrollia käytiin läpi systemaattisesti. Apuna läpikäynnissä käytettiin standardia ISO 27002, joka esittelee kontrollit laajemmin kuin ISO 27001. Kontrollien valintaan vaikutti se, onko inhimillinen tekijä

keskeisessä asemassa, jos kontrolli ei toteudu. Lisäksi painotettiin, liittyykö kontrolli päivittäiseen tekemiseen tai valmiuteen, ja vaatiiko se jatkuvaa noudattamista. Valitut kontrollit pidettiin standardin liitteen mukaisissa neljässä pääryhmässä.

5.5 Viitekehyksen muodostaminen

Viitekehys on työkalupaketti, joka sisältää periaatteita, ohjeita ja käytänteitä tietoturvallisuuden lähestymistavaksi ja hallintaan [46]. Tässä työssä muodostettiin käsitteellinen viitekehys, jonka avulla on tarkoitus nähdä yhteys tiettyjen inhimillisten tekijöiden ja ISO 27001 -standardin kontrollien välillä. Tavoitteena oli, että viitekehyksen avulla voidaan tunnistaa ja huomioida sellaiset inhimilliset tekijät, jotka voivat heikentää kontrollien toteutumista ja siten lisätä kyberturvallisuusriskiä.

Viitekehys muodostettiin yhdistämällä kirjallisuuskatsauksen perusteella valitut kyberturvallisuuteen vaikuttavat inhimilliset tekijät ja ISO 27001 -standardista valitut inhimillisiin tekijöihin liittyvät kontrollit. Lopputulos esitellään luvussa 6.3 sekä havainnollistetaan matriisiesityksenä 6.11 ja hämähäkkikaaviona 6.5.

5.6 Viitekehyksen arviointitapa

Viitekehys arvioitiin kahdella tavalla: vertailuarviointina ja asiantuntija-arviointina. Vertailuarvioinnin suoritti työn tekijä vertaamalla muodostettua viitekehystä jo olemassa oleviin vastaaviin viitekehyksiin. Asiantuntija-arvioinnin suoritti ulkopuolinen asiantuntija, jolla on tekniikan tohtorin tutkinto sekä CISSP ja ISO 27001 Lead Auditor -sertifiointi. Arviointia varten asiantuntijalle toimitettiin tässä työssä laadittu viitekehys, joka esitellään luvussa 6, sekä arviointikysely, joka on liitteessä B. Arvioinnin tavoitteena oli tarkastella viitekehyksen kattavuutta, johdonmukaisuutta ja sovellettavuutta. Kysely sisälsi väittämiä, jotka arvioitiin Likert-asteikolla. Lisäksi kyselyssä oli mahdollisuus antaa avointa palautetta.

6 Kontrolliviitekehys

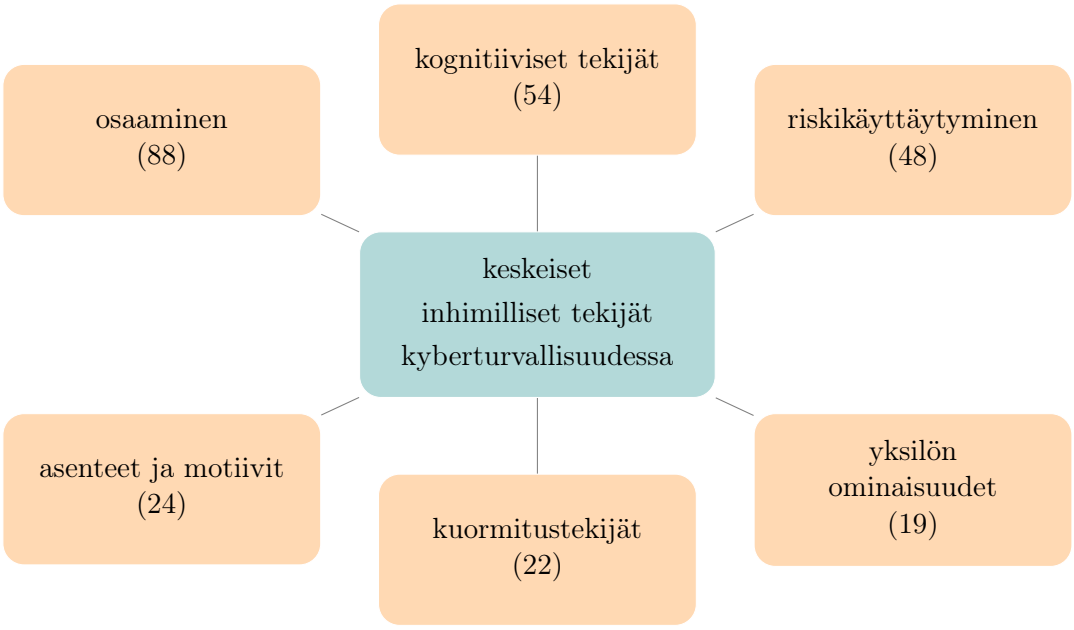
Tämä luku esittelee, mitkä inhimilliset tekijät ja ISO 27001 -kontrollit valittiin mukaan viitekehykseen ja millainen viitekehys niistä muodostui. Inhimillisten tekijöiden valinta perustui kirjallisuuskatsaukseen, jonka toteutus ja rajaukset käsiteltiin luvussa 5.3. Inhimilliset tekijät ja kontrollit analysoitiin kvalitatiivisella analyysilla, jota käsitellään luvussa 5.4. Viitekehyksen muodostamisen lähestymistavasta kerrotaan luvussa 5.5.

6.1 Keskeiset inhimilliset tekijät

Kirjallisuuskatsauksen artikkeleista käy ilmi, että ihminen on kyberturvallisuuden heikoin lenkki [43], [47], [48], [49], [50]. Ihminen voi käyttäytyä tahallaan pahantahtoisesti tai olla tietämätön oikeista toimintatavoista esimerkiksi liian vähäisen kyberturvallisuuskoulutuksen vuoksi [48]. Molemmat vaihtoehdot johtavat kyberturvallisuusriskin kasvamiseen. Yli 85 % tietomurroista ja 95 % tietoturvaloukkauksista johtuu ihmisestä [51], [52]. On kuitenkin myös tutkimuksia, joiden mukaan huono teknologinen suunnittelu on syynä ihmisen tekemiin virheisiin [43], [53]. Huono ohjelmiston käytettävyys voi johtaa tahalliseen sääntöjen rikkomiseen. Tosin huonosti suunniteltu ja toteutettu järjestelmä on pääasiassa edelleen ihmisen vastuulla, jolloin päädytään taas ihmisen tekemään virheeseen. Teknisissä järjestelmissä vakavin riski on järjestelmää käyttävä ihminen [49]. Osaamista ja tietoisuutta lisäämällä tilanne voidaan muuttaa. Ihminen voi olla tärkeä lenkki kyberturvallisuuden vahvistajana,

jos ihmisen intuitio osataan hyödyntää oikealla tavalla kyberturvallisuuden etulinjassa [47]. Inhimillisten tekijöiden tunnistaminen on siis tärkeää, jotta ihminen on kyberturvallisuuden vahvuus eikä heikkous.

Seuraavaksi esitellään muodostetut pääryhmät kirjallisuuskatsauksessa tunnistetuista keskeisistä inhimillisistä tekijöistä. Muodostetut pääryhmät on esitetty kuvassa 6.1. Jokainen pääryhmä on esitelty omassa alaluvussaan, joka sisältää myös taulukon pääryhmän inhimillisistä tekijöistä. Taulukoissa on kerrottu, kuinka monessa kirjallisuuskatsauksen artikkeleista mikäkin inhimillinen tekijä esiintyi. Lisäksi liitteen A taulukossa listataan kaikki työssä mukana olevat inhimilliset tekijät, sekä niiden alkuperäiset englanninkieliset käsitteet viitetietoineen.



Kuva 6.1: Kirjallisuuskatsauksessa tunnistetuista kyberturvallisuuteen vaikuttavista inhimillisistä tekijöistä muodostetut pääryhmät. Luku kertoo kaikkien kyseiseen ryhmään valittujen inhimillisten tekijöiden esiintymismäärien summan. Inhimillisen tekijän esiintymismäärä kertoo, kuinka monessa kirjallisuuskatsauksen artikkeleista kyseinen inhimillinen tekijä esiintyi.

6.1.1 Osaaminen

Erilaisen tiedon, tietoisuuden sekä koulutuksen ja harjoittelun riittämättömyys osoittautuivat kirjallisuuskatsauksen perusteella yleisimmiksi tekijöiksi, jotka voivat lisätä kyberturvallisuusriskejä. Tieto on ymmärtämistä kyberturvallisuusriskeistä, niiden toimintaperiaatteista ja vaikutuksista. Ilman riittävää tietoa on vaikea ymmärtää, millaisia riskejä eri toimintoihin voi liittyä. Tietoisuuden puute johtaa siihen, ettei huomata ympäristön tapahtumia ja riskejä [33]. Tämä voi heikentää riskien, kuten tietojenkalasteluviestien ja haitallisten linkkien, tunnistamista käytännön tilanteissa. Koulutus ja harjoittelu lisäävät yksilön tietoa [33]. Tiedon karttuminen puolestaan vahvistaa tietoisuutta, sillä oppimisen myötä yksilö alkaa tunnistaa ja havaita oppimiaan asioita myös omassa toimintaympäristössään. Tietoisuus ja tieto vahvistavat siten toisiaan: lisääntynyt tieto tukee havaintojen tekemistä, ja havainnot sekä uudet kokemukset voivat edelleen syventää tietoa [45].

Terveydenhuollossa tehdyssä tutkimuksessa on havaittu, että kokemukset ja tieto voivat vaikuttaa tietoisuuteen ja sen kehittymiseen [54]. Tietämättömyys voi johtua esimerkiksi riittämättömästä koulutuksesta [48]. Kyberturvallisuustietoisuuden taso vaikuttaa siihen, miten hyvin uhkia tunnistetaan ja miten niihin reagoidaan. Yhdistyneiden Arabiemiirikuntien ja Yhdysvaltojen väestöjä vertailtaessa tutkimuksessa havaittiin, että matalampi tietoisuuden taso oli yhteydessä heikompaan kyberturvallisuuskäyttäytymiseen, kuten salasanojen suojauksen laiminlyöntiin ja tietojenkalasteluviestien tunnistamisen vaikeuteen [55].

Tämän pääryhmän tekijät, jotka on lueteltu taulukossa 6.1, ovat siis selvästi yhteydessä ja vaikuttavat toisiinsa. Koulutus näyttäytyy vahvasti taustatekijänä [56]. Koulutus ja kokemukset kasvattavat tietoa ja vähentävät tietämättömyyttä. Pelkkä koulutus ei kuitenkaan riitä, jos se ei johda todelliseen ymmärrykseen ja tietoisuuteen eli kykyyn tunnistaa ja tulkita riskejä oikein silloin, kun niitä tulee vastaan arjen tilanteissa.

Noin 87 % kirjallisuuskatsauksen artikkeleista mainitsi ainakin yhden tämän ryhmän inhimillisistä tekijöistä. Tämä kertoo ryhmän inhimillisten tekijöiden tärkeydestä, kun pohditaan kyberturvallisuusriskejä ja niihin vaikuttamista. Näin suuri osuus voi kertoa myös siitä, että osaamisen puutteet ovat merkittävä huolenaihe ja myös yksi peruste sille, ettei teknologia yksin riitä kyberturvallisuuden varmistamisessa. Inhimillisillä tekijöillä on keskeinen rooli riskien ehkäisyssä ja uhkatilanteisiin reagoimisessa [47]. Tämän vuoksi tekniset ratkaisut on yhdistettävä esimerkiksi helposti ymmärrettäviin ohjeisiin ja riittävään koulutukseen [57]. Riittävällä osaamisella ihminen voi ongelman sijaan olla osa ratkaisua kyberturvallisuuden parantamisessa [53]. Ehkä tästä syystä osaamiseen liittyvät inhimilliset tekijät nousivat niin suureksi ryhmäksi kirjallisuuskatsauksen artikkelien tarkastelussa.

Taulukko 6.1: Osaamiseen liittyvät inhimilliset tekijät.

esiintymistä/38 artikkelia	**inhimillinen tekijä**
31	riittämätön tietoisuus
20	riittämätön koulutus ja harjoittelu
17	riittämätön tieto
9	puutteellinen ymmärrys
7	kokemuksen puute
4	tietämättömyys

6.1.2 Kognitiiviset tekijät

Kognitiivisilla tekijöillä tarkoitetaan inhimilliseen tiedonkäsittelyyn liittyviä prosesseja, kuten tarkkaavaisuutta, muistia ja toiminnanohjausta [58]. Nämä prosessit vaikuttavat siihen, miten ihminen havaitsee ja tulkitsee ympäristön tapahtumia. Siten kognitiiviset tekijät vaikuttavat myös kykyyn havaita tilanteita ja tehdä oikeita päätöksiä kyberturvallisuuteen liittyen. Tämän pääryhmän inhimilliset tekijät on listat-

tu taulukossa 6.2.

Kognitiivinen vinouma, kuten esimerkiksi optimismivinouma, aiheuttaa omien kykyjen yliarvioimista [59]. Kun kuvittelee kykynsä välttää negatiivisia tapahtumia todellisuutta suuremmiksi, vaikutus päätöksentekoon kyberturvallisuustilanteessa voi olla merkittävä ja voi johtaa riskikäyttäytymiseen ja altistaa uhkien toteutumiselle. Tietoisuuskampanjat ja koulutukset eivät välttämättä riitä korjaamaan tällaisia ongelmia, sillä niiden taustalla vaikuttavat psykologiset käyttäytymismallit.

Kognitiivisiin tekijöihin vaikuttavat erilaiset kuormitustekijät, kuten stressi ja kiire. Nämä tekijät kuuluvat tässä työssä kuormitustekijöiden pääryhmään. Tässäkin havaitaan, kuinka eri pääryhmien inhimilliset tekijät ovat yhteydessä ja vaikuttavat toisiinsa. Kuormitustekijät esitellään myöhemmin luvussa 6.1.5. Tutkimus osoittaa, että sairaalan henkilökunnan kohdalla stressin ja kiireen kasvaessa kognitiivinen kokonaiskuormitus lisääntyy, tarkkaavaisuus heikkenee ja päätöksenteko vaikeutuu [60]. Tarkkaavaisuudella tarkoitetaan kykyä keskittyä ympäristön vihjeisiin niiden ympärillä olevista häiriötekijöistä huolimatta [61]. Heikentynyt tarkkaavaisuus vaikuttaa suoraan kyberturvallisuusuhkien havaitsemiseen ja voi heikentää kykyä kiinnittää huomiota poikkeaviin tilanteisiin. Ajattelu- ja päätöksentekokyvyn kuormittuminen näkyy suoraan virheinä, riskinottona ja heikentyneenä kykynä tunnistaa uhkia [62]. Vaikka taitoa ja osaamista olisi, kyberturvallisuustilanne heikkenee, kun kognitiivinen kuorma kasvaa.

Erikoistilanteet voivat lisätä epävarmuutta ja pelkoa, joita hyökkääjät hyödyntävät huijauksissa [33]. Tällaiset tilanteet voivat lisätä psykologista kuormitusta ja voivat heikentää kykyä arvioida riskejä ja tehdä turvallisia, sääntöjenmukaisia päätöksiä. Tietojenkalasteluhyökkäyksissä voidaan käyttää hyväksi yksilön pelkoa, jotta hyökkääjä saa uhrin toimimaan haluamallaan tavalla [31]. Pelko voi vaikuttaa siihen, ettei riskien havaitsemisesta tai toteutumisesta uskalleta raportoida. Mahdolliset seuraukset ja syyllistäminen voivat pelottaa liikaa [53].

Emotionaalisella haavoittuvuudella tarkoitetaan altistumista manipulaatiolle tunteiden kautta. Tällaisessa tilanteessa hyökkääjä voi pyrkiä herättämään kohteessaan voimakkaita tunteita, kuten pelkoa, ohjatakseen kohteensa toimimaan haluamallaan tavalla [31]. Kohteen harkintakyky voi heiketä ja johtaa haitallisiin päätöksiin kyberturvallisuuden näkökulmasta.

Tunteisiin perustuva manipulointi on keskeinen osa sosiaalisen manipuloinnin hyökkäyksiä. Tunnetilat voivat vaikuttaa merkittävästi yksilön toimintaan eikä voimakkaiden tunteiden vaikutuksessa välttämättä kyetä toimimaan täysin rationaalisesti. Hyökkääjät voivat käyttää tällaisia tilanteita saadakseen yksilön toimimaan hyökkääjän haluamalla tavalla. Seurauksena voi olla taloudellisia menetyksiä tai arkaluontoisen tiedon vuotamista. Kyberturvallisuusriskien hallinnassa onkin syytä huomioida myös yksilöiden yleinen hyvinvointi, kuormitus ja alttius emotionaaliselle vaikuttamiselle. [45]

Jotta kyberturvallisuusriskit voidaan havaita tehokkaasti ja tarpeeksi ajoissa, tarvitaan käyttäjien valppautta, jatkuvaa valvontaa ja tietoturvahälytyksiä [61]. Tarvitaan siis sekä automaatiota että ihmisen toimintaa. Jos ympäristössä tulee jatkuvasti hälytyksiä, siitä voi seurata herkkyyden heikkenemistä hälytyksille ja siten uhkatietoisuuden vähenemistä [62]. Tämä tarkoittaa, että hälytyksiä tulee jatkuvasti ja niin paljon, ettei niihin enää ehditä tai jakseta reagoida. Tällainen tilanne voi olla esimerkiksi tietoturvavalvomon analyytikoilla. Seuraus on hälytysväsymys, joka lisää kognitiivista kuormitusta ja voi johtaa loppuunpalamiseen [63].

Kognitiiviset tekijät vaikuttavat joko parantaen tai heikentäen suoriutumista [32]. Nämä tekijät liittyvät vahvasti päätöksentekoon ja ongelmanratkaisuun. Näin ollen kognitiiviset tekijät voivat vaikuttaa merkittävästi yksilön kykyyn havaita ja arvioida kyberturvallisuusuhkia.

Taulukko 6.2: Kognitiiviset inhimilliset tekijät.

esiintymistä/38 artikkelia	**inhimillinen tekijä**
11	riskien havaitsemisen haasteet
8	kognitiiviset vinoumat ja harhat
8	kognitiivinen kuormitus
7	päätöksenteon haasteet
7	heikentynyt tarkkaavaisuus
5	pelko
4	emotionaalinen haavoittuvuus
4	hälytysväsymys

6.1.3 Riskikäyttäytyminen

Riskikäyttäytymisen pääryhmään on koottu ne inhimilliset tekijät, jotka lisäävät riskikäyttäytymistä tietoisesti tai tiedostamatta. Nämä on lueteltu taulukossa 6.3Ryhmän yleisin tekijä on riskialtis käyttäytyminen, joka kyberturvallisuusriskinä tuli esille lähes 37 %:ssa tarkastelluista artikkeleista. Riskialttiissa käyttäytymisessä sääntöjen rikkominen voi johtua esimerkiksi mukavuudenhalusta, riskien vähättelystä tai luottamuksesta siihen, ettei mitään haitallista tapahdu [59]. Riskialttiiseen käyttäytymiseen voivat vaikuttaa myös esimerkiksi väsymys ja ikä [59], joka osoittaa yhteyden tämän työn eri pääryhmien välillä. Ohjeiden ohittamiseen houkuttelee esimerkiksi kiire [51], joka tässä työssä on asetettu kuormitustekijöiden pääryhmään. Riskialtis käyttäytyminen voi myös johtua siitä, että ei tiedetä, miten pitäisi toimia. Impulsiivisesti eli harkitsemattomasti käyttäytyvät voivat altistua muita helpommin tietoturvariskeille esimerkiksi avaamalla epäilyttäviä linkkejä tai jättämällä tietoturvavaroitukset huomioimatta [50].

Ihmisen luottamuksen hyväksikäyttäminen on helpompaa kuin monen hakkeroin-

tiohjelmiston käyttö [42]. Luottamuksen hyväksikäyttäminen tarkoittaa, että tutkittuaan kohteensa taustatietoja, hyökkääjä pyrkii saamaan kohteensa luottamuksen ja sen jälkeen toimimaan tavalla, joka johtaa tietoturvan rikkomiseen ja esimerkiksi henkilötietojen tai käyttöoikeuksien vuotamiseen hyökkääjälle. Ylivarmuus voi kohdistua omaan osaamiseen, jolloin liian itsevarmana omista taidoistaan voikin ongelmia ratkoessaan luoda uusia ongelmia tai pahentaa alkuperäistä tilannetta [53]. Luottamushaasteet eivät koske vain kokemattomia käyttäjiä, vaan jopa kyberturvallisuuden ammattilaiset voivat epäonnistua luottamukseen liittyvissä sosiaalisen manipuloinnin testeissä [64]. Tietämättömyys riskeistä, omien kykyjen väärinarviointi ja liiallinen luottamus viesteihin tai ihmisiin voi altistaa esimerkiksi sosiaaliselle manipuloinnille ja tietojenkalastelulle.

Tehokkaana pidetty käänteinen sosiaalinen manipulointi perustuu siihen, että hyökkääjä saavuttaa hyökkäyksen uhrinsa luottamuksen [31]. Kun tämän jälkeen uhrille aiheutetaan ongelma, hän ottaa itse oma-aloitteisesti yhteyttä hyökkääjään. Uhri luottaa saavansa tilanteeseensa apua hyökkääjältä, joka kuitenkin käyttää tilaisuuden hyväkseen ja pääsee uhrin avustuksella varastamaan luottamuksellisia tietoja tai saa uhrin siirtämään hyökkääjälle rahaa. Myös jatkuvasti yleistyviin romanssihuijauksiin käytetään uhrin sosiaalista manipulointia emotionaalisten tekijöiden ja liiallisen luottamuksen kautta [31].

Huolimattomuus tarkoittaa huolellisuuden laiminlyöntiä eli tekemiseen ei keskitytä ja kiinnitetä tarpeeksi huomiota, jolloin lopputuloksena voi olla virhe tai vahinko. Yksi tyypillinen huolimattomuusvirhe voi tapahtua sähköpostia lähetettäessä, kun hyväksytään sähköpostiohjelman ehdottama vastaanottajan osoite tarkistamatta, onko se halutun vastaanottajan osoite [42]. Näin luottamuksellista tietoa voi päätyä väärälle vastaanottajalle.

Sääntöjen rikkominen eroaa riskialttiista käyttäytymisestä siinä, että sääntöjen rikkominen on aina tietoinen päätös ja teko. Rikkominen voi olla laiminlyönti, vaikka

säännöt ja toimintatavat tiedetään, tai tahallinen sääntöjen kiertäminen, jos säännön koetaan olevan esteenä työn sujuvalle etenemiselle [65]. Sääntöjen rikkomista on esimerkiksi sääntöjen vastaisesti kollegan tunnusten käyttäminen työn nopeuttamiseksi [53]. Tämä eroaa aiemmasta tunnustenkäyttöesimerkistä juuri siinä, että nyt toisen tunnuksia käytetään tietoisella päätöksellä, vaikka tarkasti tiedetään, että toiminnalla rikotaan sääntöjä. Aiemmin esitetty esimerkki tunnusten jakamisesta riskialttiissa käytöksessä tarkoitti sitä, että ei edes ajateltu rikottavan sääntöjä tunnuksia jaettaessa.

Uteliaisuus on psykologinen piirre, jota hyökkääjät hyödyntävät sosiaalisessa manipuloinnissa [66]. Hyökkääjän ei tarvitse olla teknisesti taitava, vaan hän voi käyttää hyväkseen kohteen uteliaisuutta saadakseen hänet avaamaan esimerkiksi sähköpostin liitetiedoston tai haitallisen linkin [31]. Tällainen toiminta voi johtaa haitallisten ohjelmien asentumiseen tai arkaluontoisten tietojen päätymiseen hyökkääjälle.

Edellä kuvatut inhimilliset tekijät ja niiden seuraukset osoittavat, että käyttäytymiseen ja psykologisiin ominaisuuksiin liittyvät piirteet voivat merkittävästi vaikuttaa kyberturvallisuusriskien syntymiseen ja lisääntymiseen.

Taulukko 6.3: Riskikäyttäytymiseen liittyvät inhimilliset tekijät.

esiintymistä/38 artikkelia	**inhimillinen tekijä**
14	riskialtis käyttäytyminen
13	luottamushaasteet
11	huolimattomuus
7	sääntöjen rikkominen
3	liiallinen uteliaisuus

6.1.4 Asenteet ja motiivit

Asenteiden ja motiivien pääryhmään on koottu inhimillisiä tekijöitä, jotka vaikuttavat yksilön suhtautumiseen kyberturvallisuuteen, ja voivat siten lisätä kyberturvallisuusriskejä. Nämä on listattu taulukkoon 6.4.

Asenne kertoo, mitä ihminen ajattelee ja tuntee, ja se voi olla myönteistä tai kielteistä. Yksilön asenne tietoturvaa kohtaan vaikuttaa suoraan siihen, miten hän käyttäytyy ja toimii tietoturvakäytäntöjen suhteen [51]. Teknologiaan kohdistuva liiallinen luottamus voi heikentää käyttäjän kykyä tunnistaa kyberturvallisuusriskejä [61]. Autonomisissa järjestelmissä hyökkääjä voi manipuloida käyttäjän liiallista luottamusta järjestelmään esimerkiksi syöttämällä vääriä hälytyksiä tai viestejä käyttöliittymään. Tämä voi johtaa siihen, että käyttäjä reagoi liian hitaasti tai tekee vääriä päätöksiä kriittisissä tilanteissa [67].

Pahantahtoinen toiminta voi tarkoittaa esimerkiksi haitallisen sisäpiiriläisen tekemää hyökkäystä [68]. Sisäpiiriläisellä tarkoitetaan esimerkiksi luvalla organisaatiossa toimivaa henkilöä, kuten työntekijää, joka kuitenkin toimii organisaation etuja vastaan. Aiemmin tässä luvussa käsitelty huolimattomuus voi johtaa tahattomaan sisäpiiriläisenä toimimiseen, jolloin hyökkääjä saa pääsyn organisaation järjestelmiin [69]. Omien etujen asettaminen muiden edelle voi johtaa itsekkääseen ja haitalliseen toimintaan ja siten kybervahinkoihin [69]. Tällaisen toiminnan taustalla voi olla esimerkiksi tyytymättömyys tai taloudellisen hyödyn tavoittelu. Sisäpiiriuhat ovat yksi vahingollisimmista kyberhyökkäysmuodoista [50]. Ne voivat aiheuttaa organisaatioille merkittäviä taloudellisia tappioita ja immateriaalioikeuksien menetyksiä. Lisäksi sisäpiiriläinen voi pahantahtoisuudellaan esimerkiksi uudelleenkonfiguroida järjestelmiä toimimaan väärin, manipuloida dataa ja estää hälytysjärjestelmiä toimimasta [70].

Välinpitämättömyys voi olla sääntöjen tahallista huomiotta jättämistä, mutta myös sitä, ettei tiedä toimivansa väärin. Kyberturvallisuusasioista ei osata ehkä vä-

liittää riittämättömän koulutuksen takia, ja sääntöjä tulee tiedostamatta rikottua työtehtävien sujuvoittamiseksi [69]. Huolimattomuus voi altistaa vaarojen aliarvioimiselle tai tietojenkalastelulle [32], [33].

Väärät uskomukset voivat olla konkreettisia virheellisiä käsityksiä esimerkiksi siitä, miten tietojenkalastelu toimii tai millainen on turvallinen salasana [71]. Toisaalta ne voivat olla myös emotionaalisia käsityksiä, kuten yleinen pelko teknologiaa kohtaan.

Asenteet ja motiivit voivat ilmetä sekä tahallisena vahingoittamisena että tilanteina, joissa turvallisuusohjeita sivuutetaan tietoisesti muiden tavoitteiden, kuten työn sujuvuuden, kustannuksella. Molemmat ilmiöt voivat johtaa merkittävään kyberturvallisuusriskien lisääntymiseen.

Taulukko 6.4: Asenteisiin ja motiiveihin liittyvät inhimilliset tekijät.

esiintymistä/38 artikkelia	**inhimillinen tekijä**
7	asennehaasteet
6	liiallinen teknologiaan luottaminen
4	pahantahtoinen toiminta
4	välinpitämättömyys
3	väärät uskomukset

6.1.5 Kuormitustekijät

Kuormitustekijöiden pääryhmään kuuluvat inhimilliset tekijät, jotka kuormittavat ihmistä fyysisesti tai henkisesti. Tällaisia tekijöitä ovat esimerkiksi stressi, kiire ja väsymys, jotka on listattu taulukkoon 6.5. Mainitut inhimilliset tekijät johtavat edelleen kuormituksen kasvamiseen, josta voi edelleen seurata esimerkiksi toimintakyvyn, tarkkaavaisuuden ja päätöksenteon heikkenemistä [60].

Stressi esiintyi 26 %:ssa kirjallisuuskatsauksen artikkeleista kyberturvallisuus-

riskinä. Esimerkiksi sairaaloissa työskentelevillä työympäristö on stressaava, mikä vähentää työntekijöiden kykyä tunnistaa tietojenkalasteluhyökkäyksiä [60]. Henkilöstöpulasta ja liian suuresta työmäärästä johtuva stressi altistavat terveydenhuollon henkilökunnan tekemään huonoja päätöksiä [72]. On kuitenkin mainitsemisen arvoista, että stressi esiintyi eräässä artikkelissa myös positiivisena tekijänä. Artikkelissa todettiin, että tietyn tason stressi voi jopa edistää tietoturvatietoisuutta ja vaikuttaa positiivisesti riskien tiedostamiseen [73].

Väsymys lisää kognitiivista kuormitusta, josta seuraa heikentynyt päätöksenteko ja vähentynyt tarkkaavaisuus, mikä vaikuttaa merkittävästi kyberturvallisuuskäytäntöjen noudattamiseen [59], [62]. Myös aikapaine voi lisätä hyökkääjien kohteeksi joutumista [32]. Mitä kiireellisempi työtilanne, sitä enemmän esiintyy riskialtista käyttäytymistä [51].

Taulukko 6.5: Kuormitustekijöihin liittyvät inhimilliset tekijät.

esiintymistä/38 artikkelia	**inhimillinen tekijä**
10	stressi
7	väsymys
5	paine ja kiire

6.1.6 Yksilön ominaisuudet

Yksilön ominaisuuksilla tarkoitetaan piirteitä, jotka tekevät hänestä ainutlaatuisen ja erottavat hänet muista yksilöistä. Yksi keskeisistä kyberturvallisuusriskeihin vaikuttavista yksilön ominaisuuksista on ikä [59]. Muita tässä työssä mukana olevia yksilön ominaisuuksia ovat sukupuoli ja persoonallisuus. Tämän pääryhmän inhimilliset tekijät on listattu taulukkoon 6.6.

Sekä nuoremmat että vanhemmat ikäluokat voivat olla alttiita kyberturvallisuusriskeille. Vanhemmilta ikäluokilta voi puuttua kiinnostus ja taidot teknologiaa

kohtaan. Teknologian käyttöä ja siihen liittyviä uhkia voi myös olla vaikeampi ymmärtää ja omaksua, mikä altistaa erilaisille huijauksille, kuten tietojenkalastelulle. Nuoremmilla käyttäjillä voi olla paremmat tekniset taidot ja rutiini käyttää teknologiaa. Heillä on kuitenkin suurempi taipumus liialliseen henkilökohtaisten tietojen jakamiseen verkossa [59]. Hyökkääjät voivat kerätä jaettua tietoa sosiaalisesta mediasta ja käyttää sitä yksilöiden profilointiin sekä kohdennettujen hyökkäysten toteuttamiseen.

Nuorille työharjoittelijoille Espanjassa tehdyssä kyselytutkimuksessa ikä ja sukupuoli vaikuttivat yksilöiden arvioihin omasta toimintakyvystään kyberhyökkäystilanteessa [52]. Nuorimmat vastaajat kokivat eniten epävarmuutta kyvystään toimia tilanteessa asianmukaisesti. Miesvastaajat ilmaisivat naisvastaajia enemmän itsevarmuutta omasta toimintakyvystään, vaikka heidän kokemansa osaaminen ei välttämättä ollut naisvastaajia korkeampaa. Vastaava sukupuoliero on havaittu myös slovenialaisten päätöksentekijöiden tietoisuustasossa, jossa miehet osoittautuivat naisia tietoisemmiksi useimmissa kyberuhkatilanteissa ja -ratkaisuissa [74].

Yksilön persoonallisuuden ominaisuudet, kuten ulospäinsuuntautuneisuus ja emotionaalinen epävakaus, ovat yhteydessä vahingossa tapahtuvaan tiedonjakoon [43]. Tämä voi altistaa hyökkääjien tekemälle yksilön sosiaaliselle manipuloinnille, jolla esimerkiksi kerätään arkaluonteista tietoa, kuten käyttäjätunnuksia. Myös ylikorostunut itsevarmuus omista kyvyistä on persoonallisuuteen liittyvä yksilöllinen piirre, joka voi johtaa kyberturvallisuusriskien aliarvioimiseen [75].

Yksilön ominaisuudet vaikuttavat siihen, miten kyberturvallisuusuhkia havaitaan ja arvioidaan. Tämä voi lisätä tai vähentää kyberturvallisuusriskejä. Osa yksilön ominaisuuksista on melko pysyviä, kun taas osa voi muuttua esimerkiksi kokemusten ja elämäntilanteen vaikutuksesta. Yksilöiden erilaiset ominaisuudet on syytä huomioida esimerkiksi järjestelmiä ja koulutuksia suunniteltaessa. Se, mikä sopii yhdelle yksilölle, ei välttämättä sovi toiselle.

Taulukko 6.6: Yksilön ominaisuuksiin liittyvät inhimilliset tekijät.

esiintymistä/38 artikkelia	**inhimillinen tekijä**
8	ikä
6	sukupuoli
5	persoonallisuus

6.2 Keskeiset ISO 27001 -kontrollit

Viitekehykseen valikoituneet kontrollit valittiin luvussa 5.4 kuvatulla menetelmällä painottaen inhimillisten tekijöiden roolia kontrollin epäonnistumisessa. Valitut kontrollit esitellään seuraavissa alaluvuissa standardin liitteen mukaisissa neljässä pääryhmässä.

6.2.1 Organisaatioon liittyvät kontrollit

Organisaatioon liittyvissä kontrolleissa inhimillisillä tekijöillä osoittautui olevan keskeinen rooli. Vaikka kontrollit määritellään organisaatiotasolla, niiden käytännön toteutuminen edellyttää aina ihmisen toimintaa. Tämän ryhmän kontrollit ja niiden yhteydet inhimillisten tekijöiden pääryhmiin on esitetty taulukossa 6.7.

Kontrollin 5.4 mukaan organisaation johdon vastuulla on seurata ja varmistaa, että henkilöstö noudattaa tietoturvavaatimuksia [76]. Johto seuraa aktiivisesti henkilöstön toimintaa ja myös puuttuu tarvittaessa havaittuihin poikkeamiin. Kuormitustekijät, kuten väsymys ja stressi, ja riskikäyttäytyminen, kuten huolimattomuus, voivat kuitenkin johtaa siihen, että valvonta ei toteudu systemaattisesti tai poikkeamiin ei reagoida [53]. Haasteena voi myös olla osaaminen, kuten riittämätön tietoisuus, jolloin johto ei tiedä, mitä pitää valvoa ja valvonta epäonnistuu [74]. Myös välinpitämätön asenne voi johtaa siihen, että johto ei pidä valvontaa tärkeänä [53].

Nämä tekijät voivat johtaa tämän kontrollin toteutumisen heikentymiseen.

Kontrolli 5.8 määrittelee, että tietoturva on huomioitava myös kaikissa organisaation projekteissa [76]. Projekti kestää aina tietyn aikaa ja siihen on varattu tietyt resurssit. Kuormitustekijät, kuten kiire ja ylikuormitus, voivat johtaa siihen, ettei tietoturva-asioita huomioida riittävällä tavalla [53]. On tärkeää tunnistaa ja huomioida tietoturvavaatimukset sekä projektin suunnittelussa että toteutuksessa, koska riskikäyttäytyminen, kuten huolimattomuus tai sääntöjen rikkominen, voi johtaa tietoturvavaatimusten laiminlyöntiin ja altistaa projektin tietoturvariskeille. Projektihenkilöstöltä voi myös puuttua tarpeellista tietoturvaosaamista, joka altistaa tietoturvariskeille [52]. Riittämätön tieto yhdessä kuormitustekijöiden ja riskikäyttäytymisen kanssa voivat heikentää tämän kontrollin toteutumista.

Kontrollin 5.10 mukaan tiedon ja laitteiden hyväksyttävälle käytölle on oltava turvallisen käytön säännöt [76]. Käyttäjien on tunnettava laaditut säännöt ja noudatettava niitä. Osaaminen, kuten riittämätön tietoisuus, voi johtaa siihen, että käyttäjä ei ymmärrä esimerkiksi laitteiden lukitsemisen merkitystä [65]. Lisäksi asennehaasteet voivat johtaa siihen, ettei sääntöjä noudateta [53]. Tähän liittyy myös riskikäyttäytyminen, kuten sääntöjen rikkominen ja huolimattomuus, jotka voivat johtaa laitteiden väärinkäyttöön [65]. Laite voi jäädä lukitsematta ja altistua luvattomalle käytölle, mikä voi heikentää tämän kontrollin toteutumista.

Myös tiedonsiirrolle on oltava turvalliset käytännöt ja toimintatavat [76]. Kontrolli 5.14 velvoittaa, että tiedonsiirrolle, tiedonsiirtolaitteille ja niiden käytölle on oltava tarpeelliset sopimukset ja käyttösäännöt. Tämä koskee kaikkea tietoa eri muodoissa, esimerkiksi tietokoneen kovalevyjä, sähköpostia, papereita ja kokouskeskusteluja. Osapuolilla on oltava riittävä osaaminen, jotta eri tiedonsiirtomuotojen erityispiirteet tulee huomioitua [53]. Tämä voi vaatia esimerkiksi johdon, IT-osaston ja mahdollisesti lakiosaston yhteistyötä. Kuormitustekijät, kuten väsymys ja kiire, voivat haitata sopimusten ja sääntöjen sisällön tekemistä ja hyväksymistä [53]. Näistä

voi seurata, että tämän kontrollin toteutuminen heikkenee.

Kontrolli 5.17 käsittelee salasanojen ja muiden tunnistautumistietojen turvassa pitämistä, ja uusien käyttäjien henkilöllisyyden tarkistamista ennen tunnusten luovuttamista [76]. Riskikäyttäytyminen, kuten luottamushaasteet, ja kognitiiviset tekijät, kuten kognitiivinen kuormitus, voivat johtaa henkilöllisyyden tarkistamisen laiminlyöntiin. Riskikäyttäytymistä, kuten riskien vähättelyä, on salasanojen jakaminen toisille käyttäjille tai salasanojen turvaton säilyttäminen esimerkiksi kirjoitettuna näkyvälle paikalle [33]. Myös kuormitustekijät, kuten paine ja kiire, voivat johtaa kirjautumistietojen jakamiseen [53]. Tällöin tunnistautumistiedot voivat päätyä asiattomille henkilöille, mikä mahdollistaa luvattoman pääsyn järjestelmiin ja tietoihin sekä altistaa tietovuodoille. Mainitut asiat voivat heikentää tämän kontrollin toteutumista.

Kontrolli 5.18 velvoittaa, että käyttöoikeudet on myönnettävä, tarkistettava ja poistettava hallitusti [76]. Käyttöoikeuksia on hallittava systemaattisesti ja muutokset on toteutettava ajallaan. Kuormitustekijät, kuten stressi ja paine, voivat kuitenkin aiheuttaa viivästyksiä käyttöoikeuksien päivittämiseen tai ne voi jäädä kokonaan tekemättä [53]. Kognitiivisesta kuormituksesta voi seurata, että esimerkiksi organisaatiossa työt lopettaneen henkilön tunnukset jäävät voimaan tai työtehtävien muuttuessa pääsyoikeuksia ei päivitetä [33], jolloin väärinkäytökset ja tietovuodot ovat mahdollisia. Jos pääsynhallinta ei ole ajan tasalla, tämän kontrollin toteutuminen voi heikentyä.

Kontrolli 5.23 vaatii, että pilvipalveluiden käytön tietoturvaa on hallittava asianmukaisesti [76]. Kolmannen osapuolen pilvipalveluita käytettäessä prosessit on määriteltävä palveluntarjoajan kanssa vastaamaan organisaation tietoturvavaatimuksia. Niitä on valvottava ja valvonta dokumentoitava koko sopimuksen voimassaolon ajan. Sopimusten sisällön ymmärtäminen ja tietoturvavaatimusten määrittäminen vaativat osaamista [52]. Riskikäyttäytyminen, kuten luottamushaasteet, voi aiheuttaa

liiallista luottamista palveluntarjoajaan esimerkiksi sopimusta määriteltäessä [45]. Kuormitustekijät, kuten kiire ja stressi, voivat vaikuttaa valvonnan laiminlyöntiin [61]. Nämä voivat heikentää tämän kontrollin toteutumista.

Kontrolli 5.26 edellyttää, että tietoturvapoikkeamiin reagoidaan ja vastataan sovitulla tavalla, joka on ennakolta määritelty ja dokumentoitu [76]. Organisaatiolla on oltava poikkeamatilanteisiin selkeät toimintaohjeet ja niiden toteuttamiseen on oltava jatkuva valmius. Poikkeamatilanteita varten organisaatiossa on oltava myös nimetty osaava tiimi, jonka tiedossa kyseiset toimintaohjeet on oltava. Osaaminen, kuten riittämätön tieto, tietoisuus ja koulutus, voivat johtaa siihen, ettei poikkeamaa tunnisteta tai ei tiedetä, miten toimia [47]. Kuormitustekijät, kuten stressi ja väsymys, voivat aiheuttaa tilanteen virhearviointia ja viivyttää reagointia [73]. Kognitiiviset tekijät, kuten kognitiivinen kuormitus ja heikentynyt tarkkaavaisuus, voivat johtaa poikkeaman tunnistamisen epäonnistumiseen tai vääriin päätöksiin reagoinnissa [61]. Osaamiseen liittyvät puutteet yhdessä kuormitustekijöiden kanssa voivat heikentää tämän kontrollin toteutumista.

Taulukko 6.7: Organisaatioon liittyvien kontrollien ja inhimillisten tekijöiden pääryhmien väliset yhteydet.

	pääryhmä					
organisaatioon liittyvät kontrollit	osaaminen	kognitiiviset tekijät	riskikäyttäytyminen	asenteet ja motiivit	kuormitustekijät	yksilön ominaisuudet
5.4 Johdon vastuut	■		■	■	■	
5.8 Tietoturva projektinhallinnassa	■		■		■	
5.10 Resurssien hyväksyttävä käyttö	■		■	■		
5.14 Tiedonsiirto	■				■	
5.17 Tunnistautumistiedot		■	■		■	
5.18 Käyttöoikeudet		■			■	
5.23 Tietoturva pilvipalveluissa	■		■		■	
5.26 Tietoturvapoikkeamiin reagointi	■	■			■	

■ Pääryhmä vaikuttaa kontrolliin. □ Ei yhteyttä.

6.2.2 Ihmisiin liittyvät kontrollit

Ihmisiin liittyvät kontrollit määrittelevät henkilöstön keskeiset tietoturvaan liittyvät vastuut ja velvoitteet työsuhteen alusta loppuun. Tämän ryhmän kontrollit ja niiden yhteydet inhimillisten tekijöiden pääryhmiin on esitetty taulukossa 6.8.

Kontrollin 6.1 mukaan taustaselvitykset uusien työntekijöiden kohdalla varmistavat, että työntekijät ovat luotettavia ja sopivia työhönsä [76]. Riskikäyttäytyminen, kuten huolimattomuus, ja kuormitustekijät, kuten kiire ja väsymys, voivat vaikut-

taa taustaselvityksen asianmukaiseen tekemiseen [73]. Jos selvitys laiminlyödään tai tehdään puutteellisesti, voi organisaatio altistua esimerkiksi sisäpiiriuhalle [69]. Siitä voi aiheutua merkittäviä tietoturvaongelmia ja immateriaalioikeuksien menetyksiä [50]. Näistä syistä tämän kontrollin toteutuminen voi heikentyä.

Kontrolli 6.2 edellyttää, että työsuhteen ehdot on määriteltävä selkeästi työsuhteen alussa tai muutostilanteissa [76]. Kuormitustekijät, kuten kiire ja väsymys, voivat aiheuttaa ehtojen riittämättömän läpikäynnin [73]. Lisäksi välinpitämätön asenne voi johtaa siihen, että ehtoja ei pidetä tärkeinä eikä niitä noudateta [53]. Tämä voi johtaa työntekijän tahattomaan ehtojen tai vaatimusten rikkomiseen ja esimerkiksi luottamuksellisten tietojen vuotamiseen. Mainitut asiat voivat heikentää tämän kontrollin toteutumista.

Kontrolli 6.3 velvoittaa, että henkilöstö on koulutettava ja valmennettava työtehtävien vaatimissa tietoturva-asioissa [76]. Osaaminen, kuten tietoisuus, on varmistettava, jotta henkilöstö osaa tunnistaa riskit ja toimia sääntöjen mukaisesti [52]. Jos koulutus laiminlyödään esimerkiksi kuormitustekijöiden, kuten kiireen vuoksi [53], voi henkilöstö altistua esimerkiksi tietojenkalastelulle. Tämä voi heikentää tämän kontrollin toteutumista.

Kontrolli 6.5 asettaa vaatimukset tiettyjen tietoturvaan liittyvien tehtävien suorittamiselle työsuhteen päättyessä tai muuttuessa [76]. Organisaation laitteet on palautettava ja pääsyoikeudet suljettava. Kuormitustekijät, kuten kiire tai väsymys, tai kognitiiviset tekijät, kuten heikentynyt tarkkaavaisuus, voivat johtaa tehtävien, kuten tunnusten tai kulkuoikeuksien sulkemisen laiminlyöntiin [53], [61]. Tästä voi seurata luvaton pääsy organisaation tiloihin tai järjestelmiin. Tämä voi heikentää tämän kontrollin toteutumista.

Kontrolli 6.6 asettaa vaatimukset luottamuksellisuus- tai salassapitosopimusten dokumentoinnille ja säännölliselle päivittämiselle [76]. Henkilöstön on ymmärrettävä sopimusten sisältö ja noudatettava niitä jokapäiväisessä työssä. Sopimusten

tarkoituksena on esimerkiksi määritellä, mitä tietoa suojataan ja miten sitä saa käsitellä. Riskikäyttäytyminen, kuten sääntöjen rikkominen tai huolimattomuus, voi aiheuttaa esimerkiksi tietovuodon [65]. Osaaminen, kuten puutteellinen ymmärrys, ja asenteet, kuten välinpitämättömyys, voivat johtaa tiedon käsittelyyn sopimuksen vastaisesti tai sen jakamiseen luvattomille tahoille [52], [53]. Nämä tekijät voivat heikentää tämän kontrollin toteutumista.

Kontrolli 6.7 vaatii, että etätyössä on noudatettava toimenpiteitä, joilla suojataan tietoa organisaation tilojen ulkopuolella työskenneltäessä [76]. Ohjeistukset koskevat sekä paperilla että laitteilla olevan tiedon käsittelyä. Osaaminen, kuten riittämätön tietoisuus, voi johtaa siihen, että suojattavaa tietoa ei tunnisteta tai osata suojata esimerkiksi julkisilla paikoilla työskenneltäessä [52]. Myös riskikäyttäytyminen, kuten huolimattomuus, tai asenteet, kuten välinpitämättömyys, voivat vaarantaa tiedon luottamuksellisuuden julkisissa tiloissa tai liikennevälineissä työskenneltäessä [53], [65]. Nämä tekijät voivat heikentää tämän kontrollin toteutumista.

Kontrolli 6.8 velvoittaa henkilöstöä raportoimaan havaitsemistaan tai epäilemistään tietoturvatapahtumista organisaation tarjoamien ilmoituskanavien kautta [76]. Kaikkien on tiedettävä ilmoituskanavasta ja osattava käyttää sitä, ja ilmoituskanavan on oltava helposti saatavilla. Osaaminen, kuten riittämätön tieto tai tietoisuus, voi johtaa siihen, että ilmoitus jätetään tekemättä tai riskejä ja tapahtumia ei tunnisteta ollenkaan [61]. Kognitiiviset tekijät, kuten pelko ja päätöksenteon haasteet, voivat aiheuttaa sen, että ilmoitus jää tekemättä [53]. Nämä tekijät voivat heikentää tämän kontrollin toteutumista.

Taulukko 6.8: Ihmisiin liittyvien kontrollien ja inhimillisten tekijöiden pääryhmien väliset yhteydet.

ihmisiin liittyvät kontrollit	pääryhmä: osaaminen	kognitiiviset tekijät	riskikäyttäytyminen	asenteet ja motiivit	kuormitustekijät	yksilön ominaisuudet
6.1 Taustaselvitykset			■		■	
6.2 Työsuhteen ehdot				■	■	
6.3 Tietoisuus, koulutus ja valmennus	■				■	
6.5 Vastuut työsuhteen päättyessä		■			■	
6.6 Salassapitosopimukset	■		■	■		
6.7 Etätyö	■		■	■		
6.8 Tietoturvatapahtumien raportointi	■	■				

■ Pääryhmä vaikuttaa kontrolliin. □ Ei yhteyttä.

6.2.3 Fyysiset kontrollit

Tämän ryhmän kontrollit liittyvät vahvasti fyysisen turvallisuuden tukemiseen, kuten kulunvalvontaan ja tilojen lukitsemiseen. Yksilön päivittäinen toiminta voi kuitenkin vaikuttaa merkittävästi osaan näistä kontrolleista. Tämän ryhmän kontrollit ja niiden yhteydet inhimillisten tekijöiden pääryhmiin on esitetty taulukossa 6.9.

Kontrollin 7.2 mukaan kulunvalvonnalla on tarkoitus varmistaa, että ainoastaan valtuutetuilla henkilöillä on pääsy tietoihin ja tiloihin [76]. Riskialttiita alueita, kuten lastauslaitureita, on erityisesti valvottava, jotta ulkopuolisia ei pääse organi-

saation tiloihin. Kuormitustekijät, kuten väsymys ja kiire, tai riskikäyttäytyminen, kuten huolimattomuus, voivat aiheuttaa riskin, että ulkopuolinen henkilö pääsee tiloihin valtuutetun henkilön mukana [43]. Myös kognitiivinen kuormitus ja riskien havaitsemisen haasteet voivat johtaa siihen, että epäilyttävää henkilöä tai tilannetta ei tunnisteta uhkaksi [61]. Nämä voivat heikentää tämän kontrollin toteutumista.

Kontrolli 7.4 vaatii fyysisen turvallisuuden valvonnan toteuttamista, jotta havaitaan mahdollinen luvaton fyysinen pääsy organisaation tiloihin [76]. Jatkuvaa valvontaa toteutetaan valvontajärjestelmillä joko organisaation oman henkilöstön tai ulkopuolisen valvontapalvelun toimesta. Valvonta edellyttää jatkuvaa toimintaa ja tarvittaessa nopeaa reagointia. Jos reagointi laiminlyödään esimerkiksi kuormitustekijöiden, kuten kiireen vuoksi, voi ulkopuolisia päästä luvatta tiloihin, laitteistoiden luo ja luottamuksellisten tietojen äärelle [43]. Myös kognitiiviset tekijät, kuten heikentynyt tarkkaavaisuus ja hälytysväsymys, voivat johtaa siihen, että poikkeava toiminta jää huomaamatta tai hälytyksiin ei reagoida [61]. Tämä voi heikentää tämän kontrollin toteutumista.

Tyhjä työpöytä ja tyhjä näyttö on kontrollin 7.7 nimi. Kontrollin tavoite on vähentää luvatonta pääsyä tietoihin ja tietojen katoamista [76]. Tämä koskee sekä laitteiden näytöillä olevia tietoja että fyysistä tiedonsäilytystä paperilla tai tallennuslaitteissa. Tietoja voidaan suojata esimerkiksi fyysisillä lukittavilla säilytysratkaisuilla, tietokoneen lukitsemisella tai uloskirjautumisella sekä tarpeettoman tiedon asianmukaisella hävittämisellä. Kognitiiviset tekijät, kuten riskien havaitsemisen haasteet, voivat ilmetä siten, että ei pidetä todennäköisenä, että kukaan lukisi tai veisi tietoa toimiston pöydältä [61]. Osaaminen, kuten riittämätön tietoisuus tai puutteellinen ymmärrys, voi puolestaan johtaa siihen, että ei tunnisteta riskiä, joka liittyy tietokoneen jättämiseen lukitsematta poistuttaessa paikalta [52]. Nämä tekijät voivat heikentää tämän kontrollin toteutumista.

Kontrolli 7.9 edellyttää että organisaation omistamien laitteiden katoaminen,

vahingoittuminen, varkaus tai vaarantuminen on estettävä [76]. Tämä koskee myös muiden omistamia laitteita, joilla käsitellään tai tallennetaan organisaation tietoja. Laitteita on suojattava ja valvottava organisaation ohjeiden mukaisesti. Riskikäyttäytyminen, kuten sääntöjen rikkominen ja luottamushaasteet, voivat johtaa siihen, että ohjeita ei noudateta ja laitteet voivat jäädä valvomatta [65]. Myös osaaminen, kuten riittämätön tieto ja tietoisuus, voi johtaa siihen, ettei laitteiden turvallista käyttöä hallita tai noudateta, mikä altistaa tietoturvariskeille [52]. Nämä voivat heikentää tämän kontrollin toteutumista.

Taulukko 6.9: Fyysisten kontrollien ja inhimillisten tekijöiden pääryhmien väliset yhteydet.

	pääryhmä					
fyysiset kontrollit	osaaminen	kognitiiviset tekijät	riskikäyttäytyminen	asenteet ja motiivit	kuormitustekijät	yksilön ominaisuudet
7.2 Kulunvalvonta		■	■		■	
7.4 Fyysisen turvallisuuden valvonta		■			■	
7.7 Tyhjä työpöytä ja tyhjä näyttö	■	■				
7.9 Omaisuuden turvallisuus kiint. ulkop.	■		■			

■ Pääryhmä vaikuttaa kontrolliin. □ Ei yhteyttä.

6.2.4 Teknologiset kontrollit

Teknologiset kontrollit keskittyvät nimensä mukaisesti teknisten verkkojen, laitteistojen ja ohjelmistojen suojaamiseen. Näiden kontrollien avulla suojataan sekä lait-

teiden että niillä käsiteltävän ja tallennettavan tiedon turvallisuutta. Tämän ryhmän kontrollit ja niiden yhteydet inhimillisten tekijöiden pääryhmiin on esitetty taulukossa 6.10.

Kontrolli 8.1 vaatii käyttäjän päätelaitteiden suojaamista siten, että laitteella käsitelty tai sinne tallennettu tieto pysyy suojattuna [76]. Organisaatioilla on oltava tätä varten selkeät toimintatavat ja ohjeistukset, joissa määritellään ainakin laitteiden rekisteröinnistä, fyysisestä suojauksesta ja ohjelmistojen asennusrajoituksista. Riittämätön tieto ja tietoisuus toimintatavoista ja ohjeistuksista altistaa kyberturvallisuusriskeille [52]. Kuormitustekijät, kuten kiire, tai riskikäyttäytyminen, kuten huolimattomuus, voivat johtaa ohjeistusten laiminlyöntiin [53], [65]. Nämä voivat heikentää tämän kontrollin toteutumista.

Kontrolli 8.7 edellyttää tiedon suojaamista haittaohjelmia vastaan asianmukaisilla havaitsemis- ja torjuntaohjelmistoilla [76]. Tämän lisäksi edellytetään tietoturvatietoisuutta, joka ei toteudu ilman riittävää koulutuksessa saatua tietoa. Myös järjestelmien pääsyn- ja muutostenhallinnasta on huolehdittava. Osaaminen, kuten riittämätön tietoisuus ja tieto, voi johtaa siihen, että haittaohjelmia ei tunnisteta tai torjuntaohjelmistoja ei osata käyttää oikein [52]. Riskikäyttäytyminen, kuten huolimattomuus tai sääntöjen rikkominen, voi johtaa esimerkiksi epäilyttävien liitteiden avaamiseen tai haitallisten ohjelmistojen asentamiseen [65]. Kuormitustekijät, kuten väsymys ja kiire, voivat heikentää tarkkaavaisuutta ja johtaa ohjeistusten laiminlyöntiin [53]. Nämä tekijät voivat heikentää tämän kontrollin toteutumista.

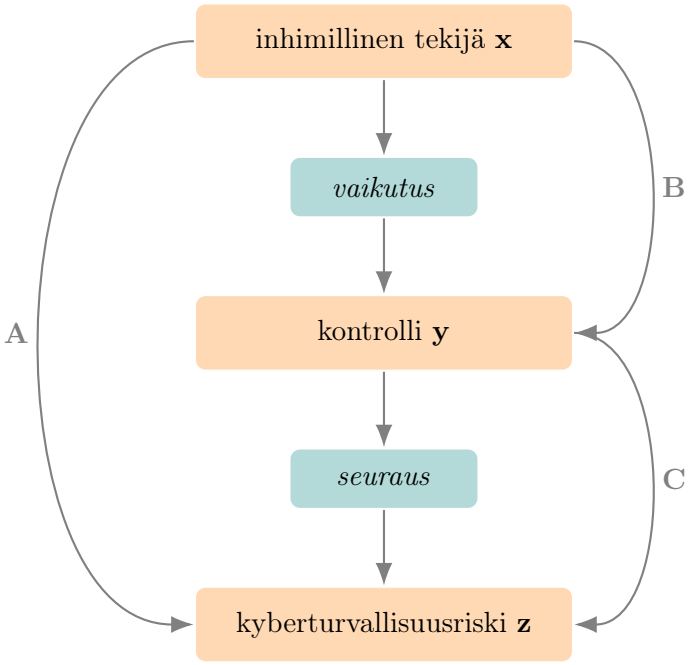
Taulukko 6.10: Teknologisten kontrollien ja inhimillisten tekijöiden pääryhmien väliset yhteydet.

	pääryhmä					
teknologiset kontrollit	osaaminen	kognitiiviset tekijät	riskikäyttäytyminen	asenteet ja motiivit	kuormitustekijät	yksilön ominaisuudet
8.1 Käyttäjän päätelaitteet	■		■		■	
8.7 Suojaus haittaohjelmia vastaan	■		■		■	

■ Pääryhmä vaikuttaa kontrolliin. □ Ei yhteyttä.

6.3 Synteesi ja yhteenveto

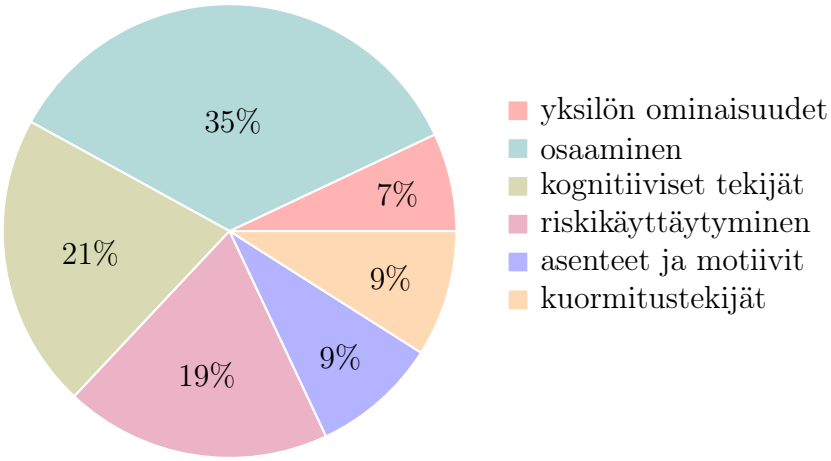
Tämän kontrolliviitekehyksen muodostamisen peruslogiikka on esitetty kuvassa 6.2. Kuvan mukaisesti, kun inhimillinen tekijä vaikuttaa kontrolliin, siitä voi seurata jokin kyberturvallisuusriski tai riskin kasvaminen. Kirjallisuuskatsauksessa tunnistettiin inhimilliset tekijät, jotka voivat vaikuttaa kyberturvallisuusriskiin (kuvan 6.2 kaari A). Kontrollien valinnassa pohdittiin kunkin kontrollin vaatimaa tiettyä toimintaa ja sitä, miten jokin inhimillinen tekijä voi vaikuttaa kykyyn toteuttaa kyseinen toiminta (kaari B). Tästä voi seurata kyberturvallisuusriski (kaari C) ja kontrollin toteutumisen heikkeneminen.



Kuva 6.2: Kontrolliviitekehyksen peruslogiikka. A: kirjallisuuskatsauksen tunnistama vaikutus, B: kontrollin valintaperuste, C: seuraus, jos kontrolli ei toteudu

6.3.1 Inhimillisten tekijöiden ja kontrollien valinnasta

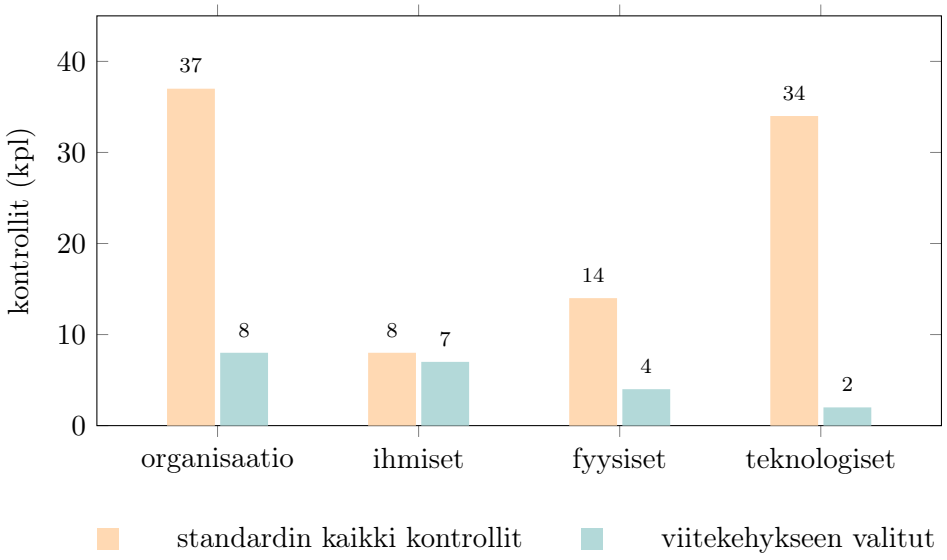
Kirjallisuuskatsauksessa tarkasteltiin valitut 38 artikkelia, joista valikoitui mukaan yhteensä 255 inhimillisen tekijän merkintää. Näistä muodostettiin kuusi inhimillisten tekijöiden pääryhmää. Kuvassa 6.3 on esitetty, miten merkinnät jakautuivat pääryhmien välillä. Selvästi suurimman pääryhmän 35 %:n osuudella muodostivat osaamiseen liittyvät inhimilliset tekijät. Seuraavina tulivat kognitiiviset tekijät 21 %:n osuudella ja riskikäyttäytyminen 19 %:n osuudella. Asenteet ja motiivit -pääryhmään sekä kuormitustekijöiden pääryhmään päätyi molempiin yhtä suuri 9 %:n osuus inhimillisistä tekijöistä. Pienimmäksi jäi yksilön ominaisuudet -ryhmä 7 %:n osuudella.



Kuva 6.3: Inhimillisten tekijöiden pääryhmien artikkelimainintojen jakautuminen.

ISO 27001 -standardin kaikki 93 kontrollia tarkasteltiin osana valintaprosessia. Näistä mukaan valittiin 21 kontrollia, mikä vastaa 23 % kaikista kontrolleista. Standardissa kontrollit on jaettu neljään ryhmään, ja sama ryhmäjako pidettiin valituille kontrolleille. Kuvassa 6.4 on esitetty ryhmittäin valittujen ja kaikkien standardin kontrollien lukumäärät. Kuvasta nähdään, että ihmisiin liittyvien kontrollien ryhmästä mukaan valikoitui 88 % standardin kontrolleista. Lukumääräisesti vain yksi kontrolli jäi viitekehyksen ulkopuolelle. Tähän ryhmään kuuluvat kontrollit kosketttavat yksittäisiä ihmisiä [76], joten ne sopivat tarkasteltaviksi inhimillisten tekijöiden kautta. Fyysiset kontrollit koskevat fyysisiä esineitä ja teknologiset kontrollit koskevat teknologiaa [76]. Tämä selittää sitä, että näistä ryhmistä valikoitui pienempi määrä kontrolleja mukaan viitekehykseen. Fyysiset kontrollit käsittelevät esimerkiksi fyysistä pääsyä tiloihin. Fyysisistä kontrolleista valikoitui mukaan 29 %. Teknologiset kontrollit ovat suurelta osin järjestelmä- ja prosessikeskeisiä eikä niinkään inhimillisiä ja ihmisen jatkuvaan suoraan toimintaan liittyviä. Ne käsittelevät esimerkiksi ohjelmistoja, verkkoja ja arkkitehtuuria. Näitä hallitaan pääasiassa teknisillä ratkaisuilla. Teknologisista kontrolleista mukaan päätyi siis vain 6 %. Jos kontrolli ei koske

yksittäisiä ihmisiä, fyysisiä esineitä tai teknologiaa, se luokitellaan organisaatioon liittyväksi kontrolliksi. Tämä ryhmä sisältää kontrolleja, jotka liittyvät organisaation tietoturvan hallinnolliseen perustaan. Kontrollit käsittelevät esimerkiksi organisaation tietoturvapolitiikkaa, vastuita ja poikkeamatilanteita. Viitekehykseen mukaan valikoitui 22 % tämän ryhmän kontrolleista. Ne liittyivät esimerkiksi tunnistautumistietoihin, käyttöoikeuksiin ja tietoturvapoikkeamiin reagointiin.



Kuva 6.4: ISO 27001 -standardin kontrollien ja viitekehykseen valittujen kontrollien lukumäärät ryhmittäin.

6.3.2 Viitekehys matriisiesityksenä

Luvussa 6.1 esiteltiin kirjallisuuskatsauksessa tunnistetuista inhimillisistä tekijöistä kootut pääryhmät. Luvussa 6.2 esiteltiin valitut ISO 27001 -kontrollit ryhmittäin ja analysoitiin jokainen valittu kontrolli inhimillisten tekijöiden riskien näkökulmasta. Kontrollit yhdistettiin inhimillisten tekijöiden pääryhmiin, joiden seurauksena jokin kyberturvallisuusriski voi kasvaa ja kontrollin toteutuminen heikentyä. Tulokset on esitetty matriisimuodossa taulukossa 6.11. Matriisin yläreunassa on kontrolliryhmät ja vasemmassa sarakkeessa inhimillisten tekijöiden ryhmät.

Taulukko 6.11: Inhimillisten tekijöiden ja kontrolliryhmien väliset yhteydet: lukumäärä ja osuus kontrolliryhmän kontrolleista (%).

kontrollit / **inhimilliset tekijät**	**organisaatio**	**ihmiset**	**fyysiset**	**teknologiset**	**yhteensä**
osaaminen	6 (75 %)	4 (57 %)	2 (50 %)	2 (100 %)	14 (67 %)
kognitiiviset tekijät	3 (38 %)	2 (29 %)	3 (75 %)	0 (0 %)	8 (38 %)
riskikäyttäytyminen	5 (63 %)	3 (43 %)	2 (50 %)	2 (100 %)	12 (57 %)
asenteet ja motiivit	2 (25 %)	3 (43 %)	0 (0 %)	0 (0 %)	5 (24 %)
kuormitustekijät	7 (88 %)	4 (57 %)	2 (50 %)	2 (100 %)	15 (71 %)
yksilön ominaisuudet	0 (0 %)	0 (0 %)	0 (0 %)	0 (0 %)	0 (0 %)

Väritys kuvaa osuutta: 0-24 % vaalea sinivihreä, 25-49 % tumma sinivihreä, 50-74 % vaalea oranssi, 75-100 % tumma oranssi.

Ensimmäinen huomio matriisissa kiinnittyy siihen, että inhimillisten tekijöiden yksilön ominaisuudet -pääryhmään ei yhdistetty yhtään kontrollia. Niitä ei siis mainittu kontrollien analyysissä kertaakaan. Asenteet ja motiivit -pääryhmään yhdistyi 24 % kaikista kontrolleista, ja ne olivat organisaatioon ja ihmisiin liittyvistä kontrolliryhmistä. Kontrolliryhmien pystysarakkeita tarkasteltaessa havaitaan, että teknologisissa kontrolleissa on ainoastaan 100 %:n ja 0 %:n merkintöjä. Ne ovat siis joko täysin alttiita tai ei lainkaan alttiita inhimillisten tekijöiden vaikutukselle. Tässä ryhmässä tosin oli vain kaksi kontrollia mukana.

Eniten kontrolleja, 71 %, yhdistettiin kuormitustekijöiden pääryhmään. Tämän pääryhmän inhimilliset tekijät osoittautuivat siis vaikuttaneen eniten kontrollien toteutumisen heikkenemiseen. Osaamisen pääryhmään yhdistettiin 67 % ja riskikäyttäytymisen pääryhmään 57 % kontrolleista. Nämä mainitut kolme pääryhmää ja niiden inhimilliset tekijät vaikuttavat siis tämän analyysin mukaan eniten valittu-

jen kontrollien toteutumiseen. Näiden kolmen pääryhmän tulokset tosin ovat hyvin lähellä toisiaan.

Organisaatioon liittyvillä kontrolleilla on pystyrivillään tasaisesti merkintöjä, jotka ovat osittain melko suuriakin. Tämän ryhmän kontrollit ovat siis laajasti alttiita eri ryhmien inhimillisille tekijöille. Korkeimmat luvut ovat kuormitustekijöillä 88 %, osaamisella 75 % ja riskikäyttäytymisellä 63 %. Ihmisiin liittyvät kontrollit ovat tasaisemmin alttiita eri ryhmien inhimillisille tekijöille. Sekä osaamisen että kuormitustekijöiden pääryhmät yhdistyivät 57 %:in ihmisiin liittyvistä kontrolleista. Fyysiset kontrollit yhdistyivät 75 %:n osuudella sekä kognitiivisiin tekijöihin että kuormitustekijöihin. Lisäksi 50 % fyysisistä kontrolleista yhdistyi sekä osaamisen että riskikäyttäytymisen pääryhmiin.

Organisaatioon ja ihmisiin liittyvät kontrollit saivat kaikki merkintöjä eri inhimillisten tekijöiden pääryhmiin. Ainoastaan jo mainittu yksilön ominaisuudet -pääryhmä jäi kokonaan ilman merkintöjä. Fyysisiä kontrolleja oli mukana vain neljä, joten ne saivat siinä suhteessa hyvin merkintöjä, tosin yksilön ominaisuuksien lisäksi asenteet ja motiivit -ryhmä jäi niiden kohdalla ilman merkintöjä. Teknologisten kontrollien ryhmän tulos oli erikoisin ehkä johtuen vain kahdesta mukana olleesta kontrollista. Asenteet ja motiivit -pääryhmä näkyi ainoastaan organisaatioon ja ihmisiin liittyvissä kontrolleissa. Kognitiiviset tekijät liittyivät selkeästi eniten fyysisiin kontrolleihin.

Kuormitustekijöiden ryhmään yhdistyi siis suhteellisesti eniten kontrolleja, mutta vain pienellä erolla osaamisen ryhmään. Kuormitustekijöiden ryhmässä yleisin inhimillinen tekijä on stressi, jonka jälkeen tulevat väsymys sekä paine ja kiire. Työn kuormitus voi aiheuttaa painetta ja kiirettä, joiden seuraus voi olla riskialttiin toiminnan lisääntyminen [32]. Väsymys voi puolestaan heikentää päätöksentekoa ja tarkkaavaisuutta tietoturvakäytäntöihin [59]. Tilanteen parantamiseksi tulisi pohtia näiden tekijöiden taustalla olevia syitä.

Toiseksi yleisimmän, osaamisen ryhmän yleisimmät inhimilliset tekijät ovat riittämätön tietoisuus ja riittämätön koulutus. Kuten luvussa 6.1.1 kerrottiin, nämä liittyvät läheisesti toisiinsa. Näiden tekijöiden parantamiseksi yksi keskeinen ratkaisu on koulutuksen ja tietoisuusohjelmien lisääminen [59]. Koulutuksella voidaan myös muuttaa passiivista tietoisuutta aktiiviseksi valmiudeksi [61].

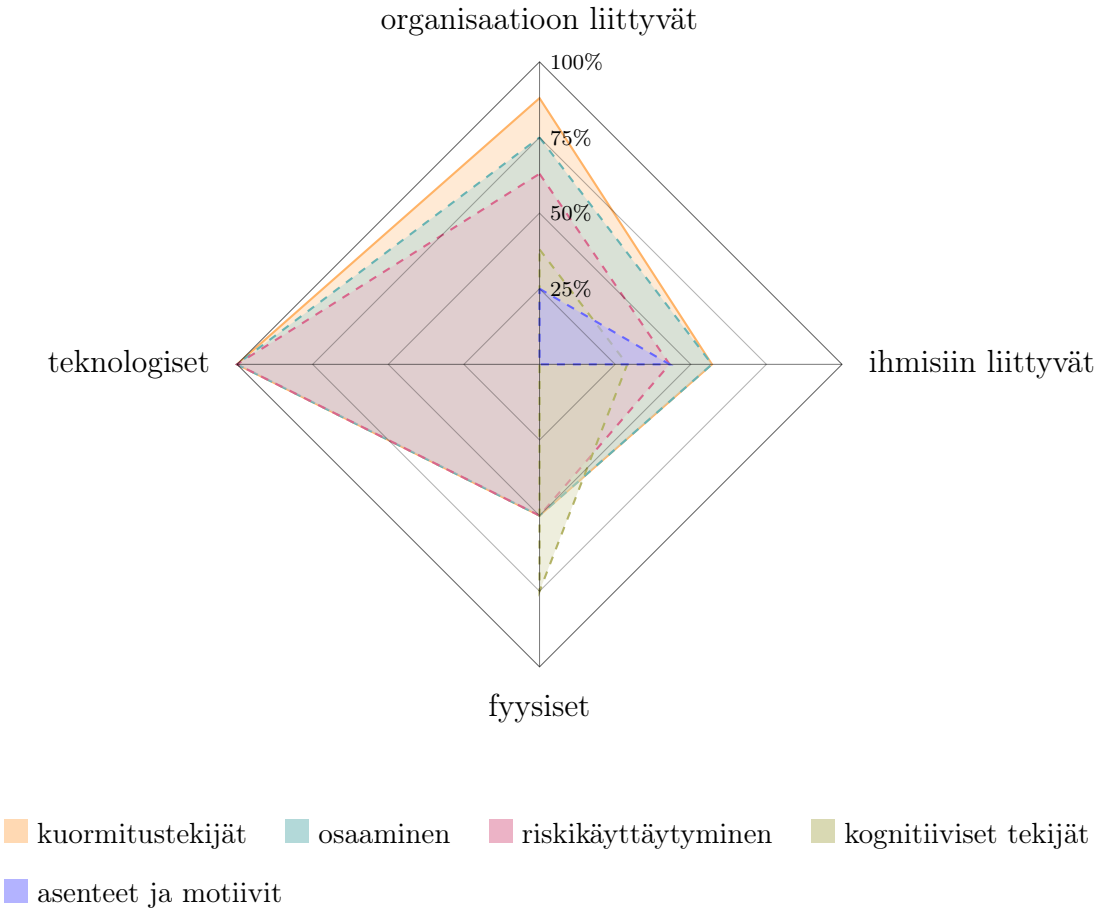
Riskikäyttäytyminen tuli kolmantena ryhmänä, jossa yleisimmät inhimilliset tekijät ovat riskialtis käyttäytyminen, luottamushaasteet ja huolimattomuus. Riskialttiiseen käyttäytymiseen on esitetty ratkaisuna erilaisia koulutusmuotoja ja pelillistettyjä palkitsemisjärjestelmiä [62]. Riskikäyttäytyminen voi johtua esimerkiksi väsymyksestä ja kiireestä, jolloin taustatekijöihin puuttuminen on keskeistä [72].

Organisaatioon ja ihmisiin liittyvät kontrollit osoittautuivat tässä analyysissä laajimmin alttiiksi inhimillisten tekijöiden vaikutuksille. Näiden kahden ryhmän kontrollit yhdistyivät kaikkiin muihin inhimillisten tekijöiden pääryhmiin paitsi yksilön ominaisuudet -ryhmään. Lisäksi näiden kahden ryhmän kontrollit muodostavat selkeän enemmistön, 71 %, kaikista mukaan valituista kontrolleista. Organisaatioon liittyvät kontrollit muodostavat perustan organisaation ISMS:n rakentamiselle. Kontrollit määrittelevät organisaation strategisen perustan sekä vastuut ja velvoitteet. Ihmisiin liittyvät kontrollit puolestaan määrittelevät esimerkiksi henkilöstön tietoturvatehtäviä ja -velvoitteita työsuhteen alusta loppuun. Molemmissa ryhmissä ihmisen toiminnalla on merkittävä rooli, minkä vuoksi juuri näiden ryhmien kontrolleihin on syytä kiinnittää erityistä huomiota inhimillisten tekijöiden vaikutuksia arvioitaessa.

6.3.3 Soveltaminen käytännössä

Tässä työssä tunnistettujen inhimillisten tekijöiden ja valittujen kontrollien yhteyksien muodostaminen mahdollisti niiden yhdistämisen kyberturvallisuusriskien hallintaa tukevaksi viitekehykseksi. Kuvassa 6.5 on esitetty analyysi, joka osoittaa, että

inhimillisten tekijöiden pääryhmät eroavat toisistaan jonkin verran vaikutuksensa laajuuden suhteen. Kuormitustekijöiden pääryhmä osoittautui laaja-alaisimmaksi yhdistymällä kaikkiin neljään kontrolliryhmään vähintään 50 %:n osuuksilla. Tämä tarkoittaa, että esimerkiksi stressin, väsymyksen ja kiireen hallinta on kyberturvallisuusriskien hallinnan kannalta tärkeää. Osaaminen ja riskikäyttäytyminen muodostavat seuraavaksi tärkeimmän osa-alueen melko pienellä erolla kuormitustekijöihin, jonka jälkeen kognitiiviset tekijät sekä asenteet ja motivaatiot täydentävät viitekehyksen pienemmillä osa-alueillaan.



Kuva 6.5: Inhimillisten tekijäryhmien yhteydet ISO 27001 -kontrolliryhmiin. Akselit kuvaavat kontrolliryhmää ja polygonien koko tekijäryhmän vaikutuslaajuutta.

Kyberturvallisuuslain 7 §:n mukaan toimijan on tunnistettava, arvioitava ja hallittava riskejä, jotka kohdistuvat sen toiminnassa käytettävien viestintäverkkojen ja järjestelmien turvallisuuteen [3]. Tässä työssä muodostettu viitekehys voi tukea tätä velvoitetta tarjoamalla tavan tunnistaa inhimilliset tekijät osana riskien arviointia. Lain 8 §:n edellyttämässä kyberturvallisuuden riskienhallinnan toimintamallissa tulee huomioida kaikki vaaratekijät [3]. Tämä työ osoittaa, että inhimilliset tekijät ovat osa riskienhallinnan kokonaisuutta.

Lain 9 §:ssä luetellaan riskienhallinnan osa-alueita, joihin inhimillinen tekijä on suoraan yhteydessä [3]. Erityisesti henkilöstöturvallisuus ja kyberturvallisuuskoulutus sekä pääsynhallinta ja todentamisen menettelytavat ovat alueita, joihin osaamisen ja kuormitustekijöiden inhimillisillä tekijöillä on vaikutusta. Lisäksi poikkeamien havainnointi ja käsittely edellyttävät henkilöstöltä riittävää osaamista ja valmiutta toimia oikein kriittisellä hetkellä. Näihin osaamisen ja kuormitustekijöiden pääryhmien inhimillisillä tekijöillä voi myös olla vaikutusta.

Lain 10 §:n käsittelemä johdon vastuu kyberturvallisuuden riskienhallinnan toteuttamisesta ja valvonnasta on suoraan yhteydessä osaamisen pääryhmän inhimillisiin tekijöihin [3]. Johdon on oltava tarpeeksi kouluttautunut ja perehtynyt kyberturvallisuusasioihin, jotta se voi täyttää lain vaatimat vastuunsa.

Työssä esitettyä viitekehystä voidaan hyödyntää pohjatietona tietoturvan suunnittelussa huomioimalla ennakolta toimenpiteet inhimillisten tekijöiden pääryhmien mahdollisista vaikutuksista. Käytännössä tämä tarkoittaa puuttumista ensisijaisesti kuormitustekijöihin ja osaamisen puutteisiin, riskikäyttäytymisen tunnistamista sekä organisaatioon ja ihmisiin liittyvien kontrollien erityistä huomioimista.

7 Tulokset ja niiden tarkastelu

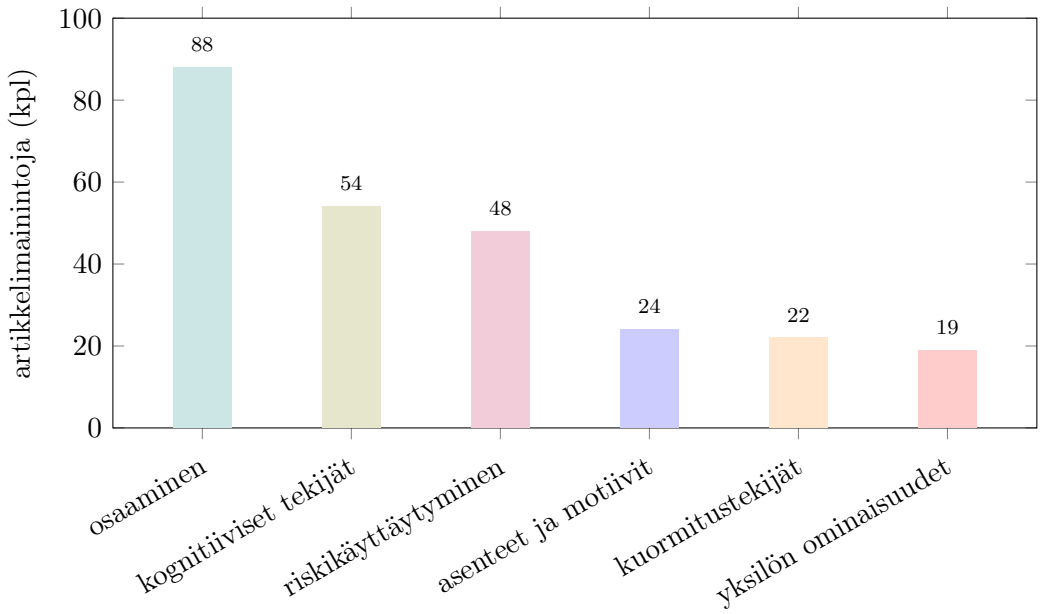
Tässä luvussa esitetään vastaukset tutkimuskysymyksiin. Lisäksi käsitellään muodostetun viitekehyksen arviointia, joka suoritettiin kahdella tavalla: vertailuarviointina ja asiantuntija-arviointina. Luvun lopuksi pohditaan tuloksia ja työn aikana vastaan tulleita haasteita.

7.1 Vastaukset tutkimuskysymyksiin

Tähän työhön asetettiin kolme tutkimuskysymystä, joihin kaikkiin saatiin vastaukset työn edetessä. Seuraavaksi käsitellään jokainen tutkimuskysymys erikseen ja niihin saadut vastaukset.

TK1. Mitkä ovat kirjallisuuden perusteella keskeiset inhimilliset tekijät, jotka voivat lisätä kyberturvallisriskejä?

Tässä työssä suoritettiin kevennetty systemaattinen kirjallisuuskatsaus. Artikkeleja etsittiin kahdesta tietokannassa useammalla hakulauseella. Seulontojen jälkeen mukaan valikoitui 38 artikkelia, joista tähän työhön valikoitui mukaan 255 inhimillisen tekijän englanninkielistä esiintymää. Näitä ryhmittelemällä päädyttiin kuuteen inhimillisten tekijöiden pääryhmään, jotka on esitetty kuvassa 7.1. Kuvasta havaitaan, että osaamisen pääryhmään kuuluvat inhimilliset tekijät osoittautuivat tämän työn perusteella lisäävän eniten kyberturvallisuusriskejä. Seuraavaksi suurimpina ryhminä esiintyivät kognitiivisiin tekijöihin ja riskikäyttäytymiseen liittyvät inhimilliset tekijät.



Kuva 7.1: Inhimillisten tekijöiden pääryhmien artikkelimainintojen jakautuminen.

Taulukossa 7.1 on lueteltu yksittäiset inhimilliset tekijät, jotka esiintyivät määrällisesti eniten kirjallisuuskatsauksen artikkeleissa. Kolme eniten esiintynyttä inhimillistä tekijää ovat riittämätön tietoisuus, riittämätön koulutus ja harjoittelu sekä riittämätön tieto. Nämä kaikki kuuluvat osaamisen pääryhmään, joka siis osoittautui kirjallisuudessa useimmin esiintyneeksi ryhmäksi. Seuraavat kolme yksittäistä inhimillistä tekijää kuuluvat kolmanneksi suurimpaan riskikäyttäytymisen pääryhmään. Nämä kolme inhimillistä tekijää ovat riskialtis käyttäytyminen, luottamushaasteet ja huolimattomuus. Kognitiiviset tekijät nousivat ryhmänä toiseksi, mutta yksittäisissä inhimillisissä tekijöissä riskikäyttäytymisen pääryhmän inhimilliset tekijät menivät niiden edelle.

Kirjallisuuskatsauksen perusteella osaamiseen liittyvät inhimilliset tekijät ovat keskeisiä lisäämään kyberturvallisuusriskejä. Organisaatioiden on tärkeää tunnistaa ja huomioida nämä tekijät. Koulutuksilla ja harjoituksilla voidaan lisätä henkilöstön tietoa, joka auttaa ymmärtämään riskejä ja toimimaan oikein erilaisissa riskitilanteissa. Lisääntyvällä tiedolla on suora vaikutus tietoisuuteen, joka tarkoittaa ky-

kyä huomioida ympäristön tapahtumat ja riskit. Osaamisen tekijöitä vahvistamalla voidaan suoraan vaikuttaa riskikäyttäytymiseen. Tiedon ja tietoisuuden kasvaessa osataan tunnistaa riskit, jolloin riskikäyttäytyminen vähenee.

Taulukko 7.1: Yleisimmät inhimilliset tekijät. Luku kertoo, kuinka monessa kirjallisuuskatsauksen artikkelissa inhimillinen tekijä esiintyi.

lkm	**inhimillinen tekijä**	**pääryhmä**
31	riittämätön tietoisuus	osaaminen
20	riittämätön koulutus ja harjoittelu	osaaminen
17	riittämätön tieto	osaaminen
14	riskialtis käyttäytyminen	riskikäyttäytyminen
13	luottamushaasteet	riskikäyttäytyminen
11	huolimattomuus	riskikäyttäytyminen
11	riskien havaitsemisen haasteet	kognitiiviset tekijät
10	stressi	kuormitustekijät

TK2. Mitkä ovat ISO 27001 -standardin keskeiset kontrollit, joiden toteutumista kirjallisuudesta tunnistetut inhimilliset tekijät voivat heikentää?

ISO 27001 -standardin kaikki 93 kontrollia käytiin yksitellen läpi. Kontrolli valittiin, jos todettiin, että jollakin kirjallisuuskatsauksella tunnistetuista inhimillisistä tekijöistä muodostetuista kuudesta pääryhmästä voi olla vaikutusta kontrollin toteutumiseen, ja se täytti myös muut valinnalle luvussa 5.4.2 asetetut ehdot: onko inhimillinen tekijä keskeisessä asemassa, jos kontrolli ei toteudu, liittyykö kontrolli päivittäiseen tekemiseen tai valmiuteen, ja vaatiiko se jatkuvaa noudattamista.

Kaikki valitut 21 kontrollia on lueteltu taulukossa 7.2. Nämä ovat siis tämän työn perusteella keskeiset kontrollit, joiden toteutumista kirjallisuudesta tunnistetut inhimilliset tekijät voivat heikentää.

Taulukko 7.2: Viitekehykseen valitut kontrollit ryhmittäin.

Organisaatioon liittyvät kontrollit	
5.4	Johdon vastuut
5.8	Tietoturva projektinhallinnassa
5.10	Resurssien hyväksyttävä käyttö
5.14	Tiedonsiirto
5.17	Tunnistautumistiedot
5.18	Käyttöoikeudet
5.23	Tietoturva pilvipalveluissa
5.26	Tietoturvapoikkeamiin reagointi
Ihmisiin liittyvät kontrollit	
6.1	Taustaselvitykset
6.2	Työsuhteen ehdot
6.3	Tietoisuus, koulutus ja valmennus
6.5	Vastuut työsuhteen päättyessä
6.6	Salassapitosopimukset
6.7	Etätyö
6.8	Tietoturvatapahtumien raportointi
Fyysiset kontrollit	
7.2	Kulunvalvonta
7.4	Fyysisen turvallisuuden valvonta
7.7	Tyhjä työpöytä ja tyhjä näyttö
7.9	Omaisuuden turvallisuus kiinteistön ulkopuolella
Teknologiset kontrollit	
8.1	Käyttäjän päätelaitteet
8.7	Suojaus haittaohjelmia vastaan

Ihmisiin liittyvät kontrollit liittyvät organisaation henkilöstöön ja ihmisen suoraan toimintaan. Siksi ne loogisesti osoittautuivat olevan alttiimpia inhimillisille tekijöille: tästä ryhmästä vain yksi kontrolli kahdeksasta jäi valitsematta. Organisaatioon liittyviä kontrolleja valikoitui mukaan kahdeksan, joka on yksi enemmän kuin ihmisiin liittyviä kontrolleja, mutta kuitenkin vain 22 % tämän ryhmän kokonaiskontrollimäärästä. Organisaatioon liittyvistä kontrolleista valittua suurempi osa liittyy ihmisen toimintaa, mutta kontrolleja karsiutui pois, koska valintakriteereistä päivittäinen tekeminen ei toteutunut. Valintakriteerejä muuttamalla tämän ryhmän kontrollien ja inhimillisten tekijöiden yhteyttä voisi tutkia tarkemmin. Fyysisen turvallisuuden tukemiseen liittyviä fyysisiä kontrolleja valikoitui mukaan prosentuaalisesti enemmän (29 %), mutta määrällisesti vain neljä. Järjestelmä- ja prosessikeskeisiä teknologisia kontrolleja mukaan valikoitui vähiten sekä prosentuaalisesti (6 %) että määrällisesti, kaksi kontrollia. Teknologiset kontrollit liittyvät esimerkiksi teknisten verkkojen, laitteistojen ja ohjelmistojen suojaukseen. Valintakriteerejä tarkentamalla valitut kaksi kontrollia olisi voinut jättää pois, kuten asiantuntija mainitsi arvioinnissaan. Teknologisten kontrollien ryhmä on yksi erinomainen jatkotutkimuskohde. Kriteerejä muuttamalla ja henkilöstön työroolit huomioimalla voisi näiden kontrollien yhteyttä inhimillisiin tekijöihin tutkia tarkemmin.

Jotta organisaatio saavuttaa määrittelemänsä tietoturvatason, sen on tunnistettava, arvioitava ja käsiteltävä mahdolliset tietoturvariskit. Riskien käsittelyprosessin toteuttamiseen tarvitaan kontrolleja, joiden avulla riskejä hallitaan ja niiden todennäköisyyttä tai vaikutusta vähennetään. Organisaatioille on siis erittäin tärkeää tunnistaa kontrollit ja niihin mahdollisesti vaikuttavat inhimilliset tekijät, jotta ne voidaan huomioida ennakolta.

TK3. Miten tunnistetut inhimilliset tekijät ja valitut ISO 27001 -standardin kontrollit voidaan yhdistää viitekehykseksi, joka tukee kyberturvallisuusriskien hallintaa kyberturvallisuuslain vaatimusten näkökulmasta?

Tunnistetuilla inhimillisillä tekijöillä todettiin olevan vaikutusta valittujen kontrollien toteutumiseen. Inhimillisten tekijöiden ja kontrollien välillä oli siis yhteys, joka mahdollisti viitekehyksen muodostamisen. Viitekehyksen avulla todettiin, että inhimillisten tekijöiden pääryhmät eroavat toisistaan siinä, kuinka laajasti ne yhdistyivät eri kontrolliryhmiin. Kuormitustekijöiden pääryhmällä osoittautui olevan laajin vaikutus kontrollien toteutumiseen. Seuraavaksi laajimman vaikutuspiirin muodostivat osaamisen ja riskikäyttäytymisen pääryhmät.

Kyberturvallisuuslain 7 § velvoittaa toimijoita tunnistamaan, arvioimaan ja hallitsemaan riskejä. Tätä täsmentävät lain 8–9 §, jotka sisältävät velvoitteita riskienhallinnan toimintamallista, jolla tunnistetaan riskejä ja määritetään toimenpiteitä niiden hallitsemiseksi. ISO 27001 -standardi asettaa vastaavat vaatimukset riskienhallinnalle. Standardissa riskien käsittelyprosessin toteutuksessa käytetään tietoturvakontrolleja. Lailla ja standardilla on siis sama tavoite: riskien hallitseminen. Tässä työssä osoitettiin, että inhimilliset tekijät ovat yksi kyberturvallisuuteen vaikuttavista riskeistä, ja että ne voivat heikentää kontrollien toteutumista. Muodostetussa viitekehyksessä nämä yhdistyvät: tunnistamalla, mitkä inhimilliset tekijät vaikuttavat mihinkin kontrolleihin, voidaan riskejä hallita ennakolta sekä standardin että lain edellyttämällä tavalla. [3], [37]

Kyberturvallisuuslain 10 § määrittelee, että toimijan johto vastaa kyberturvallisuuden riskienhallinnan toimintamallin toteuttamisesta, hyväksymisestä ja valvonnasta. Tähän lain pykälään liittyy viitekehyksessä mukana oleva kontrolli 5.4 Johdon vastuut, jonka mukaan johdon vastuulla on seurata ja varmistaa, että henkilöstö noudattaa tietoturvavaatimuksia. Johdolla on valvontavastuu ja epäkohtiin on puututtava. Jotta nämä onnistuvat, johdolla on oltava riittävä osaaminen ja tietoisuus tietoturvavaatimuksista. Kuormitustekijät, kuten stressi ja väsymys, voivat heikentää johdon valvontaa ja epäkohtiin puuttumista. Muodostettua viitekehystä voidaan käyttää tunnistamaan nämä inhimilliset tekijät, etteivät ne vaikuta heiken-

tävästi kontrollin toteutumiseen ja siten myös lain noudattamiseen. [3], [37]

Kyberturvallisuuslain 11–17 § määrittelevät poikkeamatilanteiden velvoitteista. Näihin pykäliin liittyy standardissa kontrolleja kuten 5.24–5.30, mutta ne rajautuivat tämän työn ulkopuolelle, koska kontrollien valintakriteereinä oli kontrollin liittyminen päivittäiseen tekemiseen ja jatkuvaan noudattamiseen. Poikkeamatilanteisiin liittyvien kontrollien lisääminen viitekehykseen on yksi jatkotutkimusaiheista. [3], [37]

7.2 Vertailuarviointi

Viimeisimmästä tieteellisestä tutkimuksesta ei ollut löydettävissä työssä esitettyyn viitekehykseen verrattavissa olevia vaihtoehtoja. Lisäksi laajemmat viitekehykset, kuten Yhdysvaltain standardisointi- ja teknologiainstituutin kyberturvallisuuden viitekehys (engl. National Institute of Standards and Technology Cybersecurity Framework, NIST CSF), huomioivat inhimilliset tekijät vain osittain organisaatiokulttuurin kautta [77]. Monet kirjallisuudesta löydetyt tutkimusten viitekehykset kohdistuvat suppeasti yksittäisiin ilmiöihin, kuten Chowdhury et al. aikapaineeseen [78]. Tässä työssä tehdyssä viitekehyksessä on kaksi osuutta: ensimmäisenä kirjallisuuskatsauksella inhimillisten tekijöiden tunnistaminen ja niiden ryhmittely, sekä toisena inhimillisten tekijöiden yhdistäminen valittuihin ISO 27001 -standardin kontrolleihin.

Khadka ja Ullah [29] ovat muodostaneet viitekehyksen, jota varten he ovat tehneet kirjallisuuskatsauksen tunnistaakseen kyberturvallisuuteen liittyviä inhimillisiä tekijöitä. Artikkelissa esitetty synteesi havainnollistaa inhimillisen tekijän keskeistä merkitystä kyberturvallisuudessa sekä vahvistajana että vaarantajana. Tutkimuksessa on kerätty ja yhdistetty tietoa useilta eri tieteenaloilta ja tuloksena esitetty viitekehys kyberturvallisuuden resilienssin parantamiseksi.

Khadkan ja Ullahin [29] esittelemät johtopäätökset tukevat tämän työn viite-

kehyksen muodostamisen alkuosaa. Sekä esitetyssä tutkimuksessa että tässä työssä on tunnistettu inhimillisiä tekijöitä kirjallisuudesta ja löydetty yhteys inhimillisten tekijöiden ja kyberturvallisuuden riskienhallinnan välille. Tutkimuksessa esitetty viitekehys menee tätä työtä huomattavasti pidemmälle ja ehdottaa konkreettisia ratkaisuja inhimillisten ja teknisten tekijöiden yhdistämiseksi. Artikkelissa mainitaankin, että viitekehyksiä inhimillisen tekijän ja kyberturvallisuuden yhdistämisestä on runsaasti, mutta niistä puuttuu usein käytännön sovellettavuus. Siksi tekijät ovat halunneet tehdä aidosti sovellettavan viitekehyksen, jossa he yhdistävät inhimilliset tekijät, tekniset järjestelmät ja organisaation strategian. Viitekehyksen muodostamisessa tunnistetaan paljon samoja inhimillisiä tekijöitä kuin tässä työssä, kuten kognitiivisia ja kuormitustekijöitä. Khadkan ja Ullahin viitekehys on muodostettu neljänä pilarina, jotka sisältävät konkreettisia toimintoja ja koulutusratkaisuja. Tässä työssä esiteltyä viitekehystä voisi lähteä kehittämään samaan suuntaan tai yhdistämään Khadkan & Ullahin viitekehyksen kanssa.

7.3 Asiantuntija-arviointi

Viitekehyksen ulkopuolisen arvioinnin suoritti kyberturvallisuuden johtavassa asiantuntijatehtävässä toimiva henkilö, jolla on tekniikan tohtorin tutkinto sekä CISSP- ja ISO 27001 Lead Auditor -sertifioinnit. Tämän työn tekijä hankki arvioijan eikä arvioija ole tekijälle entuudestaan tuttu. Arvioijan henkilöllisyys on ainoastaan työn tekijän tiedossa. Arvioijalle lähetettiin luettavaksi tämän työn luku 6 sekä arviointilomake, joka sisälsi 15 väittämää ja neljä avointa kysymystä. Väittämissä oli käytössä viisiasteinen Likert-asteikko: täysin samaa mieltä, jokseenkin samaa mieltä, neutraali, jokseenkin eri mieltä ja täysin eri mieltä. Väittämät arvioijan vastauksineen sekä avoimet kysymykset on esitetty liitteessä B. Arviointi oli sovittu suoritettavaksi viikon sisällä materiaalin saamisesta.

Kattavuus-väittämät

Arvioinnin mukaan viitekehys käsittelee aihetta riittävän laajasti ja se sisältää keskeiset inhimilliset tekijät. Arvioija oli jokseenkin samaa mieltä siitä, että keskeiset tietoturvakontrollit on huomioitu ja ettei viitekehyksestä puutu oleellisia asioita. Kontrollien valintaperusteet ja siten kontrollien kattavuus viitekehyksessä olivat jääneet arvioijalle hieman epäselviksi. Tämä johtunee ainakin osittain siitä, ettei arvioijalla ollut luettavanaan lukua 5, joka olisi ainakin osittain selventänyt kontrollien valintaperusteita, joita voisi kehityskohteena edelleen selventää ja tarkentaa.

Johdonmukaisuus-väittämät

Viitekehyksen rakenteen selkeys, inhimillisten tekijöiden valinnan looginen kuvaus sekä ristiriitaisuuksien puuttuminen saivat jokseenkin myönteisen arvion. Viitekehyksen muodostamisen selkeä kuvaus ja viitekehyksen johdonmukaisuus saivat neutraalin arvion, ja kontrollien valinnan looginen kuvaus jokseenkin erimielisen arvion. Tästä voisi päätellä, että viitekehys on oikeansuuntainen, mutta erityisesti kontrollien valinnan perusteluja sekä viitekehyksen muodostamisen kuvausta tulisi selkeyttää. Viitekehyksen johdonmukaisuuden arviota olisi varmasti parantanut paremmat tiedot inhimillisten tekijöiden ja kontrollien valinnasta, joten luku 5 olisi ehdottomasti pitänyt olla arvioijan luettavissa.

Sovellettavuus-väittämät

Arvioija suhtautui viitekehyksen käytettävyyteen varauksellisesti. Viitekehyksen ymmärrettävyys ja soveltuvuus eri toimialoille saivat jokseenkin myönteisen arvion, mutta käytännön hyödynnettävyys organisaatioille sekä tuki ISO 27001 -standardin ja kyberturvallisuuslain vaatimusten huomioimiseen jäivät neutraalille tasolle. Nämä tulokset viittaavat siihen, että viitekehyksen käytettävyyttä ja sen kytkentää sekä standardin että lain vaatimuksiin tulisi vahvistaa. Lisäksi viitekehystä on syy-

tä edelleen kehittää ja lisätä konkreettisia toimenpiteitä tunnistamaan inhimillisiä tekijöitä ja siten estämään niiden negatiiviset vaikutukset tietoturvakontrollien toteutumiseen.

Avoimet kysymykset

Viitekehyksen vahvuudeksi arvioinnissa mainittiin inhimillisten tekijöiden laaja-alainen tarkastelu organisaatioissa tyypillisesti korostuvan osaamis- ja tietoisuusnäkökulman sijaan, ja että inhimillisten tekijöiden monitahoisuus on huomioitu. Myös alan tutkimuksen käsittelyä pidettiin kattavana ja laadukkaana:

> *Kattava kokonaisuus inhimillisistä tekijöistä ja vaikutuksesta organisaatioiden tietoturvaan. Alan tutkimusta on käsitelty kattavasti ja laadukkaasti.*

Kehityskohteiksi viitekehykselle mainittiin lisäpohdinta ja analysointi koskien erityisesti niitä inhimillisten tekijöiden ja kontrollien muodostamia pareja, joiden välillä ei löydetty yhteyttä. Tämä palaute huomioitiin vielä työn tulosten pohdinnoissa luvussa 7.4:

> *Jäin kaipaamaan pohdintaa inhimillisten tekijöiden ja ISO 27001 kontrollien välisten yhteyksien osalta (esim. Taulukko 6.7 jne.) osa-alueista joissa kontrollien ja inhimillisten tekijöiden välillä ei ole huomattu yhteyttä (taulukkojen valkoiset solut). Eli tarkoittaako tämä sitä, ettei kyseiseen kontrolliin ole vaikutusta inhimillisillä tekijöillä, vai eikö vain kyseisestä aiheesta ole tutkimuskirjallisuutta.*

Lisäksi arvioija ei pitänyt täysin perusteltuna teknologisten kontrollien ottamista mukaan tähän viitekehykseen. Nyt valituksi tulleiden kontrollien (8.1 ja 8.7) osalta vaikutus riippuu arvioijan mukaan merkittävästi henkilön roolista organisaatiossa:

rivityöntekijän toiminnalla on vähäinen vaikutus, kun taas IT- ja tietoturvahenkilöstön kohdalla vaikutus voi olla merkittävä. Arvioija mainitsikin jatkotutkimuskohteena inhimillisten tekijöiden vaikutuksen, kun huomioidaan henkilön rooli organisaatiossa.

Arvioijan mukaan viitekehyksestä voisi olla hyötyä erityisesti henkilöstön kouluttamisessa ja tietoisuuden lisäämisessä esimerkiksi huomioimalla inhimilliset tekijät ja niiden mahdolliset vaikutukset organisaation turvallisuuteen. Lisäksi viitekehys voi auttaa tunnistamaan paremmin mahdolliset inhimillisten tekijöiden vaikutukset kontrolleihin ja niiden toteutumiseen.

Kokonaisuutena arviointi vahvisti viitekehyksen olevan oikean suuntainen. Arvioinnissa tuli kuitenkin esille selkeitä kehityskohteita erityisesti kontrollien valinnassa ja niiden perusteluissa sekä viitekehyksen selkeämmästä kytkemisestä ISO 27001 -standardiin ja kyberturvallisuuslakiin.

7.4 Tulosten pohdintaa

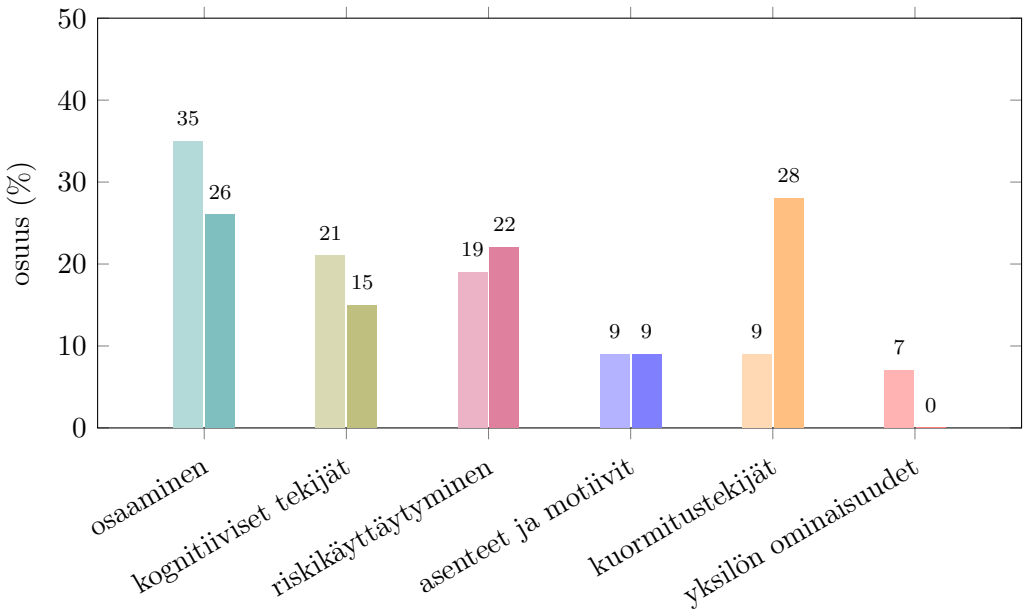
Tässä työssä kirjallisuudessa havaitut inhimilliset tekijät jaettiin kuuteen pääryhmään. Näiden ryhmien ja valittujen standardin kontrollien välille muodostettiin yhteyksiä. Yksi pääryhmistä, yksilön ominaisuudet, jäi täysin ilman kytköksiä mihinkään inhimillisten tekijöiden pääryhmistä. Yksilön ominaisuuksien pääryhmässä tässä työssä olivat ikä, sukupuoli ja persoonallisuus. Nämä määriteltiin yksilön piirteiksi, jotka tekevät yksilöstä ainutlaatuisen ja erottaa muista yksilöistä. Luvun 6 analyyseissä mainitaan yksilön ominaisuuksien yhteyksiä osaamisen, riskikäyttäytymisen ja kognitiivisten tekijöiden pääryhmien inhimillisiin tekijöihin. Tutkimuksissa on todettu myös iän ja sukupuolen yhteys stressiin [79], [80]. Näistä voidaan päätellä, että yksilön ominaisuudet ovat taustatekijöitä, jotka vaikuttavat muihin inhimillisiin tekijöihin, vaikka eivät suoraan näy tämän työn tuloksissa erillisinä yhteyksinä.

Luvussa 6 esitellyssä analyysissä havaittiin myös muita vaikutusketjuja inhimil-

listen tekijöiden pääryhmien välillä, kuten asenteiden ja kuormitustekijöiden vaikutus osaamiseen ja riskikäyttäytymiseen sekä osaamisen ja kognitiivisten tekijöiden vaikutus kuormitustekijöihin ja riskikäyttäytymiseen. Tästä voidaan päätellä, että inhimillisten tekijöiden vaikutusketjut ovat erittäin laajoja, ja antavat aihetta erilliselle lisätutkimukselle tarkempien syy-seuraus-suhteiden selvittämiselle.

Asenteet ja motiivit -pääryhmä ei yhdistynyt ollenkaan fyysisten kontrollien ryhmään. Tämä voi selittyä fyysisten kontrollien pienestä määrästä tai siitä, että asenteet ja motiivit -ryhmä vaikuttaa osaamisen ja riskikäyttäytymisen ryhmään, joihin molempiin fyysiset kontrollit kuitenkin yhdistyivät. Edellä mainittu osaamisen ja kognitiivisten tekijöiden vaikutus kuormitustekijöihin voi selittää eroa, joka näkyy kuvassa 7.2. Tässä kuvassa on esitetty jokaiselle inhimillisten tekijöiden pääryhmälle kaksi pylvästä: vasen esittää kyseisen pääryhmän inhimillisten tekijöiden osuutta kirjallisuuskatsauksessa tunnistetuista inhimillisistä tekijöistä ja oikeanpuoleinen pylväs esittää kyseisen ryhmän inhimillisten tekijöiden yhteyksien osuutta kontrolleihin kaikista muodostuneista yhteyksistä. Pylväät eivät siis ole suoraan verrannollisia toisiinsa, mutta on mielenkiintoista verrata eroa näiden kahden ryhmän välillä. Molemmat kuitenkin esittävät kyberturvallisuusriskiä kasvattavien inhimillisten tekijöiden ryhmiä. Jos kontrolli ei toteudu, kyberturvallisuusriski kasvaa.

Kuvassa 7.2 kuormitustekijöiden yhteyksien osuus 28 % on huomattavasti suurempi kuin kyseisen pääryhmän esiintyvyys kirjallisuuskatsauksessa, mikä on vain 9 %. Vastaavasti osaamisen ja kognitiivisten tekijöiden osuudet ovat kirjallisuuskatsauksessa suuremmat kuin yhteyksien kohdalla. Aiemmin käsitelty yksilön ominaisuuksien ryhmän yhteyksien 0 %:n osuus voi myös olla yhteydessä kuormitustekijöiden korkeaan yhteyksien osuuteen. Syy-seuraus-suhteiden jatkotutkimusajatus saa tässäkin kohtaa vahvistusta.



Kuva 7.2: Inhimillisten tekijöiden pääryhmien jakautuminen kirjallisuuskatsauksessa (vasen palkki) ja yhdistymisessä (oikea palkki) valittuihin kontrolleihin.

Kuormitustekijät, kuten stressi, väsymys ja kiire, osoittautuivat tässä työssä eniten standardin kontrollien toteutumiseen vaikuttaviksi inhimillisiksi tekijöiksi. Toiseksi vaikuttavimmaksi pääryhmäksi osoittautui osaamisen pääryhmä. Tämän voi ajatella olevan positiivinen tulos organisaatioiden kannalta, koska näiden kahden ryhmän inhimillisiin tekijöihin organisaatiot voivat halutessaan vaikuttaa. Haastavampaa ja kyseenalaisempaa olisi yrittää vaikuttaa esimerkiksi työntekijöiden ikään ja sukupuoleen. Kuormitustekijät eivät myöskään ole ristiriidassa organisaation suorituskyvyn kehittämisen kanssa. Jos kuormitustekijöitä osataan hallita oikein, ne voivat jopa tukea organisaation suorituskykyä. Vaikka stressi on tunnistettu maailmanlaajuisesti terveyshuoleksi, kaikki työpaikalla koettu stressi ei ole negatiivista [81]. Hallittu stressin määrä lisää positiivista mielialaa ja tuottavuutta. Alhainen stressi voi aiheuttaa tylsistymistä ja motivaation puutetta, ja liian korkea stressitaso voi pahimmillaan johtaa uupumukseen ja loppuunpalamiseen.

Osaamisen inhimillisten tekijöiden pääryhmä osoittautui tässä työssä toiseksi yleisimmäksi syyksi standardin kontrollisen toteutumisen epäonnistumiseen. Ero ensimmäiseksi tulleeseen kuormitustekijöiden pääryhmään on kuitenkin tämän työn mittakaavassa hyvin pieni. Mukaan valituista 21 kontrollista 15 yhdistyi kuormitustekijöiden pääryhmään ja 14 yhdistyi osaamisen pääryhmään. Näidenkin kahden pääryhmän todettiin myös vaikuttavan toisiinsa.

7.5 Viitekehyksen uutuusarvo

Inhimillisistä tekijöistä kyberturvallisuudessa on esitelty viitekehys jo vuonna 2002 [82]. Myöhemmissä viitekehyksissä inhimillisiä tekijöitä on yhdistetty ainakin henkilöstön halukkuuteen noudattaa tietoturvaohjeistuksia [26], sosiaalisen manipuloinnin hyökkäyksiin [31], kyberturvallisuusriskeihin rautateillä [43] sekä turvallisuuskulttuuriin ja tietojenkalasteluun [33]. Kirjallisuudesta löydetyt viitekehykset kohdistuvat siis inhimillisiin tekijöihin ja lisäksi yksittäisiin ilmiöihin.

NIS2-direktiiviin ja ISO 27001 -standardin kontrolleihin liittyen löydettiin yksi viitekehys. Tämä kokonaisvaltainen tietoturvan hallintaan ja vaatimustenmukaisuuteen liittyvä viitekehys yhdistää operatiiviset, tekniset, inhimilliset ja fyysiset tietoturvan osa-alueet ja pyrkii yhdenmukaistamaan ne EU:n yleisen tietosuoja-asetuksen ja tekoälysäädöksen sekä NIS2-direktiivin kanssa [83]. Tämä erittäin laaja viitekehys ei kuitenkaan sido standardia tai sen kontrolleja inhimillisiin tekijöihin.

Tässä työssä muodostettu viitekehys yhdistää kirjallisuudesta tunnistetut inhimilliset tekijät ISO 27001 -standardin kontrolleihin. Tämä kytkös inhimillisten tekijöiden ja kontrollien väliltä puuttuu aiemmista viitekehyksistä. Lisäksi tämän työn viitekehys kytkeytyy kyberturvallisuuslain velvoitteisiin, mikä tekee siitä käytännössä sovellettavan työkalun lain vaatimusten täyttämiseen. Tämä näkökulma on myös uusi: Ainoa löydetty lainsäädäntöön liittyvä viitekehys yhdisti kontrollit NIS2-direktiiviin, mutta inhimillisten tekijöiden linkitys puuttui tästäkin viitekehyksestä.

Tätä ketjua - inhimilliset tekijät, ISO 27001 -standardin kontrollit ja lainsäädäntö - kokonaan kattavaa viitekehystä ei aiemmasta tutkimuksesta löydetty, joka vahvistaa tämän työn viitekehyksen uutuusarvoa.

7.6 Työn haasteet

Tässä työssä suoritettu inhimillisten tekijöiden ryhmittely osoittautui melko suureksi haasteeksi. Inhimilliset tekijät oli ilmaistu artikkeleissa englanniksi hyvin eri tavoilla, joka haastoi eri termien yhdistämistä ja suomeksi kääntämistä. Ryhmiä oli myös haastavaa määritellä ja rajata yksiselitteisesti, koska monet inhimilliset tekijät olisi voinut sijoittaa useampaankin ryhmään. Näin olisi voinut tehdäkin, mutta sen katsottiin laajentavan ja monimutkaistavan tätä työtä liikaa. Kompromisseja jouduttiin tekemään, jotta ryhmien määrät ja koot saatiin pidettyä tämän työn kokoon ja laajuuteen suhteutettuna sopivina. On huomioitava, että tehty ryhmittely vaikuttaa analyysin tuloksiin, ja toisenlainen ryhmittelytapa olisi voinut tuottaa erilaisen lopputuloksen.

Myös kontrollien valinta piti pohtia tarkasti tähän työhön sopivaksi. Valinnan rajauksia korjattiin useamman kerran, jotta saatiin perustellusti valittua tähän työhön sopiva määrä kontrolleja. Suuremmankin määrän kontrolleja olisi voinut perustellusti ottaa mukaan, mutta työ olisi tässäkin kohden levinnyt liian laajaksi. Laajempi kontrollien valinta olisi voinut tuottaa erilaisen lopputuloksen.

Viitekehyksen validointia piti pohtia, koska viitekehystä ei tämän työn puitteissa ollut mahdollista kehittää niin pitkälle, että sen olisi voinut implementoida oikeasti käyttöön. Validoinnissa päädyttiin ulkopuoliseen asiantuntijaan, joka arvioi viitekehyksen kattavuuden, johdonmukaisuuden ja sovellettavuuden.

8 Yhteenveto ja jatkotutkimukset

Tässä luvussa tarkastellaan tätä työtä kokonaisuutena. Aluksi pohditaan, mitä tehtiin ja mitä työssä saavutettiin. Lopuksi koostetaan, miten tuloksia voisi käyttää, mitkä ovat niiden rajoitukset ja miten tästä voisi jatkaa.

8.1 Yhteenveto

Tämän työn tavoitteena oli muodostaa inhimilliset tekijät huomioiva käsitteellinen viitekehys, joka voisi auttaa organisaatioita toteuttamaan kyberturvallisuuslain vaatimukset ISO 27001 -standardia apuna käyttäen. Tätä varten oli tutustuttava kyberturvallisuuden lainsäädäntöön, ISO 27001 -standardiin ja inhimillisiin tekijöihin.

Työ aloitettiin tutustumalla kyberturvallisuuden lainsäädäntöön sekä EU-tasolla että Suomen kansallisella tasolla. Yksi tärkeimmistä EU:n kyberturvallisuuteen liittyvistä säädöksistä on kyberturvallisuusdirektiivi NIS2. Suomessa NIS2-direktiivin velvoitteet täyttää kyberturvallisuuslaki. Sen tavoitteena on parantaa yhteiskunnan kriittisten toimialojen kyberturvallisuustasoa. Laissa määritellään toimijat, joita laki velvoittaa. Nämä toimijat voivat käyttää ISO 27001 -standardia apunaan lain velvoitteiden täyttämiseen. Standardin noudattaminen on vapaaehtoista, mutta se on hyvä apuväline lain velvoitteiden täyttämisessä. Standardi velvoittaa sitä noudattavaa organisaatiota tekemään tietoturvallisuuden hallintajärjestelmän, jonka osana organisaation on tunnistettava omaan toimintaansa liittyvät riskit. Nämä riskit on arvioitava ja niille on suunniteltava käsittelyprosessit. Sitä varten on määriteltävä

riskin käsittelyyn tarvittavat tietoturvakontrollit ja toimenpiteet, miten kontrollit toteutetaan. Kontrolleja on lueteltu standardissa 93, mutta listan ulkopuolisiakin kontrolleja on sallittua käyttää, jos organisaation toiminta sitä vaatii.

Kyberturvallisuusriskiin vaikuttavien inhimillisten tekijöiden tunnistamiseksi suoritettiin kevennetty systemaattinen kirjallisuuskatsaus. Tähän käytettiin kahta tietokantaa: IEEE ja Web of Science. Tietokantahaulla saatiin 685 artikkelia, joista seulontojen jälkeen mukaan valikoitui 38 artikkelia. Näistä analyysiin mukaan kerättiin yhteensä 255 inhimillisen tekijän merkintää. Tunnistetut inhimilliset tekijät ryhmiteltiin, kunnes jäljellä oli kuusi pääryhmää: osaaminen, kognitiiviset tekijät, kiskikäyttäytyminen, asenteet ja motiivit, kuormitustekijät ja yksilön ominaisuudet.

Standardin 93 tietoturvakontrollia on jaoteltu standardissa neljään ryhmään: organisaatioon liittyvät, ihmisiin liittyvät, fyysiset ja teknologiset kontrollit. Samat ryhmät pidettiin tässä työssä. Mukaan valittiin ne kontrollit, joiden toteutumiseen tunnistetuilla inhimillisten tekijöiden pääryhmillä todettiin olevan vaikutusta. Inhimillisten tekijöiden pääryhmien ja valittujen standardin kontrollien välille saatiin yhteyksiä, joita perusteltiin kirjallisuuskatsauksen artikkeleilla. Tuloksena siis todettiin, että inhimilliset tekijät voivat vaikuttaa standardin tietoturvakontrollien toteutumiseen. Näin pystyttiin muodostamaan viitekehys, joka yhdistää inhimillisten tekijöiden pääryhmät standardin valittuihin kontrolleihin.

Viitekehyksen avulla todettiin, että kuormitustekijöiden, osaamisen ja riskikäyttäytymisen inhimillisten tekijöiden pääryhmillä on eniten vaikutusta valittujen kontrollien toteutumiseen. Erot olivat melko pieniä kyseisten pääryhmien välillä, joten lisätutkimuksen tarvetta on tämän asian suhteen. Organisaatioon liittyvät kontrollit osoittautuivat olevan eniten alttiita kaikkien pääryhmien inhimillisille tekijöille.

Tässä työssä todettiin, että inhimillisillä tekijöillä on vaikutusta standardin kontrollien toteutumiseen, joilla on yhteys kyberturvallisuuslakiin. Muodostetulla viitekehyksellä on siis yhteys kyberturvallisuuslakiin, jonka toteutumisessa se voi toimia

apuvälineenä. Kyberturvallisuuslaki velvoittaa tunnistamaan, arvioimaan ja hallitsemaan kyberturvallisuusriskejä, joista yksi on inhimillinen tekijä. Viitekehys voi tukea inhimillisten tekijöiden tunnistamisessa ja huomioimisessa. Laki määrittelee myös riskienhallinnasta ja johdon vastuusta, jotka ovat viitekehyksessä mukana useiden kontrollien kautta. Muodostetun viitekehyksen todettiinkin voivan toimia apuvälineenä kyberturvallisuuslain velvoitteiden täyttämisessä.

Tässä työssä muodostettiin viitekehys Kyberturvallisuuslain näkökulmasta. Käytetty standardi on kuitenkin kansainvälinen ja Kyberturvallisuuslaki EU:n NIS2:n valtiotason toimeenpano. Viitekehystä voitaisiin siis lähes suoraan jatkokehittää myös muissa EU-jäsenvaltioissa. Viitekehyksen käyttöönotto vaatii kuitenkin varmasti jatkotutkimusta ja -kehitystä inhimillisten tekijöiden syy-seuraus-suhteiden selvittämiseksi ja käytännön toimenpiteiden, toimialojen ja roolien tarkentamiseksi ja lisäämiseksi.

Kirjallisuudesta löytyy viitekehyksiä kyberturvallisuuteen ja inhimillisiin tekijöihin liittyen. Tämän työn viitekehystä vastaavaa, joka yhdistäisi inhimilliset tekijät ISO 27001 -standardin tietoturvakontrolleihin, ei aiemmasta tutkimuksesta löydetty. Lisäksi tämä työ kytkee viitekehyksen kyberturvallisuuslain velvoitteisiin. Tämä työ täyttää siten tunnistetun tutkimusaukon ja tarjoaa työkalun lain velvoittamille organisaatioille.

8.2 Jatkotutkimukset

Viitekehystä voisi laajentaa koskemaan suurempaa joukkoa kontrolleista. Tässä työssä keskityttiin valitsemaan ne kontrollit, jotka liittyvät päivittäiseen tekemiseen ja valmiuteen. Tässä kohden tämän työn ulkopuolelle jäi kontrolleja, jotka liittyvät inhimilliseen tekijään, mutta vain kertaluonteisesti, ajallisesti harvoin tai ovat erityisosaajien, kuten IT-henkilöstön, vastuulla. Jatkokehityksellä viitekehyksestä saisi entistä laajemman ja monipuolisemmin erilaisten organisaatioiden ja eri henkilös-

töryhmien käyttöön sopivan apuvälineen kyberturvallisuusriskien hallintaan. Myös viitekehyksen arvioija ehdotti jatkokehityksenä työntekijöiden roolien huomioimista. Tämä tukisi myös laajemman kontrollijoukon mukaan ottamista. Arvioija mainitsi erityisesti teknologisten kontrollien ryhmän, joihin rivityöntekijällä on hyvin vähäinen vaikutus, mutta IT- ja tietoturvahenkilöstön kohdalla vaikutus voi olla merkittävä. Lisäksi poikkeamatilanteisiin liittyvät kontrollit jäivät viitekehyksen ulkopuolelle. Lisäämällä ne viitekehykseen, siitä saadaan kehitettyä entistä kattavampi työkalu organisaatioiden käyttöön.

Tässä työssä muodostettiin teoreettinen viitekehys, jonka voisi tarpeellisten kehityskohteiden toteuttamisen jälkeen implementoida todellisessa ympäristössä. Implementointi voisi tapahtua pienessä tai keskisuuressa organisaatiossa, joka on suunnittelemassa ISO 27001 -standardin käyttöönottoa. Käyttöönoton jälkeen voisi myös suorittaa validoinnin. Tosin implementointia ennen viitekehyksen yhteyttä sekä Kyberturvallisuuslakiin että ISO 27001 -standardiin tulisi vahvistaa.

Lähdeluettelo

[1] World Economic Forum, *Global Cybersecurity Outlook 2026*, luettu: 22.1.2026, 2026. url: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.

[2] Euroopan unionin neuvosto, *Cybersecurity*, luettu: 10.3.2026, 2024. url: https://www.consilium.europa.eu/en/topics/cybersecurity/.

[3] Suomen eduskunta, *Kyberturvallisuuslaki*, luettu: 18.1.2026, 2025. url: https://www.finlex.fi/fi/lainsaadanto/saadoskokoelma/2025/124.

[4] Euroopan komissio, *Cybersecurity Strategy*, luettu: 10.3.2026, 2020. url: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

[5] SFS Suomen Standardit ry, *Mikä on standardi?*, luettu: 10.32026, 2024. url: https://sfs.fi/standardeista/mika-on-standardi/.

[6] Yleisradio, *"En ole valtavan yllättynyt" – tietoturva-asiantuntija kertoo, miten Helsingin tietomurto oli mahdollinen*, luettu: 10.3.2026, 2024. url: https://yle.fi/a/74-20088567.

[7] A. Sangwan, "Human Factors in Cybersecurity Awareness", teoksessa *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, Gurgaon, India, 2024, s. 1–7. DOI: 10.1109/ISCS61804.2024.10581139.

[8] Euroopan komissio, *Types of EU law*, luettu: 15.1.2026. url: https://commission.europa.eu/law/law-making-process/types-eu-law_en.

[9] Euroopan unionin neuvosto, *Timeline - cybersecurity*, luettu: 18.1.2026, 2025. url: https://www.consilium.europa.eu/en/policies/cybersecurity/timeline-cybersecurity/.

[10] Euroopan parlamentti ja Euroopan unionin neuvosto, *Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus)*, luettu: 18.1.2026, 2019. url: http://data.europa.eu/eli/reg/2019/881/oj.

[11] Euroopan parlamentti ja Euroopan unionin neuvosto, *Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847 digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös)*, luettu: 16.1.2026, 2024. url: http://data.europa.eu/eli/reg/2024/2847/oj.

[12] Euroopan parlamentti ja Euroopan unionin neuvosto, *Euroopan parlamentin ja neuvoston asetus (EU) 2025/38, toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberuhkien ja poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten ja asetuksen (EU) 2021/694 muuttamisesta (kybersolidaarisuussäädös))*, luettu: 18.1.2026, 2025. url: http://data.europa.eu/eli/reg/2025/38/oj.

[13] Euroopan parlamentti ja Euroopan unionin neuvosto, *Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554 finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU)*

N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta, luettu: 16.1.2026, 2022. url: http://data.europa.eu/eli/reg/2022/2554/oj.

[14] Euroopan parlamentti ja Euroopan unionin neuvosto, *Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557 kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta*, luettu: 18.1.2026, 2022. url: http://data.europa.eu/eli/dir/2022/2557/oj.

[15] Suomen eduskunta, *Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta*, luettu: 18.1.2026, 2025. url: https://www.finlex.fi/fi/lainsaadanto/2025/310?language=fin.

[16] Euroopan komissio, *The Commission calls on 23 Member States to fully transpose the NIS2 Directive*, luettu: 18.1.2026, 2024. url: https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive.

[17] Euroopan komissio, *NIS2 Directive implementation in Finland*, luettu: 18.1.2026, 2024. url: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-finland.

[18] Euroopan parlamentti ja Euroopan unionin neuvosto, *Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 verkko- ja tietojärjestelmien korkeatasoisen yhteisen kyberturvallisuuden varmistamisesta (NIS2-direktiivi)*, luettu: 13.1.2026, 2022. url: http://data.europa.eu/eli/dir/2022/2555/oj.

[19] Suomen eduskunta, *Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta*, luettu: 12.3.2026, 2025. url: https://www.finlex.fi/fi/lainsaadanto/saadoskokoelma/2025/125.

[20] Liikenne- ja viestintävirasto Traficom, *Kyberturvallisuuteen liittyvät säädökset*, luettu: 11.3.2026, 2026. url: https://traficom.fi/fi/saadokset?group=k

yberturvallisuus&limit=20&offset=0&query=&saadoksentyyppi=%255B10%255D&sort=created.

[21] Suomen eduskunta, *Asian käsittelytiedot HE 179/2025 vp*, luettu: 11.3.2026, 2025. url: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_179+2025.aspx.

[22] Suomen eduskunta, *Laki sähköisen viestinnän palveluista*, luettu: 11.3.2026, 2015. url: https://www.finlex.fi/fi/lainsaadanto/2014/917.

[23] N. Robinson, "Human Factors Security Engineering: The Future of Cybersecurity Teams", *EDPACS*, vol. 67, nro 5, s. 1–17, 2023. DOI: 10.1080/07366981.2023.2211429.

[24] B. Cusack ja K. Adedokun, "The Impact of Personality Traits on User's Susceptibility to Social Engineering Attacks", teoksessa *Proceedings of the 16th Australian Information Security Management Conference*, Perth, Australia: Edith Cowan University, 2018, s. 83–89. DOI: 10.25958/5c528ffa66693.

[25] H. W. Glaspie ja W. Karwowski, "Human Factors in Information Security Culture: A Literature Review", teoksessa *Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity*, Los Angeles, California, USA: Springer, 2017, s. 269–280. DOI: 10.1007/978-3-319-60585-2_25.

[26] M. Arif, M. Badila, J. M. Warden ja A. Ur Rehman, "A Study of Human Factors Toward Compliance with Organization's Information Security Policy", *Information Security Journal*, vol. 34, nro 3, s. 235–250, 2025. DOI: 10.1080/19393555.2025.2457702.

[27] J. Mason, *Cybersecurity Beginner's Guide*, 2. painos. Birmingham, UK: Packt Publishing, 2025, luku 5, ISBN: 978-1836207474.

[28] W. J. Triplett, "Addressing Human Factors in Cybersecurity Leadership", *Journal of Cybersecurity and Privacy*, vol. 2, nro 3, s. 573–586, 2022. DOI: 10.3390/jcp2030029.

[29] K. Khadka ja A. B. Ullah, "Human Factors in Cybersecurity: An Interdisciplinary Review and Framework Proposal", *International Journal of Information Security*, vol. 24, nro 3, s. 119, 2025. DOI: 10.1007/s10207-025-01032-0.

[30] S. Thomson, M. Bewong, A. Mahboubi ja T. Zia, "Social Engineering Attacks: A Systemisation of Knowledge on People Against Humans", teoksessa *2025 IEEE International Conference on Big Data (BigData)*, Macau, China, 2025, s. 3752–3761. DOI: 10.1109/BigData66926.2025.11402315.

[31] D. Tan Jia Jun, A. Sahban Rafsanjani, S. Aslam ja M. Behjati, "Human Factors in Information Security: A Quantitative Study with Technical Solutions to Prevent Social Engineering Attacks", *Digital Threats: Research and Practice*, vol. 6, nro 4, s. 1–35, 2025. DOI: 10.1145/3767320.

[32] D. Arévalo, D. Valarezo, W. Fuertes, M. F. Cazares, R. O. Andrade ja M. Macas, "Human and Cognitive Factors involved in Phishing Detection. A Literature Review", teoksessa *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*, Las Vegas, Nevada, USA, 2023, s. 608–614. DOI: 10.1109/CSCE60160.2023.00105.

[33] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci ja M. F. Costabile, "Human Factors in Phishing Attacks: A Systematic Literature Review", *ACM Computing Surveys*, vol. 54, nro 8, s. 173, 2021, ISSN: 0360-0300. DOI: 10.1145/3469886.

[34] International Organization for Standardization, *ISO — International Organization for Standardization*, luettu: 14.1.2026. url: https://www.iso.org.

[35] FINAS, *FINAS-Akkreditointipalvelu*, luettu: 14.1.2026. url: https://www.finas.fi/Sivut/default.aspx.

[36] R. d. S. Leme, J. de Souza Pinto, L. G. Zanon, T. F. Sigahi, G. H. S. M. d. Moraes, S. R. Moro ja R. Anholon, "Information security management: a fuzzy DEMATEL analysis of the new ISO/IEC 27001:2022 controls", *Information and Computer Security*, 2025. DOI: 10.1108/ICS-10-2024-0269.

[37] *SFS-EN ISO/IEC 27001:2023 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, English language version, SFS Suomen Standardit ry, 2023.

[38] M. Elgeddawy ja M. Abouraia, "Pragmatism as a Research Paradigm", teoksessa *Proceedings of the 23rd European Conference on Research Methodology for Business and Management Studies*, vol. 23, Porto, Portugal, 2024. DOI: 10.34190/ecrm.23.1.2444.

[39] P. A. Busch, "Philosophical stances in information systems research: a case analysis and critical reflection", *Humanities and Social Sciences Communications*, vol. 13, nro 1, 2026. DOI: 10.1057/s41599-025-06427-x.

[40] B. Eltahawy, "An Integration of Cyberprivacy, Cybersecurity, and Smart Grid Strategies for Protecting Critical Infrastructure", Ph.D. dissertation, University of Vaasa, Vaasa, Finland, 2025, ISBN: 978-952-395-227-0.

[41] F. Li, S. Han, C.-H. Lee, S. Feng, Z. Jiang ja Z. Sun, "A New Era in Human Factors Engineering: A Survey of the Applications and Prospects of Large Multimodal Models", *International Journal of Human–Computer Interaction*, vol. 41, nro 18, s. 11 867–11 880, 2025. DOI: 10.1080/10447318.2024.2446511.

[42] M. Alsharif, S. Mishra ja M. AlShehri, "Impact of Human Vulnerabilities on Cybersecurity.", *Computer Systems Science & Engineering*, vol. 40, nro 3, s. 1153–1166, 2022. DOI: 10.32604/csse.2022.019938.

[43] E. Thron, S. Faily ja H. Dogan, "Human Factors and Cyber Security Risks on the Railway - The Critical Role Played by Signalling Operations", *Information and Computer Security*, vol. 32, nro 2, s. 236–263, 2024, ISSN: 2056-4961. DOI: 10.1108/ICS-05-2023-0078.

[44] H. Abroshan, J. Devos, G. Poels ja E. Laermans, "COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic", *IEEE Access*, vol. 9, s. 121 916–121 929, 2021. DOI: 10.1109/ACCESS.2021.3109091.

[45] Z. Wang, H. Zhu ja L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods", *IEEE Access*, vol. 9, s. 11 895–11 910, 2021. DOI: 10.1109/ACCESS.2021.3051633.

[46] C. Spruill, M. Khalil ja S. Olatunbosun, "Models for Security Management", teoksessa *Image Processing, Computer Vision, and Pattern Recognition and Information and Knowledge Engineering*, sarja Communications in Computer and Information Science, L. Deligiannidis, F. Ghareh Mohammadi, F. Shenavarmasouleh, S. Amirian ja H. R. Arabnia, toim., vol. 2262, Springer, Cham, 2025, s. 354–361. DOI: 10.1007/978-3-031-85933-5_26.

[47] Z. Avrahami ja M. Zwilling, "The impact of cyber threat intelligence (CTI) on employee behavior and skills and the implications for organizational cyber resilience", *International Journal of Information Security*, vol. 24, s. 184, 2025. DOI: 10.1007/s10207-025-01096-y.

[48] G. El Hajal, R. Abi Zeid Daou ja Y. Ducq, "Human Firewall: Cyber Awareness using WhatsApp AI Chatbot", teoksessa *2021 IEEE 3rd International Multi-*

disciplinary Conference on Engineering Technology (IMCET), Beirut, Lebanon, 2021, s. 66–70. DOI: 10.1109/IMCET53404.2021.9665642.

[49] F. Z. Gozon, D. Vaczi ja E. Toth-Laufer, "Fuzzy-based Human Factor Centered Cybersecurity Risk Assessment", teoksessa *2021 IEEE 19th International Symposium on Intelligent Systems and Informatics (SISY)*, Subotica, Serbia, 2021, s. 83–88. DOI: 10.1109/SISY52375.2021.9582520.

[50] K. C. Roy ja G. Chen, "GraphCH: A Deep Framework for Assessing Cyber-Human Aspects in Insider Threat Detection", *IEEE Transactions on Dependable and Secure Computing*, vol. 21, nro 5, s. 4495–4509, 2024. DOI: 10.1109/TDSC.2024.3353929.

[51] P. K. Yeng, M. A. Fauzi ja B. Yang, "A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals", *Information*, vol. 13, s. 335, 2022. DOI: 10.3390/info13070335.

[52] A. Vallejo-Blanxart ja L. Pătraș, "Cybersecurity risks in internship programs: Intern training gaps and organizational vulnerabilities", *Industry and Higher Education*, s. 1–12, 2026. DOI: 10.1177/09504222261417831.

[53] A. Pollini, T. C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi ja D. Guerri, "Leveraging human factors in cybersecurity: an integrated methodological approach", *Cognition, Technology & Work*, vol. 24, s. 371–390, 2022. DOI: 10.1007/s10111-021-00683-y.

[54] M. Alexander ja C. Candiwan, "A Conceptual Model of Information Security Compliance and Protection Behavior through Stimulus-Organism-Response Theory", teoksessa *2024 IEEE International Conference on Computing (ICOCO)*, Kuala Lumpur, Malaysia, 2024, s. 503–508. DOI: 10.1109/ICOCO62848.2024.10928261.

[55] M. U. Shah, F. Iqbal, U. Rehman ja P. C. K. Hung, "A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance", *IEEE Access*, vol. 11, s. 87 970–87 984, 2023. DOI: 10.1109/ACCESS.2023.3296580.

[56] D. Buil-Gil, N. Lord ja E. Barrett, "The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention", teoksessa *The new technology of financial crime*, 2022, s. 5–34. DOI: 10.1080/15564886.2020.1814468.

[57] P. B. Vásquez-Méndez, D. C. Arce Cuesta ja J. L. Zambrano-Martinez, "The Human Factor: Assessing Ransomware Vulnerability in Developing Nations' Governments", *Information*, vol. 17, nro 2, s. 211, 2026. DOI: 10.3390/info17020211.

[58] K. A. Cole, A. L. Francis, M. K. Rogers ja J. Balazs, "Can individual differences in cognitive capacity predict cybersecurity performance?", *Computers Security*, vol. 155, s. 104 497, 2025, ISSN: 0167-4048. DOI: 10.1016/j.cose.2025.104497.

[59] E. A. Kenlie, C. N. Hendris, N. Nadia ja F. Adeta, "The Impact of Human Error in Cybersecurity Breaches: Understanding Behavioral Patterns and Mitigation Strategies", teoksessa *2024 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, Tangerang, Indonesia, 2024, s. 1045–1050, ISBN: 979-8-3315-3324-3. DOI: 10.1109/ICIMCIS63449.2024.10956680.

[60] S. Nifakos, K. Chandramouli, C. K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis ja S. Bonacina, "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review", *Sensors*, vol. 21, nro 15, s. 5119, 2021, ISSN: 1424-8220. DOI: 10.3390/s21155119.

[61] S. Subramaniam, U. A. Mokhtar, Z. Shukur, A. Ahmad, S. R. S. Othman ja B. I. Cheong, "Key Factors Influencing Situational Awareness for Incident Response in Healthcare", teoksessa *2025 3rd International Conference on Cyber Resilience (ICCR)*, Dubai, UAE, 2025, s. 1–7. DOI: 10.1109/ICCR67387.2025.11292458.

[62] F. Masimba, F. Gumbo ja T. Zuva, "Deciphering the Influence of Human Behavior on Cybersecurity Risks: An In-depth Review of Amplification and Mitigation Factors", teoksessa *2025 5th International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, Pretoria, South Africa, 2025, s. 1–6. DOI: 10.1109/IMITEC67386.2025.11410469.

[63] J. Tilbury, S. Flowerday, G. Bott, Y. T. Chua, E. Olson ja B. Foltz, "Human-Factor Vulnerabilities of Automation in SOCs: A Mixed-Methods Multigroup Analysis", *Computers & Security*, s. 104 871, 2026. DOI: 10.1016/j.cose.2026.104871.

[64] N. Nelufule, "The Impact of Human Aspects of Information and Cybersecurity: A Systematic Literature Survey", teoksessa *2025 MIPRO 48th ICT and Electronics Convention*, Opatija, Croatia, 2025, s. 843–848. DOI: 10.1109/MIPRO65660.2025.11131905.

[65] T. Alharbi, "A Holistic Evaluation Model for Information Security Awareness Programs in Work Environment", teoksessa *2023 Eighth International Conference On Mobile And Secure Services (MobiSecServ)*, Miami, Florida, USA, 2023, s. 1–4. DOI: 10.1109/MobiSecServ58080.2023.10329041.

[66] V. Santa Barletta, M. Calvano, F. Caruso, A. Curci ja A. Piccinno, "Serious games for cybersecurity: how to improve perception and human factors", teoksessa *2023 IEEE International Conference on Metrology for eXtended Reality,*

Artificial Intelligence and Neural Engineering (MetroXRAINE), Milan, Italy, 2023, s. 1110–1115. DOI: 10.1109/METROXRAINE58569.2023.10405607.

[67] S. Ansong ja A. Ghorbani, "Securing the Loop: A Risk Assessment Framework for Human-in-the-Loop Vulnerabilities Across SAE Levels of Autonomy", teoksessa *2025 7th International Conference on Intelligent Autonomous Systems (ICoIAS)*, Osaka, Japan, 2025, s. 57–65. DOI: 10.1109/ICOIAS69065.2025.00016.

[68] A. Ayodeji, M. Mohamed, L. Li, A. Di Buono, I. Pierce ja H. Ahmed, "Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors", *Progress in Nuclear Energy*, vol. 161, s. 104 738, 2023. DOI: 10.1016/j.pnucene.2023.104738.

[69] M. L. Green ja P. Dozier, "Understanding Human Factors of Cybersecurity: Drivers of Insider Threats", teoksessa *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, Venice, Italy, 2023, s. 111–116. DOI: 10.1109/CSR57506.2023.10224926.

[70] K. Bissadu, G. Hossain, L. P. Velagala ja S. Sonko, "Analyzing Insider Cyber Threats and Human Factors within the Framework of Agriculture 5.0", teoksessa *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, San Antonio, Texas, USA, 2024, s. 1–5. DOI: 10.1109/ISDFS60797.2024.10527290.

[71] T. Schaltegger, B. Ambuehl, N. Bosshart, A. Bearth ja N. Ebert, "Human behavior in cybersecurity: an opportunity for risk research", *Journal of risk research*, vol. 28, nro 8, s. 843–854, 2025. DOI: 10.1080/13669877.2025.2539109.

[72] K. Kioskli, T. Fotis, S. Nifakos ja H. Mouratidis, "The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-

Hygiene in Healthcare 4.0", *Applied Sciences*, vol. 13, nro 6, s. 3410, 2023, ISSN: 2076-3417. DOI: 10.3390/app13063410.

[73] D. Matijašić-Bodalec, A. Bajan, K. Šolić, P. Mamić, T. Velki, N. Bajan, A. Milostić-Srb, N. Srb, I. Fosić, S. Čukljek et al., "The Connection Between Daily/General Stress Experience and Risky Internet Behavior Among Students of Health and Non-Health Studies", *Acta Clinica Croatica*, vol. 64, nro 4, s. 716–725, 2025. DOI: 10.20471/acc.2025.64.04.08.

[74] S. Vrhovec ja B. Markelj, "We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers", *PLOS ONE*, vol. 19, nro 10, e0312266, 2024. DOI: 10.1371/journal.pone.0312266.

[75] Z. Tari ja R. Mahmud, "Augmenting Digital Ecosystem Resilience Through Human-Centric Cybersecurity Solutions", *IEEE Transactions on Engineering Management*, 2025. DOI: 10.1109/TEM.2025.3606637.

[76] *SFS-EN ISO/IEC 27002:2022:en Information security, cybersecurity and privacy protection. Information security controls*, English language version, SFS Suomen Standardit ry, 2022.

[77] E. Y. Handri, D. Indra Sensuse ja A. Tarigan, "Developing an Agile Cybersecurity Framework With Organizational Culture Approach Using Q Methodology", *IEEE Access*, vol. 12, s. 108 835–108 850, 2024. DOI: 10.1109/ACCESS.2024.3432160.

[78] N. H. Chowdhury, M. T. Adam ja T. Teubner, "Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures", *Computers & Security*, vol. 97, s. 101 931, 2020, ISSN: 0167-4048. DOI: 10.1016/j.cose.2020.101931.

[79] D. Lucini, E. Pagani, F. Capria, M. Galiano, M. Marchese, S. Cribellati ja G. Parati, "Age Influences on Lifestyle and Stress Perception in the Working Population", *Nutrients*, vol. 15, nro 2, s. 399, 2023. DOI: 10.3390/nu15020399.

[80] G. Mikneviciute, M. M. Pulopulos, J. Allaert, A. Armellini, U. Rimmele, M. Kliegel ja N. Ballhausen, "Adult age differences in the psychophysiological response to acute stress", *Psychoneuroendocrinology*, vol. 153, s. 106 111, 2023, ISSN: 0306-4530. DOI: 10.1016/j.psyneuen.2023.106111.

[81] M. Awada, B. Becerik Gerber, G. M. Lucas ja S. C. Roll, "Stress appraisal in the workplace and its associations with productivity and mood: Insights from a multimodal machine learning analysis", *PLOS ONE*, vol. 19, nro 1, e0296468, 2024. DOI: 10.1371/journal.pone.0296468.

[82] J. J. Gonzalez ja A. Sawicka, "A Framework for Human Factors in Information Security", teoksessa *Proceedings of the WSEAS International Conference on Information Security*, Rio de Janeiro, Brazil, 2002, s. 448–487.

[83] Š. Grigaliūnas, M. Schmidt, R. Brūzgiene, P. Smyrli, S. Andreou ja A. Lopata, "Holistic Information Security Management and Compliance Framework", *Electronics*, vol. 13, nro 19, s. 3955, 2024. DOI: 10.3390/electronics13193955.

[84] I. Alhasan, "Toward Proactive Cybersecurity: A Cultural Risk Profiling Framework for Predictive Cybersecurity Analytics", teoksessa *2025 3rd International Conference on Foundation and Large Language Models (FLLM)*, Vienna, Austria: IEEE, 2025, s. 954–960. DOI: 10.1109/FLLM67465.2025.11391026.

Liite A Inhimilliset tekijät

Seuraavassa taulukossa on esitetty kirjallisuuskatsauksessa tunnistetut inhimilliset tekijät luokiteltuina kuuteen pääluokkaan, jotka on järjestetty lähteiden lukumäärän mukaan laskevaan järjestykseen. Sarakkeet vasemmalta oikealle: lähteiden lukumäärä, ryhmän nimi sekä englanninkieliset käsitteet lähteineen. Englanninkieliset käsitteet on otettu lähtökohtaisesti suoraan artikkeleista aina kun se on ollut mahdollista.

88 OSAAMINEN	
31 riittämätön tietoisuus	low awareness [54]; lack of awareness [42]; situation awareness degradation [67]; lack of awareness [32]; low awareness, lack of awareness [47]; loss of situation awareness [68]; user awareness [66]; awareness [56]; lack of awareness [33]; awareness [48]; insufficient awareness, low security awareness [49]; awareness [69]; lack of awareness [31]; lack of awareness [59]; lack of awareness [72]; lack of risk awareness [62]; awareness [73]; lack of awareness [64]; lack of awareness [60]; lack of awareness [53]; outdated awareness [7]; lack of awareness [55]; low awareness [61]; limited awareness [30]; lack of awareness [43]; loss of awareness [63]; unawareness [52]; low awareness [57]; low awareness [74]; low awareness [45]; awareness [51]

20	riittämätön koulutus ja harjoittelu	lack of training, insufficient training and education [54]; untrained [68]; education [66]; lack of training [56]; lack of training [48]; lack of training, outdated training [69]; lack of training [59]; lack of training, education [72]; inadequate training, lack of learning [62]; lack of education [73]; lack of training [64]; lack of training [60]; insufficient training [53]; training [7]; limited education, lack of training [55]; lack of training [61]; lack of education [31]; training gaps [43]; lack of training [52]; insufficient training [57]
17	riittämätön tieto	insufficient knowledge [54]; lack of knowledge [65]; lack of knowledge [32]; insufficient knowledge [66]; lack of knowledge [70]; knowledge [56]; lack of knowledge [33]; not knowing, knowledge [69]; lack of knowledge [59]; lack of knowledge [72]; absence, lack of knowledge [62]; lack of knowledge [64]; knowledge-attitude-behaviour mismatch [53]; knowledge [7]; insufficient knowledge [30]; knowledge [43]; knowledge [45]
9	puutteellinen ymmärrys	inaccurate perception [47]; unable to understand the risks [33]; lack of understanding [69]; struggle with understanding [59]; lack of understanding [72]; irregularities in risk perception [62]; understanding [7]; limited understanding [55]; lack of understanding [43]
7	kokemuksen puute	lack of experience [42]; lack of experience [32]; experience [7]; lack of prior exposure to cyber incidents [61]; low experience [74]; inexperience [45]; experience [51]
4	tietämättömyys	ignorance [48]; ignorance [69]; ignorance [31]; ignorance [72]

54 KOGNITIIVISET TEKIJÄT

11	riskien havaitsemisen haasteet	risk perception [32]; low sensitivity to anomalies [47]; underestimate risks [66]; belief in the harmlessness [69]; underestimation of threats [7]; low risk perception [71]; cognitive capacity for threat detection [61]; underestimation of threat severity [75]; risk misperception [43]; risk perception [57]; distorted threat perception [45]

8	kognitiiviset vinoumat ja harhat	confirmation bias [47]; cognitive biases [59]; cognitive biases [62]; cognitive biases [53]; cognitive biases [7]; cognitive biases [75]; automation bias [63]; cognitive bias [45]
8	kognitiivinen kuormitus	cognitive workload [32]; information overload [33]; high cognitive load [62]; high workload [61]; cognitive load [31]; cognitive overload [43]; cognitive overload [63]; thought overload [45]
7	päätöksenteon haasteet	decision-making [32]; poor decision making [72]; poor decision-making [62]; decision-making [71]; decision-making [31]; unsafe security decisions [75]; decision-making [43]
7	heikentynyt tarkkaavaisuus	low attentional vigilance [32]; lack of attention [66]; limited attention [33]; reduced vigilance [60]; reduced vigilance [7]; limited attention, vigilance [61]; reduced vigilance [63]
5	pelko	fear [44]; fear [32]; fear [33]; fear [31]; fear [45]
4	emotionaalinen haavoittuvuus	emotional weakness [31]; emotional factors [59]; emotional states [62]; emotional stability [51]
4	hälytysväsymys	alarm fatigue [67]; desensitization to alarms, habituation [62]; disregard of security alert [61]; alert fatigue [63]

48 RISKIKÄYTTÄYTYMINEN

14	riskialtis käyttäytyminen	risk-taking behaviour [44]; risky behaviour [84]; unsafe behaviour [33]; risk-taking behaviour [59]; risky behaviour [72]; risky behaviour [73]; engaging in risky actions [50]; risky behaviour [7]; risky behaviour [31]; risky/unsafe behaviour [75]; unsafe security behaviour [30]; risky behaviour [43]; vulnerable behaviour [45]; risky behaviour [51]
13	luottamushaasteet	trust [84]; tendency to trust [42]; overreliance, trust manipulation [67]; trust [32]; reliability issues [68]; overconfidence [33]; overconfidence [59]; overconfident [64]; overconfidence [53]; overconfidence [7]; over-reliance [55]; exploited trust [31]; hubris [45]

11	huolimattomuus	carelessness [42]; carelessness [32]; human negligence [47]; user negligence, carelessness [70]; lack of caring [69]; negligence [59]; carelessness [72]; carelessness, negligence [60]; carelessness [7]; careless actions [31]; carelessness [45]
7	sääntöjen rikkominen	unintentional misuse [68]; non-compliant behaviour [65]; unintentionally harm [66]; unintentional policy violation [69]; bypassing security restrictions [53]; accidental, unintentional [43]; security circumvention [51]
3	liiallinen uteliaisuus	curiosity [66]; curiosity [31]; curiosity [45]

24 ASENTEET, USKOMUKSET JA MOTIIVIT

7	asennehaasteet	attitude [33]; negative attitude [31]; inappropriate attitudes [72]; attitudes [53]; differences in attitudes [75]; change in attitude [43]; attitude risk [51]
6	liiallinen teknologiaan luottaminen	greater trust in technological tools [72]; over-reliance on technological solutions [7]; over-trust in technical protection [71]; assumption that systems will handle threats [61]; over-trust in automation [43]; overreliance on automated recommendations [63]
4	pahantahtoinen toiminta	malicious intent [68]; intentionally harm [66]; fraudulent activities [70]; malignancy of the user [48]
4	välinpitämättömyys	complacency [32]; complacency [33]; lack of caring [69]; casual attitudes [7]
3	väärät uskomukset	false beliefs [71]; false beliefs [43]; false beliefs [51]

22 KUORMITUSTEKIJÄT

10	stressi	stress [44]; stress [32]; stress [66]; stress [33]; stress [59]; stress [62]; stress [73]; stress [60]; psychological stress [31]; stress [43]
7	väsymys	fatigue [66]; fatigue [33]; fatigue [59]; fatigue [72]; fatigue [62]; exhaustion [61]; fatigue [43]
5	paine ja kiire	time pressure, urgency [32]; pressure [33]; time pressure [61]; time pressure [45]; work emergency [51]

19 YKSILÖN OMINAISUUDET	
8 ikä	age [84]; age [69]; age [59]; age [60]; age [75]; age [43]; age [52]; age [74]
6 sukupuoli	gender [84]; gender [60]; gender [55]; gender [43]; gender [52]; gender [74]
5 persoonallisuus	personality traits [32]; personality [60]; personality traits [75]; personality traits [43]; personality traits [45]

Liite B Arviointikysely

1. Viitekehyksen kattavuus.

Vastaukset

Viitekehys sisältää keskeiset inhimilliset tekijät.	Viitekehys huomioi keskeiset ISO 27001 -kontrollit.	Viitekehys käsittelee aihetta riittävän laajasti.	Viitekehyksestä ei puutu oleellisia asioita.
täysin samaa mieltä	jokseenkin samaa mieltä	täysin samaa mieltä	jokseenkin samaa mieltä

2. Viitekehyksen johdonmukaisuus.

Vastaukset

Viitekehyksen rakenne on selkeä.	Inhimillisten tekijöiden valinta on kuvattu loogisesti.	Kontrollien valinta on kuvattu loogisesti.	Viitekehyksen muodostaminen on kuvattu selkeästi.	Viitekehys on johdonmukainen.	Viitekehyksessä ei ole ristiriitaisuuksia.
jokseenkin samaa mieltä	jokseenkin samaa mieltä	jokseenkin eri mieltä	neutraali	neutraali	jokseenkin samaa mieltä

3. Viitekehyksen sovellettavuus.

Vastaukset

Viitekehys on helposti ymmärrettävä.	Viitekehystä voidaan käytännössä hyödyntää organisaatioissa.	Viitekehys soveltuu eri toimialoille.	Viitekehys tukee ISO 27001 vaatimusten huomioimista.	Viitekehys tukee Kyberturvallisuuslain vaatimusten huomioimista.
jokseenkin samaa mieltä	neutraali	jokseenkin samaa mieltä	neutraali	neutraali

Avoimet kysymykset:

4. Mitkä ovat viitekehyksen vahvuudet?

5. Mitä viitekehyksestä puuttui?

6. Miten viitekehystä voisi kehittää?

7. Missä tilanteissa viitekehyksestä voisi olla käytännön hyötyä?