Waltteri Iivanainen

ISO/IEC 27001 -STANDARDIN PÄIVITYS

Siirtyminen 2013-versiosta 2022-versioon

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

2024

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä	Waltteri Iivanainen
Työn nimi	ISO/IEC 27001 -standardin päivitys: Siirtyminen 2013-versiosta 2022-versioon
Toimeksiantaja	Elisa Oyj
Vuosi	2024
Sivut	76 sivua, liitteitä 4 sivua
Työn ohjaaja	Kimmo Kääriäinen

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli tutkia ja analysoida, mitä toimenpiteitä Elisa Oyj:n tulee ottaa huomioon siirtyessään ISO/IEC 27001:2013 -standardista päivitettyyn ISO/IEC 27001:2022 -standardiin. Vuoden 2022-versio sisältää useita päivityksiä, jotka vastaavat paremmin nykyisiä tietoturvauhkia ja teknologisen ympäristön muutoksia. Tutkimuksen keskeisenä tehtävä oli selvittää, mitä uusia vaatimuksia päivitetty versio tuo mukanaan, mitä organisaatioiden tulee huomioida siirtymäprosessissa ja miten uudet vaatimukset voidaan toteuttaa käytännössä.

ISO/IEC 27001:2022 -standardi sisältää uusia hallintakeinoja ja vaatimuksia, jotka organisaatioiden on huomioitava standardin siirtymäprosessissa. Liitteessä A tehdyt muutokset edellyttävät, että organisaatiot arvioivat hallintakeinonsa uudelleen. Nämä hallintakeinot ovat suunniteltu auttamaan organisaatioita hallitsemaan tietoturvallisuuteen liittyviä riskejä.

Kattavan ja luotettavan aineiston kerääminen oli olennaista, jotta voitiin hyödyntää laajasti alan asiantuntijoiden näkemyksiä. Tämä mahdollisti konkreettisten toimenpiteiden ja ohjeistusten kehittämisen organisaatioiden siirtymäprosessin tueksi.

Opinnäytetyön tuloksena saatiin luotua kattava kuvaus ISO/IEC 27001:2022 -standardin vaatimuksista ja uusista hallintakeinoista. Lisäksi laadittiin ohjeistus, joka kuvaa kattavasti, mitä organisaatioiden tulee huomioida siirtymäprosessissa. Opinnäytetyö tarjoaa Elisa Oyj:lle kattavan ohjeistuksen ja konkreettisia toimenpiteitä, jotka tukevat sujuvaa siirtymistä kohti ISO/IEC 27001:2022 -standardia.

Asiasanat: hallintakeinot, ISO, ISO/IEC 27001:2022, ISMS, kyberturvallisuus, standardi, tietoturvallisuuden hallintajärjestelmä

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author	Waltteri Iivanainen
Thesis title	ISO/IEC 27001 standard update: Transitioning from the 2013 version to the 2022 version
Commissioned by	Elisa Oyj
Time	2024
Pages	76 pages, 4 pages of appendices
Supervisor	Kimmo Kääriäinen

ABSTRACT

The purpose of the thesis was to investigate and analyze the measures that Elisa Oyj must consider when transitioning from the ISO/IEC 27001:2013 standard to the updated ISO/IEC 27001:2022 standard. The 2022 version includes several updates that more directly respond to current cybersecurity threats and changes in the technological environment. The thesis focused on identifying the new requirements introduced by the updated version, defining the aspects that organizations need to consider during the transition process, and exploring practical ways to implement these requirements.

The ISO/IEC 27001:2022 standard includes new control measures and requirements that organizations must carefully consider, particularly the changes made in Annex A. These control measures are designed to help organizations manage risks related to information security.

Collection of comprehensive and reliable data was essential to thoroughly utilize the perspectives of industry experts. This facilitated the presentation of practical steps and tips to assist organizations through the transition process.

As a result, the thesis provides a detailed overview of the ISO/IEC 27001:2022 standard's requirements and new control measures. Also, a guide was produced outlining the procedures that organizations should consider during the transition process. For the commissioner, the thesis provides comprehensive guidance and concrete measures that support a smooth transition towards the ISO/IEC 27001:2022 standard.

Keywords: control measures, cybersecurity, information security management system, ISO, ISO/IEC 27001:2022, ISMS, standard

SISÄLLYS

1 JOHDANTO

Opinnäytetyö käsittelee ISO/IEC 27001 -standardin siirtymäprosessia vuoden 2013-versiosta vuoden 2022-versioon. Tutkimus keskittyy erityisesti siihen, miten standardin päivitys vaikuttaa organisaation tietoturvakäytäntöihin. Siltainsuun (2017) tutkimus osoittaa, että modernissa tietoyhteiskunnassa kyberrikollisuuden muotojen moninaistuessa tietoturvan merkitys korostuu. Tätä tukee Crawley (2022, 45–46), joka osoittaa, että suurin osa tietoturvaloukkauksista johtuu ulkoisten tekijöiden suorittamista kyberhyökkäyksistä. Opinnäytetyö on siis ajankohtainen, sillä digitaalisen tietoturvaympäristön nopea kehitys ja kyberturvauhkien monimuotoistuminen tekevät jatkuvista päivityksistä ja standardien uudistuksista välttämättömiä. Myös Aaltonen (2023) mainitsee, että ISO/IEC 27001:2022 -standardin päivitys on tärkeä, sillä tietoturvaympäristö on muuttunut merkittävästi.

Elisa Oyj, joka toimii opinnäytetyön toimeksiantajana, on suomalainen tietoliikenne- ja digitaalisten palveluiden markkinajohtaja (Digitalisaatiolla kestävä tulevaisuus s.a.). Yhtiön pyrkimys on varmistaa korkeatasoinen tietoturva kaikissa toiminnoissaan (Yrityksen tietoturva s.a.). Yhtiön kokonaisvaltainen lähestymistapa riskienhallintaan heijastaa sen sitoutumista turvallisen ja luotettavan toimintaympäristön ylläpitämiseen (Vastuullisuusriskien hallinta s.a.). Nämä korostavat ISO/IEC 27001:2022 -standardin merkitystä, sillä standardi tarjoaa kattavan kehyksen tietoturvariskien hallintaan (ISO/IEC 27001: 2022).

ISO/IEC 27001:2022 -standardi sisältää päivityksiä, jotka heijastavat nykyisen tietoturvaympäristön muutoksia ja uusia uhkia (Kiwa Inspecta 2023a). Nämä muutokset edellyttävät yrityksiltä huolellista suunnittelua, sopeutumista ja toimenpiteiden implementointia. Tutkimuksen päätavoitteena on tuottaa syvällinen analyysi ISO/IEC 27001:2022 -standardin tuomista muutoksista ja tarjota Elisa Oyj:lle näkökulmia, joiden avulla se voi parantaa tietoturvan tasoaan ja varmistaa sujuvan siirtymän standardin uusiin vaatimuksiin.

2 TUTKIMUSASETELMA

Kanasen (2014a) mukaan tutkimusasetelma kytkeytyy tiiviisti tutkimuksen aiheeseen ja koostuu tutkittavasta ongelmasta sekä valituista tutkimusmenetelmistä. Tutkimusasetelmat kattavat erilaisia tapoja kerätä, analysoida, tulkita ja raportoida aineistoa (Vilkka & Mankki 2024, 58). Lisäksi tutkimusasetelma tarjoaa suunnitelman tutkimuskysymysten ratkaisemiseksi käyttämällä valikoituja tiedonkeruumenetelmiä (Saaranen-Kauppinen & Puusniekka. 2006, 12).

Tämän luvun kuvaus perustuu Kanasen (2017, 13) ajatuksiin tutkimusotteista, tutkimusmenetelmistä sekä aineistonkeruu- ja analyysimenetelmistä. Tutkimusotteet voidaan jaotella useilla eri tavoilla, mutta yksinkertaisimmillaan ne voidaan ryhmitellä laadullisiin ja määrällisiin tutkimuksiin. Otteet muodostavat tutkimuksen metodologian, jonka alle sijoittuvat erilaiset tutkimusmenetelmät, eli metodit. Tutkimusotteet myös määrittelevät tutkimusmenetelmät. Tutkimusmenetelmät puolestaan jakautuvat aineistonkeruu- ja analyysimenetelmiin. Kullekin aineistonkeruumenetelmälle on kehitetty sille ominaiset aineiston analyysimenetelmät.

Tämä opinnäytetyö on toteutettu monimenetelmäisenä tutkimuksena, joka yhdistää laadullisia ja määrällisiä tutkimusmenetelmiä. Viime vuosikymmeninä monimenetelmäiset tutkimukset ovat kasvattaneet suosiotaan. Tämä johtuu niiden kyvystä tarjota laajempia ja monipuolisempia näkökulmia verrattuna niihin tutkimuksiin, jotka tukeutuvat ainoastaan yhteen menetelmään. (Vilkka & Mankki 2024, 9.) Laadullinen tutkimus nähdään usein määrällisen tutkimuksen vastakohtana. Vaikka näiden kahden tutkimusotteen eroja korostetaan usein, on mahdollista käyttää molempia otteita samassa tutkimuksessa. Näiden yhdistämisen avulla voidaan saavuttaa erilaisia näkökulmia tutkittavasta aiheesta. (Lähdesmäki ym. 2015.)

Tässä opinnäytetyössä hyödynnetään monimenetelmätutkimuksen vaiheittaista selittävää asetelmaa, jossa määrällisen ja laadullisen tutkimuksen osiot toteutetaan peräkkäin kahdessa tai useammassa osassa (Vilkka & Mankki 2024, 75). Tutkimusmenetelmien ajoitus määrittelee, suoritetaanko monime-

netelmätutkimuksen laadullinen ja määrällinen osio samanaikaisesti vai peräkkäin. Ajoitus vaikuttaa siihen, kuinka paljon tutkimuksen eri osat ovat riippuvaisia toisistaan. Osien välisen riippuvuuden ymmärtäminen on keskeistä, sillä yhden osan tulokset voivat ohjata toisen osan toteutusta. Tutkimuksessa käytettyjen menetelmien painotuksessa kyse on siitä, kuinka suuren roolin eri menetelmät saavat tutkimuskysymysten ratkaisussa ja tulosten tulkinnassa. Vaiheittaisissa tutkimuksissa ensimmäinen osio saa tyypillisesti suurimman painoarvon. (Vilkka & Mankki 2024, 58–59.) Tämä opinnäytetyö painottuu laadullisiin menetelmiin, mutta tutkimus sisältää myös määrällisen elementin asiantuntijakyselyn muodossa.

Tämä opinnäytetyö on myös interventionistinen kehittämistutkimus, joka tähtää Elisan tietoturvakäytäntöjen kehittämiseen. Tutkimukset, jotka tähtäävät aikaansaamaan muutosta, tunnetaan interventionisti tutkimuksina. Tällaisia tutkimuksia ovat kehittämistutkimus, konstruktiivinen tutkimus sekä toimintatutkimus. (Kananen 2017, 10.) Kehittämistutkimus ei itsessään ole erillinen tutkimusote, vaan se on yhdistelmä laadullisen ja määrällisen tutkimuksen elementtejä. Kehittämistutkimus voi myös koostua pelkästään laadullisesta tutkimuksesta. (Kananen 2017, 18.) On tärkeää määritellä kehitettävä kohde ja siihen liittyvä ongelma tarkasti, jotta ongelma saadaan poistettua tai minimoitua. Kehittämistutkimuksessa pelkkä ongelman tunnistaminen ei riitä, vaan se vaatii keinoja, jotka johtavat muutokseen. (Kananen 2014a, 36.)

2.1 Tutkimusongelma ja tutkimuskysymykset

Tutkimusongelmien määrittely on usein joustava prosessi, joka voi muovautua tutkimuksen edetessä. Tutkimusongelmilla on keskeinen rooli tutkimuksen suunnan ohjaamisessa, sillä ne auttavat keskittymään olennaiseen ja estävät harhautumisen aiheen kannalta epäolennaisiin asioihin. Selkeästi määritelty tutkimusongelma määrittää, mitä tutkimuksella pyritään selvittämään. (Saaranen-Kauppinen & Puusniekka 2006, 12–13.) Kananen (2014a, 32) kehottaa muotoilemaan tutkimusongelman tutkimuskysymykseksi tai useiksi tutkimuskysymyksiksi, mikä helpottaa vastausten löytämistä aineistosta. Aineiston luonne voi vaihdella, mutta sen tulisi liittyä tutkimusongelmaan ja tukea sen

ratkaisua. Mahdollisia aineistolähteitä ovat muun muassa dokumentit, äänitteet, kuvat, kirjat, muistiinpanot ja tilastot. (Kananen, 2014a, 32.)

Jakkalin (2022) mukaan organisaatioiden on säännöllisesti päivitettävä tietoturvakäytäntöjään vastatakseen jatkuvasti muuttuviin uhkiin. Vertailtaessa vuosien 2013- ja 2022-versioita voidaan todeta, että ISO/IEC 27001:2022 -standardin päivitys tuo mukanaan uusia vaatimuksia ja suosituksia, jotka ovat keskeisiä organisaation tietoturvallisuuden hallintajärjestelmien kehittämisen kannalta. Päivitys korostaa entistä tiiviimmin riskienhallinnan ja tietosuojan integroimisen merkitystä tietoturvallisuuden hallintajärjestelmiin. (ISO/IEC 27001: 2022.) Näin ollen tutkimuksen keskeinen kysymys on, mitä uusia vaatimuksia sekä muutoksia Elisan tulee ottaa huomioon ISO/IEC 27001:2022 -standardin siirtymäprosessissa.

Tutkimuksen keskeiset kysymykset, jotka ohjaavat analyysia ja työskentelyä ovat seuraavat:

1. Mitkä ovat keskeisimmät erot ISO/IEC 27001:2013- ja ISO/IEC 27001:2022 -standardien välillä?
2. Mitä organisaatioiden tulee ottaa huomioon siirtymäprosessissa?
3. Mitä muutoksia organisaatioiden on otettava huomioon toteuttaakseen ISO/IEC 27001:2022 -standardin uudet vaatimukset?

Opinnäytetyöhön valitut tutkimuskysymykset on johdettu tutkimusongelmasta ja liittyvät olennaisesti organisaatioiden ISO/IEC 27001:2022 -standardin siirtymäprosessiin. On siis tärkeää, että organisaatiot ymmärtävät miten ISO/IEC 27001:2013- ja ISO/IEC 27001:2022 -standardit eroavat toisistaan sekä mitä heidän on otettava huomioon siirtymäprosessissa ja uusimman version muutoksissa.

2.2 Aineiston keruu- ja analysointimenetelmät

Tiedon keräämiseen käytettävät menetelmät määritellään sen mukaan, millainen tutkittava kohde on ja millaista näkökulmaa tutkimuksessa hyödynnetään (Saaranen-Kauppinen & Puusniekka 2006, 47). Kun määritellään tutkimukselle sopivia menetelmiä, on ensisijaisesti otettava huomioon tutkittava ongelma. Tämän pohjalta on tärkeää arvioida, minkälaista informaatiota etsitään

ja mitkä menetelmät ovat tehokkaimpia tämän tiedon keräämisessä. (Saaranen-Kauppinen & Puusniekka 2006, 13.) Myös Kananen (2014a, 15) korostaa, että tutkimustoiminta vaatii aina tiedonkeruun, sillä tiedon avulla tutkimusongelma saadaan ratkaistua.

Interventiotutkimuksessa hyödynnetään monilähteistä aineistoa ja sitä voidaan kerätä esimerkiksi haastattelujen, havaintojen tai dokumenttien avulla. Näiden lisäksi interventiotutkimuksessa voidaan hyödyntää etenkin suuremmalle kohderyhmälle kohdistettua määrällisen tutkimuksen kyselyä. Tämän monipuolisen lähestymistavan tavoitteena on saada perusteellinen ymmärrys tutkimusongelmasta ja siihen vaikuttavista tekijöistä. (Kananen 2017, 43.)

Laadulliset ja määrälliset tiedonkeruumenetelmät voidaan jakaa primääri- ja sekundääriaineistoihin. Tässä tutkimuksessa laadullinen tutkimusosio koostuu sekundääriaineistosta, joka käsittää erilaisia dokumentteja, kuten verkkosivuja, kirjoja, tutkimuksia, standardeja, raportteja ja videoita. (Kananen 2014a, 135; 2014b 64.) Valmiit aineistot, kuten muiden tutkijoiden keräämät aineistot, tarjoavat arvokasta näkökulmaa tutkimukseen. Nämä aineistot mahdollistavat aiemmin kerätyn tiedon hyödyntämisen, tuoden esille uusia analyysejä ja perspektiivejä tutkittavaan aiheeseen. (Saaranen-Kauppinen & Puusniekka 2006, 67.) Tässä tutkimuksessa primääriaineisto koostuu kyselystä, joka on Kanasen (2014a, 136) mukaan määrällisen tutkimuksen yksi yleisimmin käytetyistä tiedonkeruumenetelmistä.

Tutkimusosio aloitetaan laadullisella aineistonkeruulla, sillä Kanasen (2017) mukaan määrällistä tutkimusta ei pysty tekemään ilman ilmiön laajempaa tuntemista. Ensimmäisessä vaiheessa kerätään perustietoa uuden ISO/IEC 27001:2022 -standardin vaikutuksista. Tämä antaa laajan ymmärryksen standardin vaikutuksista yleisellä tasolla. Tämän alkuvaiheen tietopohjan perusteella laaditaan kysely, joka suunnataan Elisan tietoturva-asiantuntijoille. Kyselyn tavoitteena on selvittää, mitkä standardin uudistukset ovat asiantuntijoiden mielestä tärkeimpiä. Saadut vastaukset analysoidaan määrällisesti ja analyysin tulokset sisällytetään opinnäytetyöhön. Nämä tulokset toimivat pohjana seuraavalle laadulliselle aineistonkeruuvaiheelle, jossa syvennytään asiantuntijoiden keskeisiin vastauksiin.

Aineiston käsittelyyn käytettäviä menetelmiä nimitetään analyysimenetelmiksi. Analyysimenetelmien käytölle on olemassa tarkat tieteelliset ohjeistukset. Lisäksi analyysimenetelmät ovat tiiviisti yhteydessä käytettyihin tiedonkeruumenetelmiin. (Kananen 2014a, 32.) Aineiston perusteellinen analyysi on välttämätöntä tutkimuskysymysten ratkaisemiseksi, mikä edellyttää aineiston aktiivista käsittelyä ja syvällistä pohdintaa, kuten Saaranen-Kauppinen & Puusniekka (2006, 75) kuvaavat. He korostavat, että aineistosta ei suoraan löydy valmiita vastauksia, vaan tutkijan on tulkittava aineistoa löytääkseen uusia näkökulmia tutkimusongelmiinsa.

Laadullisessa tutkimuksessa keskitytään tekstiaineistojen analysointiin esimerkiksi sisältöanalyysin avulla (Kananen 2014b, 42). Vuoren (2021) mukaan sisällönanalyysi soveltuu monenlaisten aineistojen, kuten tekstien, haastatteluiden, puheen sekä videoiden analysoimiseen. Saaranen-Kauppinen & Puusniekka (2006) kuvailevat, että sisällönanalyysin toteutus voi perustua aineistolähtöisyyteen, teoriaohjaukseen tai teorialähtöisyyteen. Tässä tutkimuksessa hyödynnetään aineistolähtöistä sisällönanalyysiä. Aineistolähtöisessä sisällönanalyysissä keskitytään ensisijaisesti itse aineistoon, mikä mahdollistaa teorian muodostumisen tutkimusaineiston pohjalta. Tässä lähestymistavassa analyysin lähtökohta on aineisto itsessään ilman ennalta asetettuja olettamuksia. (Saaranen-Kauppinen & Puusniekka 2006, 15.) Aineistolähtöinen sisällönanalyysi sopii hyvin opinnäytetyön aiheeseen, sillä se mahdollistaa tutkimusaineiston monipuolisen ja ennakkoluulottoman tarkastelun. Tämä voi auttaa löytämään uusia näkökulmia aiheeseen liittyen. ISO/IEC 27001:2013- ja ISO/IEC 27001:2022 -versioiden vertailu on myös keskeisessä osassa tutkimuksen tuloksia. Näiden menetelmien avulla pyritään saamaan syvällinen ymmärrys siitä, miten Elisa voi vastata ISO/IEC 27001:2022 -standardin vaatimuksiin. Myös teoreettinen viitekehys on välttämätöntä laadullisen tutkimuksen suorittamiselle, sillä se tarjoaa tutkimukselle suunnan ja merkityksen (Juhila s.a.). Teoreettinen viitekehys rakentuu aiemmista tutkimuksista, teorioista ja käsitteistä, jotka auttavat hahmottamaan tutkimuksen taustaa.

Seuraava kappale perustuu Vilkan (2021) ajatuksiin. Kyselylomakkeet ovat yleisin tapa kerätä tietoa määrällisissä tutkimuksissa. Kyselyä kutsutaan myös

survey-tutkimukseksi, jossa kaikille vastaajille esitetään samat kysymykset samalla tavalla. Tutkimusaiheen teoreettinen tausta ja aikaisemmat tutkimukset ovat olennaisia kyselyn suunnitteluvaiheessa. Kyselylomakkeen suunnittelu edellyttää myös selkeää ymmärrystä tutkimuksen tavoitteista. Kyselylomakkeessa voi olla monivalinta-, avoimia tai sekamuotoisia kysymyksiä. Tutkimusaineiston järjestäminen havaintomatriisiin eli taulukkomuotoon, mahdollistaa muuttujiin liittyvien väitteiden perustelemisen numeroiden ja tilastollisten suhteiden avulla. Havaintomatriisi rakennetaan siten, että pystysarakkeeseen sijoitetaan asiasisältöä kuvaavat muuttujat ja vaakariveille tallennetaan tutkittavien kyselylomakkeista saadut tiedot. Havaintomatriisi on tutkimuksessa keskeinen, sillä se mahdollistaa erilaisten keskilukujen laskemisen ja tulosten analysoinnin.

Kyselyssä käytetään monivalinta-, avoimia sekä sekamuotoisia kysymyksiä. Näiden avulla kerätään monipuolista ja kattavaa aineistoa, mikä edistää hyödyllisten tutkimustulosten saavuttamista. Kyselyn toimivuutta testataan ennen sen suorittamista, mikä on Vilkan (2021, 107) mukaan tärkeää. Kyselyn vastaukset järjestetään havaintomatriisiin, joka mahdollistaa suurten tietomäärien tehokkaan käsittelyn ja havainnollistamisen. Frekvenssianalyysi on keskeinen osa vastausten analysointia, sillä se auttaa selvittämään, kuinka usein tietyt näkemykset toistuvat aineistossa. Kyselyn vastaukset visualisoidaan myös erilaisten diagrammien avulla. Kyselyn määrällinen analyysi pidetään tarkoituksella melko yksinkertaisena, koska sen päätavoite on tunnistaa ISO/IEC 27001:2022 -standardin keskeiset muutokset asiantuntijoiden näkökulmasta. Mikäli kyselyn vastausprosentti jää alhaiseksi, hyödynnetään tulosten analysoinnissa myös laadullista sisällönanalysointia.

Tutkimuksen luotettavuutta varmistetaan käyttämällä laajaa ja monipuolista sekundääriaineistoa. Lisäksi kaikki käytetyt lähteet dokumentoidaan huolellisesti ja viitataan niihin asianmukaisesti. Validiteetti varmistetaan vertailemalla primääriaineistona kerättyjen kyselytutkimuksen tuloksia sekundääriaineistoon. Tämän vertailun kautta varmistetaan, että tutkimuksen tulokset ovat yhdenmukaisia olemassa olevan tiedon kanssa. Lisäksi validiteetti varmistetaan yhteistyössä opinnäytetyön toimeksiantajan kanssa. Toimeksiantaja osallistuu

tutkimuksen tulosten tarkasteluun ja arviointiin, mikä auttaa varmistamaan tulosten oleellisuuden ja käyttökelpoisuuden heidän ISO/IEC 27001:2022 -standardin siirtymäprosessissaan.

3 TIETOTURVALLISUUDEN PERUSTEET

Päivärinta (2020) toteaa, että tietoturvallisuus on nykyaikaisen tietotekniikan keskeinen osa, suojaten tietoa ja tietojärjestelmiä luvattomalta käytöltä, muutoksilta tai paljastumiselta. ISO/IEC 27000 -standardin (2020) mukaan tietoturvallisuus viittaa siihen, että tieto on arvokasta omaisuutta, joka vaatii tehokasta suojelua. Organisaatioille arvokasta tietoa ovat muun muassa digitaaliset tiedostot ja data, paperidokumentit sekä fyysinen media (What is information security? s.a.).

Kansainvälisen standardointijärjestö ISO:n mukaan tietoturva perustuu kolmeen keskeiseen pilariin: luottamuksellisuuteen, eheyteen sekä saatavuuteen. Tämä tunnetaan myös nimellä CIA-kolmikko. (Päivärinta, 2020, 11.) Nykyaikaisessa tietotekniikan maailmassa CIA-kolmikkoa on laajennettu muilla periaatteilla, kuten Donn Parkerin kuusikolla sekä CIA-AAA-mallilla. Nämä lisäävät ulottuvuutta ja syventävät käsitystä tietoturvan monimutkaisuudesta. (Päivärinta, 2020, 12–13.)

Tämä teoreettinen viitekehys tarjoaa perustan tietoturvan perusperiaatteiden ymmärtämiselle ja niiden merkitykselle informaation suojaamisessa. Se luo pohjan sille, miten ISO/IEC 27001 -standardi tukee organisaatioita näiden tavoitteiden saavuttamisessa, tarjoten suuntaviivoja riskienhallintaan ja tietoturvapolitiikkojen kehittämiseen.

3.1 CIA-kolmikko ja CIA-AAA-malli

CIA-kolmikko ohjaa organisaatioita valitsemaan sopivat teknologiat, politiikat ja käytännöt tietojärjestelmiensä suojaamiseksi (What is information security? s.a.). Se on tietoturvan perusta ja koostuu kolmesta pääelementistä: luottamuksellisuudesta, eheydestä ja saatavuudesta. Luottamuksellisuus tarkoittaa, että vain valtuutetut käyttäjät pääsevät käsiksi tietoihin. Organisaatiot suojaa-

vat tietojaan luvattomalta pääsyltä käyttämällä muun muassa salauksia ja salasanoja. (Päivärinta 2020, 11.) Eheys varmistaa, että tiedon alkuperäisyys säilyy muuttumattomana siirron aikana ja mahdollistaa sen aitouden todentamisen. Tähän käytetään keinoja, kuten käyttöoikeuksien hallintaa ja versionhallintaa, jotka estävät virheellisiä muutoksia ja auttavat tunnistamaan mahdolliset tietojen muutokset. Saatavuus puolestaan takaa, että tieto on tarvittaessa saatavilla ja käytettävissä. Organisaatiot ylläpitävät aktiivisesti laitteistoaan, pitävät ohjelmistot ja järjestelmät ajan tasalla sekä toteuttavat ennaltaehkäiseviä toimenpiteitä, kuten vikasietoisuutta ja redundanssia varmistaakseen tämän. (Hashemi-Pour & Chai 2023.) ISO/IEC 27001 -standardin mukainen tietoturvallisuuden hallintajärjestelmä auttaa yrityksiä hallitsemaan riskejä ja varmistamaan tiedon luottamuksellisuuden, eheyden ja saatavuuden (Mäki-Maukola 2023, 19–20).

CIA-kolmikkoa voidaan laajentaa CIA-AAA-mallilla, joka tuo lisäulottuvuuden tietoturvallisuuden hallintaan (Päivärinta 2020, 13.). Malli sisältää autentikoinnin (authentication), valtuutuksen (authorization) ja kirjanpidon (accounting), jotka muodostavat tietoturvakehyksen. Tämä kehys esimerkiksi säätelee pääsyä tietokoneiden resursseihin, ylläpitää käytäntöjä ja valvoo käyttöä. Se on keskeinen osa verkkojen hallintaa ja kyberturvallisuutta, sillä se auttaa varmistamaan käyttäjien henkilöllisyydet ja seuraamaan heidän toimintaansa verkossa. Autentikoinnin avulla käyttäjät todistavat henkilöllisyytensä esittämällä kirjautumistiedon, kuten salasanat, USB-avaimet tai biometriset tunnisteet, jotka vahvistetaan tietokannassa olevia tietoja vasten. (Fortinet s.a.)

Valtuutuksen aikana käyttäjille voidaan myöntää oikeuksia päästä tiettyihin järjestelmän tai verkon osiin. Valtuuttaminen määrittelee, mitä käyttäjä saa tehdä järjestelmässä. Järjestelmänvalvoja voi muokata käyttäjän oikeuksia, jolla sallitaan käyttäjälle oikeudet päästä alueelle, jotta käyttäjälle sallitaan pääsy aiemmin estetyille alueille. (Fortinet s.a.)

Kirjanpito seuraa käyttäjän toimintaa verkossa. Se kirjaa muun muassa, kuinka kauan käyttäjä on ollut kirjautuneena sekä kerää tietoja lähettämistä ja vastaanottamista tiedoista ja IP-osoitteesta. Kirjanpitoa käytetään käyttäjätoiminnan tarkastamiseen. käyttäjän toimintaa hänen ollessaan kirjautuneena

verkkoon. Se tallentaa tietoja, kuten kuinka kauan käyttäjä on ollut kirjautuneena sekä kerää käyttäjän lähettämät tai vastaanottamat tiedot ja IP-osoitteensa. Kirjanpitoa voidaan käyttää esimerkiksi käyttäjätoiminnan tarkastamiseen. (Fortinet s.a.)

3.2 Parkerin kuusikko

Parkerin kuusikko on kehitetty CIA-mallin jatkokehityksenä vastaamaan nykyaikaisen tietoturvan haasteisiin, joita perinteinen CIA-kolmikko ei ole kyennyt ratkaisemaan. Se syventää tietoturvan käsitystä lisäämällä kolme uutta ulottuvuutta, jotka ovat kriittisiä nykyaikaisille tietoverkoille ja niiden monimutkaisille uhkille. Nämä ulottuvuudet ovat hallinta, aitous sekä hyödyllisyys. (Pender-Bey s.a.)

Hallinta keskittyy tiedon fyysiseen kontrollointiin ja omistusoikeuteen, korostaen fyysisen tiedon suojauksen tärkeyttä. Aitous puolestaan korostaa tiedon alkuperän varmentamista ja varmistaa, että tiedon alkuperä on selvästi jäljitettävissä sen lähteeseen. Hyödyllisyys keskittyy tiedon merkitykseen käyttäjille ja painottaa tiedon olennaisuutta toiminnan kannalta. (Päivärinta 2020, 12.) Pender-Beyn (s.a.) mukaan nämä lisäykset tarjoavat kattavamman mallin tietojen turvaamiseen.

Parkerin kuusikon integrointi osaksi organisaation tietoturvakäytäntöjä voi parantaa valmiuksia noudattaa ISO/IEC 27001:2022 -standardia, joka edellyttää kokonaisvaltaista lähestymistapaa tietoturvan hallintaan. Malli tukee organisaatioita tunnistamaan ja hallitsemaan tietoturvan näkökulmasta kriittisiä tekijöitä, jotka voivat vaikuttaa tietojärjestelmien turvallisuuteen.

4 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ

Tietoturvallisuuden hallintajärjestelmä (ISMS) on keskeinen tekijä ISO/IEC 27000 -standardiperheen ymmärtämisessä ja yrityksen tietoturvan tehokkaassa hallinnassa. ISMS:n käyttöönotto on välttämätöntä yrityksen tietoturvatavoitteiden saavuttamiseksi, tarjoten kattavan rakenteen tietoturvakäytäntöjen, menettelyjen, prosessien, ja organisaation rakenteiden kehittämiseen ja

ylläpitoon. Tämä mahdollistaa yrityksille mukautuvan ja koordinoidun lähestymistavan tietoturvariskien hallintaan, varmistaen tietojen ja niihin liittyvän omaisuuden suojauksen erilaisilta uhilta. (Mäki-Maukola 2023, 22–23.) ISO/IEC 27000:2020 -standardin (2020) mukaan tietoturvallisuuden hallintajärjestelmä lisää mahdollisuuksia siihen, että organisaatiot voivat johdonmukaisesti saavuttaa tärkeät menestystekijät, jotka liittyvät niiden omaisuuserien suojelemiseen.

ISO/IEC 27001 -standardi edustaa tietoturvallisuuden hallintajärjestelmän mallia, joka keskittyy kokonaisvaltaisen valvontajärjestelmän luomiseen. Se korostaa jatkuvaa tarvetta määritellä, toteuttaa, seurata, tarkistaa, ylläpitää ja parantaa tietoturvatoimenpiteitä, jotta voidaan vastata muuttuviin turvallisuus- ja liiketoimintavaatimuksiin. (Calder & Gerrard 2013.) Calder ja Gerrardin (2013) mukaan, tietoturvallisuuden hallintajärjestelmän kehittäminen vaatii yrityksen johdon sitoutumista ja riittävää tukea turvallisuuskulttuurin vahvistamiseksi organisaatiossa.

PDCA-malli (Plan-Do-Check-Act) esittelee jatkuvan parannusprosessin, joka on olennainen osa ISMS:n toteuttamisessa, mahdollistaen yritykselle jatkuvan tietoturvan kehityksen ja sopeutumisen uusiin uhkiin. Riskienarviointi ja -hallinta ovat tässä prosessissa avainasemassa, kuten myös tietoturvatietoisuuden lisääminen henkilöstön keskuudessa ja tehokkaan kommunikoinnin varmistaminen tietoturvakäytäntöjen noudattamiseksi. (Mäki-Maukola 2023, 22–23.) Kappaleen loppuosa pohjautuu Crawleyn (2022) ajatuksiin. PDCA-malli koostuu suunnittelusta (plan), toteutuksesta (do), tarkastamisesta (check) ja toiminnasta (act). Suunnitteluvaiheeseen kuuluu ISMS:n tavoitteiden, politiikan, menettelyjen ja prosessien luominen riskienhallintaan sekä tiedon turvallisuuden parantaminen organisaation tietoturvatavoitteiden saavuttamiseksi. Toteutusvaiheessa nämä suunnitelmat pannaan käytäntöön. Tarkastusvaihe pitää sisällään ISMS:n arvioinnin ja seurannan. Tässä vaiheessa prosessien suorituskykyä mitataan ja arvioidaan verrattuna ISMS-politiikkaan, käytännön kokemuksiin ja tavoitteisiin. Toimintavaiheessa tehdään tarvittavat korjaukset ja parannukset perustuen tarkastusvaiheen tuloksiin ja suoritetaan ennaltaehkäiseviä toimenpiteitä ISMS:n sisäisten auditointien pohjalta. Tämä vaihe kehittää myös organisaation reagointivalmiutta tapahtumiin.

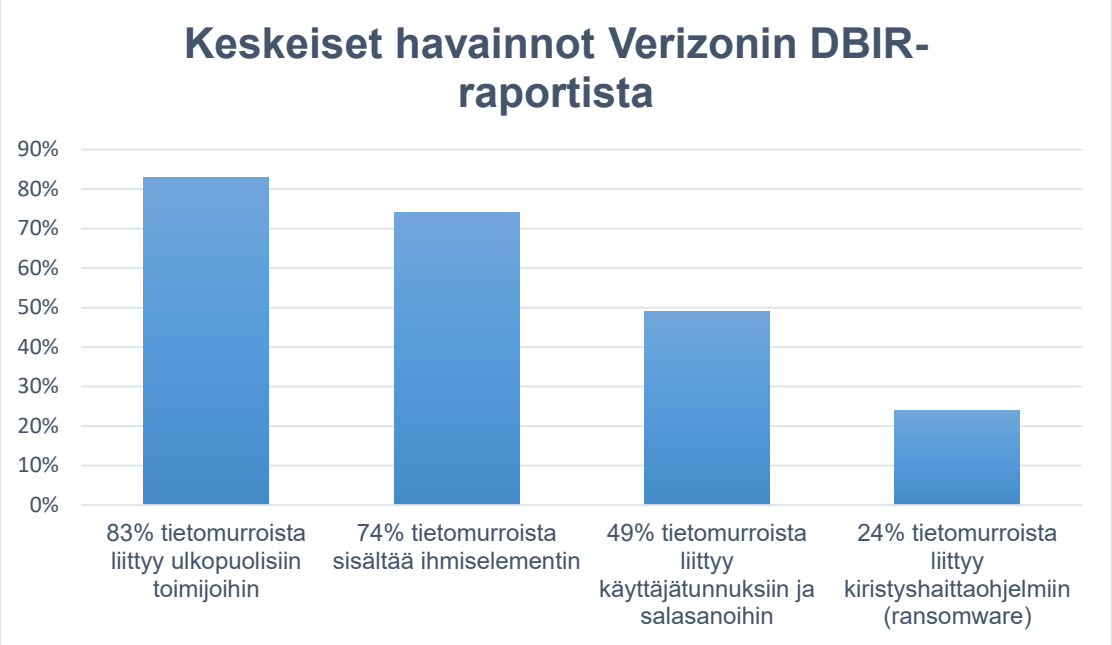
5 RISKIENHALLINTA JA KYBERUHAT

Riskienhallinta on koordinoitua toimintaa, jonka tavoitteena on hallita ja ohjata organisaation kohtaamia riskejä. Tässä yhteydessä riski tarkoittaa epävarmuuden vaikutusta organisaation tavoitteisiin, joka voi olla myönteinen, kielteinen tai molempia. (ISO 31000: 2018, 6–7.) Riskienhallintaprosessi on jatkuvaa toimintaa, missä organisaation riskienhallinnan strategioita ja toimenpiteitä säännöllisesti tarkastellaan ja mukautetaan, jotta ne pysyvät linjassa sen kehittyvien tavoitteiden ja ympäristöolosuhteiden kanssa (ISO 31000: 2018, 33). Riskienhallinnan merkitys on keskeinen, sillä ennalta arvaamaton tapahtuma voi yllättää organisaation aiheuttaen lievistä katastrofaalisiin seurauksiin. Riskien vähentämiseksi organisaation on käytettävä resursseja negatiivisten tapahtumien vaikutusten minimoimiseen, valvomiseen ja hallintaan. Jatkuva ja systemaattinen lähestymistapa riskienhallintaan auttaa määrittämään parhaat keinot tunnistaa, hallita ja lieventää merkittäviä riskejä. (What is risk management? s.a.) Riskienhallintaprosessi sisältää useita vaiheita, joista keskeisimpiä ovat riskien tunnistaminen, riskianalyysi ja -arviointi sekä riskien lieventäminen ja seuranta.

Yksinkertaisimmillaan kyberuhka viittaa tilanteeseen, jossa hakkeri tai muu pahantahtoinen toimija pyrkii pääsemään ilman lupaa verkkoon tehdäkseen kyberhyökkäyksen (Badman 2023). Kyberuhka pitää sisällään erilaisia tapahtumia, jotka voivat vahingoittaa organisaatioiden omaisuutta, toimintaa tai ihmisiä tietojärjestelmän kautta. Kyseiset tilanteet voivat tapahtua esimerkiksi, kun pahatahtoinen toimija pääsee luvattomasti käsiksi tietoihin, tuhoaa tai muuttaa niitä. (NIST s.a.)

Tilastot tietomurroista ja tietoturvaloukkauksista korostavat riskienhallinnan merkitystä. Crawleyn (2022, 45) mukaan Verizonin tietomurtojen tutkimusraportti (DBIR) on erityisen hyödyllinen yrityksille. Verizonin (2023) raportti tarjoaa arvokasta tietoa yleisten hyökkäysmenetelmistä ja auttaa organisaatioita tunnistamaan haavoittuvuuksia. Raportissa tietoturvaloukkaus määritellään tapahtumaksi, joka vaarantaa tiedon luotettavuutta, saatavuutta ja eheyttä. Tie-

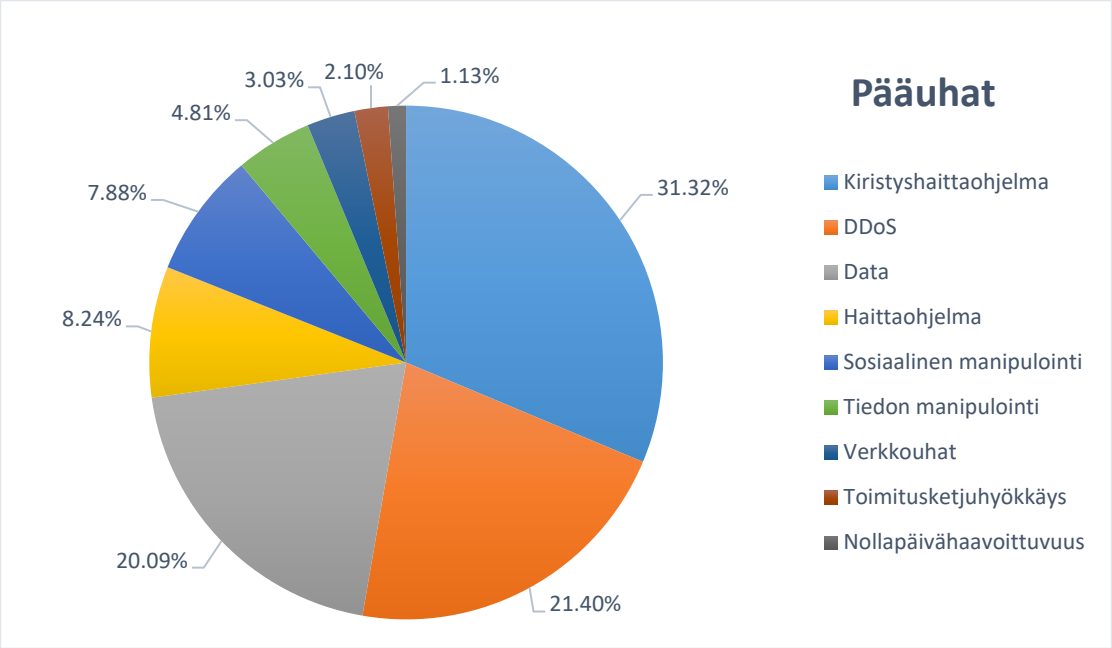
tomurrolla taas tarkoitetaan tilannetta, jossa tietoa siirretään luvatta ulkopuoliselle taholle. Seuraava kaavio havainnollistaa Verizonin tärkeimmät havainnot tietomurroista.



Kuva 1. Keskeisimmät havainnot tietomurroista (Verizon 2023)

Verizonin (2023) raportti korostaa myös, että 74 % kaikista tietomurroista sisältää inhimillisen elementin. Ihmiset ovat mukana joko virheiden, oikeuksien väärinkäytön, varastettujen tunnusten käytön tai sosiaalisen manipuloinnin kautta. Tästä voidaan päätellä, että työntekijöiden koulutuksen, perehdytyksen ja tietoturvallisuuden kulttuurin vahvistaminen voivat olla keskeisiä tekijöitä tietoturvauhkien hallinnassa.

ENISA:n uhkamaisemaraportti (2023) tarjoaa erittäin syvällisen katsauksen ajankohtaisiin kyberturvallisuusuhkiin. Seuraavasta kaaviosta ilmenee, mitkä ovat ENISA:n (2023, 6–9) raportin mukaan merkittävimmät kyberuhat organisaatioille ajalta 7.2022–6.2023.



Kuva 2. Analysoitujen tapahtumien jakautuminen uhkatyypeittäin (ENISA 2023)

ENISA:n (2023) raportti jakaa kyberuhat kahdeksaan pääkategoriaan, jotka edustavat erityyppisten uhkien yhdistelmiä. Kuvassa 2 on havainnollistettu, että kiristyshaittaohjelmat ja palvelunestohyökkäykset ovat ENISA:n (2023) raportin kaksi yleisintä hyökkäystyyppiä. Raportissa myös mainitaan, että monet hyökkäystyypit sisälsivät useampaa kuin yhtä uhkaluokkaa.

Tämän kappale perustuu IBM:n (2023) raporttiin. IBM:n vuoden 2023 raportti tarjoaa syvällistä tietoa kyberturvallisuusuhkista. Raportissa tarkastellaan, miten organisaatiot priorisoivat riskejä ja haavoittuvuuksia sekä selvitetään, millaisia vaikutuksia näillä on tietomurtojen kustannuksiin. Raportin mukaan organisaatiot, jotka käyttävät ennakoivampaa ja riskiperusteista haavoittuvuuksien hallintaa, kokevat keskimääräistä pienempiä tietomurron kustannuksia verrattuna organisaatioihin, jotka nojautuvat pelkästään alan standardeihin, kuten CVE- ja CVSS-luokituksiin. Haavoittuvuushallinnan menetelmiä ovat esimerkiksi penetraatiotestaus, haavoittuvuustestaukset ja red team testing. Ennakoivassa riskienhallinnassa IT-turvatiimit omaksuvat potentiaalisen hyökkääjän näkökulman, arvioidakseen mitkä haavoittuvuudet ovat hyväksikäytettävissä ja voivat aiheuttaa vahinkoa.

6 ISO/IEC 27000 -STANDARDISARJA

ISO/IEC 27000 -standardisarja tarjoaa kattavat ohjeistukset ja parhaita käytäntöjä organisaatioiden tietoturvan hallintaan (Mäki-Maukola 2023, 29). Tämän standardisarjan keskiössä on ISO/IEC 27001 -standardi, joka määrittelee vaatimukset tietoturvallisuuden hallintajärjestelmälle ja tarjoaa perustan organisaatioiden tietoturvakäytäntöjen kehittämiseen ja ylläpitämiseen (ISO/IEC 27001: 2022). Sen rinnalla ISO/IEC 27002 -standardi tarjoaa kattavan ohjeistuksen ISO/IEC 27001 -standardin hallintakeinojen käytännön toteutukseen, tarjoten erilaisia ohjeita ja erityisiä täytäntöönpanoneuvoja hallintakeinoille. Standardi antaa yksityiskohtaisia suosituksia hallintakeinojen käyttöönotosta, tukee parhaita käytäntöjä ja tarjoaa ohjausta standardoinnin määrittelyyn. (Mäki-Maukola 2023, 33.)

6.1 ISO/IEC 27001 -standardi

ISO/IEC 27001 -standardi on kansainvälisesti tunnettu viitekehys organisaatioiden tietoturvallisuuden hallintajärjestelmille (ISO 31000 – Risk management s.a.). Kyseinen standardi sisältää joukon vaatimuksia, jotka on suunniteltu auttamaan organisaatioita suojelemaan herkkää tietoa, lisäämään sidosryhmien luottamusta ja noudattamaan lakien ja säännösten vaatimuksia (Mäki-Maukola 2023, 31–32).

ISO/IEC 27001 -standardi julkaistiin ensimmäisen kerran vuonna 2005, ja se perustui aiemmin julkaisemattomaan BS 7799-2- standardiin (The History of ISO 27001 s.a.). Vuoden 2013-versio toi mukanaan merkittäviä päivityksiä, mukaan lukien joustavamman riskienhallintaprosessin ja laajemman soveltamisalan. Tämä versio korosti myös johtajuuden roolia informaation turvallisuuden hallintajärjestelmän tehokkuudessa, mikä osoitti selkeän siirtymisen pelkästään teknisestä lähestymistavasta kohti kokonaisvaltaista hallintaa. (IT Governance Ltd 2013.)

ISO/IEC 27001 -standardin noudattaminen auttaa organisaatioita suojelemaan arkaluonteisia tietojaan sekä rakentamaan luottamusta asiakkaiden ja sidosryhmien keskuudessa. Standardin vaatimusten täyttäminen osoittaa organisaation sitoutumista korkeimpiin tietoturvan standardeihin. Lisäksi vuoden

2022-version mukainen päivitys tarjoaa organisaatioille mahdollisuuden parantaa jatkuvasti turvallisuuskäytäntöjään vastaamaan uusia haasteita ja teknologian kehitystä. (Why is ISO 27001 Important? s.a.)

Yhteenvetona voidaan todeta, että ISO/IEC 27001 -standardi on keskeinen väline nykyaikaisen organisaation tietoturvakäytännöissä. Sen kehittyminen vuoden 2013-versiosta 2022-versioon heijastaa sitoutumista pysymään ajantasaisena teknologian ja kyberturvallisuuden jatkuvasti muuttuvassa maailmassa.

6.2 ISO/IEC 27005-, ISO/IEC 27017-, ISO/IEC 27018 -standardit

ISO/IEC 27005 -standardi puolestaan keskittyy riskienhallintaan, tarjoten yksityiskohtaisen viitekehyksen riskien arvioinnille ja hallinnalle osana tietoturvallisuuden hallintajärjestelmän käyttöönottoa ja ylläpitoa. Tämä standardi opastaa, miten riskienhallintaprosessi voidaan suunnitella, toteuttaa, ylläpitää ja parantaa jatkuvasti, soveltaen ISO/IEC 27001 -standardin mukaisia periaatteita ja vaatimuksia. (ISO/IEC 27005: 2022.)

Näiden lisäksi ISO/IEC 27017- ja ISO/IEC 27018 -standardit ovat keskeisiä ISO/IEC 27000 -standardisarjassa, jotka täydentävät ISO/IEC 27001:2022 -standardin vaatimuksia erityisesti pilvipalveluiden turvallisuuden ja henkilötietojen suojauksen osalta. ISO/IEC 27017 -standardi keskittyy pilvipalveluiden tietoturvakontrolleihin, tarjoten sekä pilvipalveluntarjoajille että pilvipalveluiden käyttäjille ohjeistusta tietoturvariskien hallintaan (ISO/IEC 27017: 2021, 5). Tämä standardi antaa lisäohjeita ISO/IEC 27002 -standardissa määriteltyjen tietoturvatoimenpiteiden toteuttamiselle ja sisältää erityisiä ohjeita pilvipalveluihin liittyen, kuten tietojen käsittelyn, tietoturvakontrollien sekä käyttäjien ja pilvipalveluntarjoajien välisen yhteistyön suhteen (ISO/IEC 27017: 2021, 9–35).

ISO/IEC 27018 -standardi on suunnattu henkilötietojen suojaamiseen julkisissa pilvipalveluissa, ohjaten pilvipalveluntarjoajia käsittelemään henkilötietoja kansainvälisten yksityisuudensuojan normien mukaisesti (ISO/IEC 27018: 2020). Lisäksi ISO/IEC 27018:2020 -versio korostaa läpinäkyvyyden, tietojen

käsittelyn rajoitusten, ja käyttäjän tietosuojaoikeuksien tärkeyttä. Standardi tarjoaa konkreettisia hallintakeinoja, jotka auttavat pilvipalveluntarjoajia noudattamaan yksityisyydensuojan parhaita käytäntöjä. (ISO/IEC 27018: 2020, Liite A.)

7 ISO/IEC 27001:2022 -STANDARDIN MUUTOKSET

ISO/IEC 27001:2022 -standardi, kuten myös ISO/IEC 27001:2023 -standardi koostuu johdannosta, vaatimuksista sekä Liite A:sta. Johdannossa esitellään standardin perustiedot ja sen tarkoitus. Vaatimukset-osio määrittelee ne konkreettiset perusteet, joiden mukaisesti organisaatiot rakentavat, ylläpitävät ja kehittävät tietoturvallisuuden hallintajärjestelmiään. Osiossa kuvataan tarkasti, mitkä prosessit ja elementit ovat välttämättömiä standardin mukaisten hallintajärjestelmien toteuttamiseksi. (ISO/IEC 27001: 2022.)

Tarkastelun perusteella, Liite A on yksi standardin keskeisimmistä osista ja se tarjoaa yksityiskohtaisen luettelon tietoturvan hallintakeinoista eli kontrolleista. Nämä hallintakeinot ovat suunniteltu auttamaan organisaatioita hallitsemaan tietoturvallisuuteen liittyviä riskejä (ISO 27001 Controls Explained: A Guide to Annex A s.a.). Kunkin hallintakeinon tavoitteena on tarjota selkeät ohjeet tietoturvakäytäntöihin liittyen, kuten miten pääsyä tietoihin valvotaan tai minkälaisia toimintatapoja noudatetaan tietojen suojaamiseksi (ISO/IEC 27001:2022). Kaikkien hallintakeinojen noudattaminen ei ole kuitenkaan pakollista. Organisaatioiden on arvioitava, kuinka olennainen kunkin hallintakeinon soveltaminen on omaan toimintaansa nähden ja perusteltava, miksi tietyt hallintakeinot mahdollisesti jätetään toteuttamatta. Tärkeää on, että kaikki valitut hallintakeinot linkittyvät suoraan organisaation riskienhallintastrategiaan. (ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide s.a.) Nykäsen (2022) mukaan aiemmin ISO/IEC 27001 -standardissa on ollut ongelmana tapa, jossa osa organisaatioista saattaa toteuttaa kaikki hallintakeinot, vaikka ne eivät ole organisaation kannalta tarpeellisia. Hän suosittelee, että organisaatiot noudattaisivat riskilähtöistä lähestymistapaa, jossa valitaan juuri ne hallintakeinot, jotka ovat tehokkaimpia kunkin organisaation erityistarpeisiin. Hänen mukaansa tavoitteena on valita hallintakeinot siten, että niistä saadaan paras mahdollinen hyöty.

7.1 Vaatimusten muutokset

Vertailemalla standardeja keskenään huomataan, että standardin kohdat 4–10 ovat pysyneet hyvin samankaltaisina ja suurin osa muutoksista on pieniä. Organisaatioiden tulee kuitenkin kiinnittää huomiota myös pienempiin muutoksiin, sillä tietoturvallisuuden hallintajärjestelmän on heijastettava uutta hallintastandardia (Calder, 2023). Alan asiantuntijoiden mukaan merkittävimmät erot ISO/IEC 27001:2022 -standardin vaatimuksissa ilmenevät erityisesti kohdissa 4.2, 6.2, 6.3, 8.1 ja 9.3.2 (Kosutic 2022; Saali 2023; PECB 2024). Vertailemalla ISO/IEC 27001:2013- ja ISO/IEC 27001:2022 -standardeja keskenään huomataan, että uusimman standardin vaatimuksista löytyy useampi merkittävä muutos:

Taulukko 1. Merkittävimmät muutokset ISO/IEC 27001:2022 -standardin vaatimuksissa (ISO/IEC 27001: 2022)

Kohta	Uusi vaatimus
4.2	• Sidosryhmien vaatimusten systemaattinen käsittely ISMS:n kautta.
4.4	• Prosessien ja niiden vuorovaikutusten yksityiskohtainen kuvaus.
6.2	• Tietoturvatavoitteiden jatkuva seuranta ja niiden dokumentointi.
6.3	• ISMS:n muutosten suunnitelmallinen toteutus.
7.4	• Viestintäprosessien toteutustavan määrittely.
8.1	• Prosessien kriteerien määrittely ja ulkopuolisten resurssien hallinta.
9.1	• Tietoturvan tehokkuuden arviointimenetelmien vertailukelpoisuus ja toistettavuus.
9.3.2	• Johdon katselmuksessa keskeisten sidosryhmien tarpeiden ja odotusten huomioiminen.

Vaatimuksen 4.2 mukaan organisaatioiden on määriteltävä ISMS:n kannalta keskeiset sidosryhmät, tunnistettava näiden sidosryhmien olennaiset vaatimukset ja osoitettava, miten ISMS vastaa näihin vaatimuksiin (ISO/IEC 27001: 2022, 7). Voidaan siis päätellä, että tämä vaatimus korostaa tarvetta systemaattiselle lähestymistavalle sidosryhmien hallinnassa. Myös Saali (2023) korostaa, että organisaatioiden on osoitettava, miten tietoturvatyö ohjataan sidosryhmien ja palveluiden näkökulmasta vastaamaan näiden tarpeita. Hänen

mukaansa vuoden 2013-versiossa vaadittiin sidosryhmien tunnistamista ja heidän toiveiden sekä vaatimustensa ymmärtämistä, mutta yhteys tietoturvallisuustyöhön ja tietoturvallisuuden hallintajärjestelmään ei ollut yhtä selkeä. Hän myös mainitsee, että uusi lisäys parantaa tapaa, jolla tietoturvallisuustyö tukee kumppanihallintaa ja integroituu organisaation sidosryhmille tarjoamiin prosesseihin ja palveluihin. Näin ollen nämä muutokset voivat muun muassa parantaa luottamusta sidosryhmien keskuudessa.

Lisäksi vaatimus 4.4 vaatii organisaatioita kuvaamaan selkeästi tietoturvallisuuden hallintajärjestelmässään tarvittavat prosessit ja niiden väliset vuorovaikutukset (ISO/IEC 27001: 2022, 8). Calder (2023) korostaa erityisesti pilviympäristöjen merkitystä, jossa organisaatiot ulkoistavat merkittäviä osia liiketoiminnastaan. On siis selvää, että tämä korostaa tarvetta ymmärtää, miten eri prosessit toimivat organisaation sisällä sekä sen ulkopuolella.

ISO/IEC 27001:2022 -standardi sisältää uuden vaatimuksen 6.2, jonka mukaan tietoturvatavoitteita on seurattava ja ne tulee olla saatavilla dokumentoituna tietona (ISO/IEC 27001: 2022, 11). Calder (2023) korostaa, että organisaatioiden on pohdittava, miten nämä heijastuvat niiden politiikkaan ja liiketoimintatavoitteisiin. Armstrong (2023) lisää, että tämän seurauksena tietoturvatavoitteiden tarkastukset on suoritettava useammin, sillä perinteinen vuosittainen tarkastus ei enää riitä.

Standardeja vertailtaessa huomataan, että ISO/IEC 27001:2022 -standardiin on lisätty kohta 6.3, joka käsittelee ISMS:n muutosten suunnittelua. ISO/IEC 27001:2022 -standardin (2022) mukaan, kun organisaatio havaitsee muutostarpeita tietoturvallisuuden hallintajärjestelmässään, sen tulee toteuttaa nämä muutokset suunnitelmallisesti. Saalin (2023) pitää uutta vaatimusta erinomaisena lisäyksenä, sillä se selkeyttää muutostarpeiden tunnistamista, niiden systemaattista suunnittelua, toteutusta sekä seurantaa. Hän korostaa, että muutosten suunnittelussa tulee myös käsitellä muutosten koulutusta henkilöstölle ja varmistaa, että muutos on ollut tarkoituksenmukainen ja riittävän vaikutta organisaation hallintajärjestelmään. Barkerin (s.a.) mukaan organisaatioilla tulee olla dokumentoitu suunnitelma, joka kirjaa aikaisemmat muutokset sekä suunnitelmat tuleville muutoksille. Hän painottaa jatkuvan parannuksen,

tapahtumienhallinnan ja sisäisten auditointiprosessien merkitystä osana ISMS:n muutos suunnittelua, jotka toimivat muutosten hallinnan todisteena. Lisäksi Morrison (2023a) muistuttaa, että organisaatioiden tulee myös varmistaa, että viestintäsuunnitelmat sisältävät ISMS:n muutoksista tiedottamisen.

Calder (2023) toteaa, että uudessa 6.3 vaatimuksessa PDCA-mallin käyttäminen on loogisin valinta vaatimuksen täyttämiseen. Hän lisää, että riippumatta käytetystä jatkuvan parantamisen kehyksestä, organisaatioiden tulisi soveltaa sitä kaikissa tilanteissa, joissa tietoturvallisuuden hallintajärjestelmää muutetaan. Hänen mukaansa tämä sisältää ISMS:n soveltamisalan laajentamisen, hallintakeinojen lisäämisen tai uusien prosessien käyttöönoton.

Voidaan päätellä, että ISO/IEC 27001:2022 -standardin vaatimus 6.3 tuo organisaatioille monia huomioitavia seikkoja. Onneksi lukuisat asiantuntijat tarjoavat ohjeita, jotka helpottavat vaatimuksen täyttämisestä. Asiaa myös lähestyä toisaalta helpommallakin tavalla, sillä Armstrong (2023) huomauttaa, että yksinkertainen tapa täyttää kohdan 6.3 vaatimuksia on sisällyttää tämä johdonmukaisesti johtoryhmän kokousten keskusteluihin ja varmistaa näiden keskustelujen dokumentointi.

Standardeja vertailtaessa huomataan, että uusimmassa standardissa on muutettu myös kohtaa 7.4. Vuoden 2013-versiossa vaadittiin, että organisaatioiden tulee määritellä, kuka viestii ja minkälaisia viestintäprosesseja käytetään (ISO/IEC 27001: 2013, 16). Nyt organisaatioiden tulee määritellä, kuinka viestintä toteutetaan (ISO/IEC 27001: 2022, 12). Vaikka uusin standardi keskittyy viestinnän toteutustavan määrittelyyn, on yhä tärkeää ymmärtää, kenen vastuulla viestintä on. Calderin (2023) mukaan tämä muutos on hyödyllinen, sillä se helpottaa tietoturvallisuuden hallintajärjestelmän integroimista osaksi laajempaa viestintästrategiaa.

Tämä kappale perustuu Calderin (2023) näkemyksiin ISO/IEC 27001:2022 -standardin 8.1 kohdan muutoksista. Tämän vaatimuksen mukaan organisaatioiden on nyt määriteltävä prosesseille kriteerit, joilla toteutetaan kuudennessa kohdassa tunnistettuja toimenpiteitä. Kuudennessa kohdassa keskitytään riskien arviointiin, joka ohjaa kahdeksannen kohdan mukaisia päätöksiä

siitä, millaisia hallintakeinoja käytetään riskienhallintaan. ISO/IEC 27002:2022 -standardi esittelee ensimmäistä kertaa hallintakeinojen attribuutit, jotka tarjoavat ohjeistusta näiden hallintakeinojen suunnitteluun ja toteutukseen. Ne määrittelevät, millaisia ominaisuuksia hallintakeinojen tulisi sisältää, jotta ne voivat tehokkaasti hallita tunnistettuja riskejä. Hallintakeinojen attribuutit auttavat määrittelemään, miten hallintakeinot integroidaan organisaatio tietoturvallisuuden hallintajärjestelmään.

Standardeja vertaillessa käy myös ilmi (8.1), että 2013-versiossa keskityttiin vain ulkoistettujen prosessien hallintaan (ISO/IEC 27001: 2013, 18). Uusimmassa versiossa vaatimukset ovat laajentuneet kattamaan myös muut ulkopuolelta hankitut resurssit, kuten tuotteet ja palvelut, jotka ovat olennaisia tietoturvallisuuden hallintajärjestelmälle (ISO/IEC 27001: 2022, 13).

Calder (2023) painottaa myös kohdan 9.1 merkitystä, jossa vaaditaan, että tietoturvallisuuden hallintajärjestelmän tarkkailuun, mittaamiseen, arviointiin ja analysointiin käytettävien menetelmien tulisi tuottaa vertailukelpoisia ja toistettavia tuloksia. Hän myös toteaa, että tämä on ollut vaatimuksena riskienarvioinnissa jo pitkän aikaa. Calderin mukaan nykyään on entistä tärkeämpää, että tietoturvallisuuden hallintajärjestelmän tehokkuuden tarkkailu, arviointi, analysointi ja mittaaminen voidaan näyttää toteen tavalla, joka tuottaa vertailukelpoisia tuloksia, jos esimerkiksi joku muu kuin tavallisesti sitä tekevä henkilö suorittaa prosessin. Hänen mukaansa prosessin tulee olla selkeästi dokumentoitu ja johdon katselmuksen sekä sisäisen auditoinnin tulosten tulisi olla jatkuvasti johdonmukaisia.

Standardeja vertailtaessa havaitaan, että kohtaan 9.3.2 on lisätty uusi elementti, joka korostaa tietoturvallisuuden hallintajärjestelmän kannalta keskeisten sidosryhmien tarpeiden ja odotusten huomioimisen tärkeyttä johdon katselmuksessa. Calderin (2023) mukaan tällä tavalla varmistetaan, että organisaatio seuraa aktiivisesti muutoksia uhkakuvissa ja sääntely-ympäristössä. Hänen mukaansa tämä tarkoittaa myös asiakkaiden tunnistamisen ja heidän sisällyttämisensä organisaatioiden hallintajärjestelmään. Näin ollen organisaatioiden on tärkeää pohtia, miten he voivat tehokkaasti implementoida tämän

muutoksen osaksi olemassa olevia prosessejaan. Esimerkiksi muuttuva sääntely-ympäristö voi vaatia uudenlaista ajattelua ja lähestymistapaa riskienhallintaan.

7.2 Hallintakeinojen muutokset

Uusimman päivityksen myötä ISO/IEC 27001:2022 -standardi on kokenut muutoksia, erityisesti Liite A:ssa suositeltaviin hallintakeinoihin. Aikaisemmin standardi jakautui neljääntoista eri hallintatavoitealueeseen, jotka on nyt yhdistetty neljäksi laajemmaksi hallintateemaksi. Uudet hallintatavoitealueet ovat organisaatio, henkilöstö, fyysinen sekä teknologia. Nämä auttavat organisaatioita hallintakeinojen rakentamistyössä, kun saman aihepiirin hallintakeinot löytyvät helpommin. Tämän lisäksi standardin hallintakeinot ovat vähentyneet 114:stä 93:een. Tämä ei kuitenkaan tarkoita hallintakeinojen vähentämistä, vaan aiempien toimenpiteiden yhdistämistä ja tehokkaampaa organisointia. (Saali 2023.) Voidaan siis päätellä, että muutoksen tavoitteena on parantaa tietoturvan hallintaa ja tehdä hallintakeinojen valinnasta joustavampaa ja helpompaa. 2022-version hallintakeinoista 35 on pysynyt täysin ennallaan, 23 on nimetty uudelleen, 11 uutta otettiin käyttöön sekä 57 hallintakeinoa yhdistettiin 24 hallintakeinoon (PECB 2023). Seuraavassa taulukossa käydään läpi 11 uutta hallintakeinoa.

Taulukko 2. ISO/IEC 27001:2022 -standardin uudet hallintakeinot (ISO/IEC 27001: 2022, Liite A)

Uudet hallintakeinot	Selitys
A.5.7 Uhkatiedon seuranta	• Standardi edellyttää organisaatioilta tietoturvauhkien jatkuvaa keräämistä ja analysointia. • Uhkat jaetaan strategisiin, taktisiin ja operatiivisiin tasoihin. • Tämä tuo tarkempaa uhkaseurantaa ja -hallintaa.
A.5.23 Pilvipalvelujen tietoturvallisuus	• Korostetaan pilvipalveluiden tietoturvallisuutta. • Vaaditaan prosesseja, jotka vastaavat organisaation tietoturvavaatimuksiin ja tunnistavat pilvipalveluiden erityisriskit.
A.5.30 Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa	• Keskittyy tieto- ja viestintätekniikan valmiuden suunnitteluun liiketoiminnan jatkuvuuden varmistamiseksi. • Vaatii suunnittelua, toteutusta, ylläpitoa ja testausta.
A.7.4 Fyysisen turvallisuuden valvonta	• Vaaditaan toimitilojen suojaamista luvattomalta pääsyltä esimerkiksi kameravalvonnan avulla. • Tärkeää luokitella tilat niiden sisältämien tietojen ja omaisuuserien (assets) mukaan.
A.8.9 Konfiguraationhallinta	• Laitteiden, ohjelmistojen ja verkkojen konfiguraatiot sekä niiden turvallisuusvaatimukset on dokumentoitava ja seurattava.
A.8.10 Tietojen poistaminen	• Koskee tietojen poistamista, korostaen, että tallennusvälineissä olevat tiedot on poistettava, kun niitä ei enää tarvita. • Liittyy tiedon elinkaaren hallintaan.
A.8.11 Tietojen peittäminen	• Hallintakeinon tavoitteena on vähentää tietovuodon vaikutuksia käyttämällä menetelmiä, kuten pseudonymisointia ja anonymisointia.
A.8.12 Tietovuotojen estäminen	• Korostetaan tietovuotojen estämisen merkitystä, vaatien teknisiä ratkaisuja ja havainnointikykyä arkaluonteisten tietojen suojeluun.
A.8.16 Valvontatoiminnot	• Painottaa verkkojen, järjestelmien ja sovellusten valvontaa poikkeavan toiminnan tunnistamiseksi ja tietoturvahäiriöiden arviointia. • Edistää proaktiivista toimintaa mahdollisten uhkien hallinnassa.
A.8.23 Verkkosuodatus	• Keskittyy ulkoisten verkkosivustojen sisällön hallintaan. • Tavoitteena vähentää altistumista haitallisille sisällöille.
A.8.28 Turvallinen ohjelmointi	• Painottaa erityisesti ulkopuolisten toimittajien hankkimia ohjelmistoja. • Tavoitteena varmistaa, että ohjelmistot ovat turvallisia sekä organisaation, että sen sidosryhmien kannalta.

Taulukon 2 luomisessa on hyödynnetty ISO/IEC 27001:2013- ja ISO/IEC 27001:2022 -standardeja sekä Nykäsen (2022) ja Saalin (2023) ajatuksia hallintakeinojen muutoksista. Osaa uusista hallintakeinoista tarkastellaan tarkemmin opinnäytetyön luvussa 10.

7.2.1 Uusien hallintakeinojen vaikutus

Vaikka uusimmassa standardissa lisättiin 11 uutta hallintakeinoa, on tärkeää huomata, että näiden uusien hallintakeinojen sisältö ei ole kaikilta osin uutta. Monet niistä perustuvat aiemmin esitettyihin toteutusohjeisiin ja käytäntöihin, jotka ovat ohjanneet, miten tiettyjä hallintakeinoja tulisi soveltaa. Uusimmassa versiossa on päätetty tuoda esiin aiemmin vähemmälle huomiolle jääneistä elementeistä, antaen niille enemmän näkyvyyttä. (Nykänen 2022.)

Tämä kappale perustuu Saalin (2023) ajatuksiin hallintakeinoista. Tarkasteltaessa organisaation hallintakeinoja tietoturvan näkökulmasta, on tärkeää lähestyä niitä kriittisen analyysin kautta. Tämä edellyttää pohdintaa, jonka avulla voidaan varmistaa, että kunkin hallintakeinon soveltaminen organisaation toimintaympäristöön on perusteltua ja tehokasta. Ensimmäinen askel on siis määritellä, mitä kukin hallintakeino konkreettisesti tarkoittaa organisaation kontekstissa. Tämä tarkoittaa standardin tekstien tulkinnan sovittamista organisaation tarpeisiin nähden. On tärkeää ymmärtää, miksi tietyt hallintakeinot on valittu käytettäväksi. Tämä luonnollisesti vaikuttaa uusien hallintakeinojen vaikutukseen organisaatiolle.

Saalin (2023) mukaan kullakin hallintakeinolla tulisi olla määritelty vastuuhenkilöt tai -tiimit organisaatiossa, jotka vastaavat hallintakeinojen toteuttamisesta, seurannasta ja jatkuvasta kehittämisestä. Hänen mukaansa uusien ISO/IEC 27001:2022 -standardissa määriteltyjen 11 hallintakeinon kohdalla on erityisen tärkeää varmistaa, että niiden implementointiin liittyvät prosessit, ohjeistukset ja tarkastuslistat ovat ajan tasalla. Saali muistuttaa, että on tärkeää myös tarkastaa, että ne integroituvat organisaation olemassa oleviin tietoturvaprosesseihin.

Tämä kappale perustuu myös Saalin (2023) ajatuksiin hallintakeinojen tehokkaasta soveltamisesta sekä hallintakeinojen elinkaari ajattelusta. Hänen mukaansa hallintakeinojen tehokas soveltaminen edellyttää myös niiden jatkuvaa arviointia ja kehittämistä. Tämä tarkoittaa muun muassa käsikirjojen päivittämistä, uusien prosessien ja ohjeiden kehittämistä tarpeen mukaan, sekä säännöllistä seurantaa, mittausta ja auditointia. Riskienhallinnan näkökulmasta on keskeistä, että mahdolliset muutokset riskiympäristössä huomioidaan ja että hallintakeinoja päivitetään vastaavasti. Näiden lisäksi on tärkeää tunnistaa ja ymmärtää hallintakeinojen elinkaari. Elinkaariajattelu auttaa organisaatioita rakentamaan yhtenäisiä ja kattavia toimintamalleja, jotka eivät ainoastaan vastaa nykyisiin vaatimuksiin vaan myös auttavat pitkän aikavälin tavoitteita.

Voidaan siis päätellä, että uusien hallintakeinojen käyttöönotto ei ole kertaluonteinen tapahtuma vaan jatkuva prosessi. Mielestäni on siis tärkeää arvioida niiden tehokkuutta ja soveltuvuutta säännöllisesti, jotta voidaan varmistaa, että ne vastaavat muuttuvia ulkoisia ja sisäisiä uhkia.

7.2.2 Hallintakeinojen valinta ja attribuutit

Kuten aiemmin tekstissä mainittiin, osa päivitetyn Liite A:n hallintakeinoista ovat yhdistelmiä vanhoista hallintakeinoista. Tämän takia, on erittäin tärkeää tarkastella kaikkia päivitetyn Liite A:n hallintakeinoja yksitellen. Armstrong (2023) muistuttaa, että ISO/IEC 27002:2022 -standardi tarjoaa paljon uutta lisätietoa ja ajantasaisempaa ohjeistusta. Hänen mukaansa tämä tulee ottaa huomioon olemassa olevissa hallintakeinoissa siirryttäessä ISO/IEC 27001:2013 -standardista ISO/IEC 27001:2022 -standardiin.

ISO/IEC 27002:2022 -standardin versiossa on uutena ominaisuutena attribuutit, joiden tavoitteena on helpottaa ISO/IEC 27001:2022 -standardin Liite A hallintakeinojen valintaa (Nykänen 2022). Tätä korostaa myös Harvey (2024), jonka mukaan attribuuttien käyttö tukee työtä. Hän lisää, että attribuutteja hyödyntää jo monet yritykset riskien arvioinnin ja soveltuvuuslausunnon osalta. Lisäksi on kehitteillä ISO/IEC 27028 -ohjestandardi, joka tarjoaa tietoa hallinta-

keinojen attribuuttien kehittämisestä ISO/IEC 27002:2022 -standardin mukaisesti (ISO/IEC CD 27028 s.a.). ISO/IEC 27002:2022 -standardin hallintakeinon kuvauksessa attribuuttitaulukko voi esimerkiksi näyttää seuraavanlaiselta.

Taulukko 3. Attribuuttitaulukko (ISO/IEC 27002:2022)

Hallintakeinon tyyppi	Tietoturvaominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Henkilöstöturvallisuus	#Hallinto-tapa_ja_ekosysteemi

ISO/IEC 27002:2022 -standardin attribuutteja voidaan hyödyntää monin eri tavoin. Niitä voidaan käyttää tunnistettujen riskien lieventämiseen riskienarviointiprosessin aikana sekä osana riskien käsittelyprosessia. (Pivot Point Security 2024b.) Myös Manimbo (s.a.) toteaa, että organisaatioiden tulisi pitää niitä työkaluina riskien arviointi- ja käsittelyprosesseissa. Pinnell (s.a.) muistuttaa, että organisaatiot voivat myös luoda omia attribuutteja. Seuraava kuva havainnoi miltä itse tehty attribuuttitaulukko voi näyttää.

Taulukko 4. Taulukko havainnoi miltä itse luotu attribuuttitaulu voi näyttää (Pinnell s.a.)

Hallintakeino	Riskin viite	Toteutuksen kehitysvaihe	Toteutusvaihe	Vastuuosasto/vastuuhenkilö	Tietoturvaominaisuudet	Tietoturvan osa-alueet
5.10	#2 #19	#Taso_2	#Osittain_toteutettu	#CISO	#Luottamuksellisuus	#Hallinto-tapa_ja_ekosysteemi
5.24	#5	#Taso_3	#Kokonaan_toteutettu	#CISO #CSO	#Eheys	#Puolustus

Tässä tapauksessa attribuuttitaulukkoon on lisätty kohdat: riskin viite, toteutuksen kehitysvaihe, toteutusvaihe ja vastuuosasto/vastuuhenkilö. Organisaatiot voivat siis luoda omia attribuutteja ja hyödyntää räätälöityjä attribuuttitaulukoita, joka voi auttaa esimerkiksi tietojen hallinnassa ja tietojen löytämisessä.

Loppu kappale perustuu Nykäsen (2022) ajatuksiin attribuutteihin liittyen. Jokaiselle hallintakeinolle on määritelty viisi attribuuttia ISO/IEC 27002:2022 -standardissa. Ensimmäinen attribuutti, hallintakeinon tyyppi kertoo, toimiiko hallintakeino ennaltaehkäisevästi, havaitsevasti vai korjaavasti. Tämä auttaa

organisaatioita valitsemaan toisiaan täydentäviä hallintakeinoja vähentäen riskiä, että yhden hallintakeinon pettäessä seuraisi suurempia ongelmia. Tavoitteena on, että erityyppiset hallintakeinot tukisivat toisiaan. Tämän lisäksi määritellään tietoturvan tietoturvaominaisuudet, kuten luottamuksellisuus, eheys ja saatavuus, joita yleisesti kutsutaan CIA-kolmikoksi. Kohta kyberturvallisuuteen liittyvät käsitteet, kuten tunnistus, suojaus, vaste ja palautus ohjaavat, miten hallintakeinoja sovelletaan kyberturvallisuuden kontekstissa. Toiminnalliset kyvykkyydet selventävät, miten hallintakeinoja voidaan jaotella organisaation eri yksiköille. Esimerkiksi fyysinen turvallisuus ja henkilöstöturvallisuus voidaan määrittää tiettyjen yksiköiden vastuulle näiden attribuuttien perusteella. Viimeinen attribuutti, tietoturvan osa-alueet, joka on sopusoinnussa NIS-direktiivin kanssa, auttavat etenkin NIS-direktiivin piiriin kuuluvia organisaatioita valitsemaan sopivat hallintakeinot.

Attribuuttien käyttö voi siis helpottaa erityisesti hallintakeinojen valintaa ja vähentää organisaatioille merkityksettömien hallintakeinojen käyttöä. Selkeästi määritellyt attribuutit voivat helpottaa myös sertifiointielimen työtä, kun he arvioivat organisaation hallintakeinoja. Tätä tukee Nykänen (2022), jonka mukaan sertifiointia varten on tehtävä soveltuvuuslausunto, jossa käydään läpi esimerkiksi mitkä hallintakeinoista ovat oleellisia ja riskiperusteisesti perusteltuja.

Kuten edellä mainittu, Liite A:n muutokset vaativat organisaatioita uudelleenjärjestämään hallintakeinonsa. Protivitin (s.a.) mukaan tähän voidaan soveltaa kahta erilaista lähestymistapaa. Ensimmäinen vaihtoehto on tarkastella, kuinka hyvin nykyiset riskien arvioinnit kattavat päivitetyn Liite A:n hallintakeinot. Uudet hallintakeinot tulee arvioida niiden soveltuvuuden osalta, ja tietoturvariskien käsittelysuunnitelmia saatetaan tarvita päivittää. Tämän myötä myös soveltuvuuslausunto (SoA) tulee päivittää kuvastamaan kaikkia lisättyjä ja muutettuja hallintakeinoja.

Toinen vaihtoehto on suorittaa uusi riskien arviointi ja tunnistaa uudesta Liite A:sta relevantit hallintakeinot, jotka ovat olennaisia riskien hallitsemiseksi. Varmistetaan, että kaikki relevantit hallintakeinot sisältyvät arviointiin. Tietoturvariskien käsittelysuunnitelmat saattavat vaatia muutoksia heijastamaan uusia

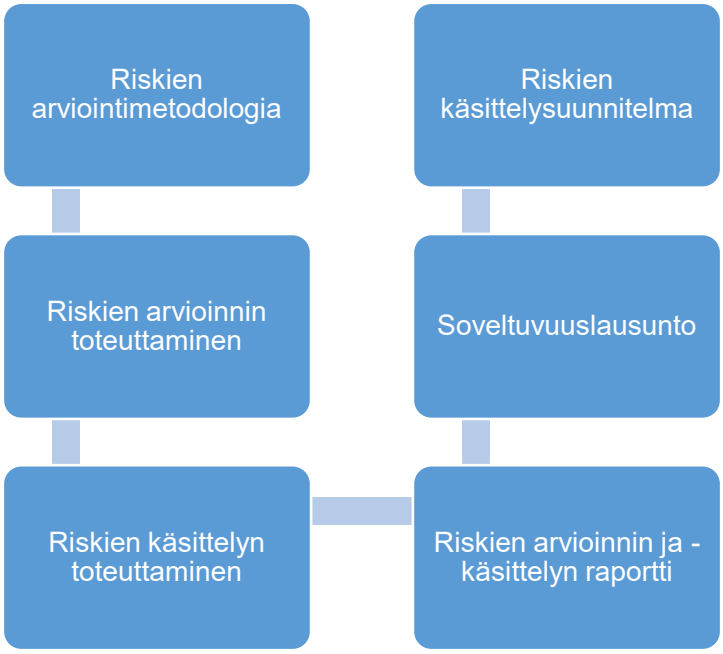
riskejä, jotka vaativat käsittelysuunnitelmaa. On myös tarpeen luoda uusi soveltuvuuslausunto, joka vastaa uusia hallintakeinoja. Viimeisenä tulee päivittää kaikki asiakirjat, jotka viittaavat vanhoihin hallintakeinoihin. (Protiviti s.a.)

On siis tärkeää, että organisaatiot suunnittelevat hallintakeinojen valinnat huolellisesti ja perustavat ne vastaamaan todellisia tarpeitaan riskien hallitsemiseen. Organisaatioille merkityksettömien hallintakeinojen valitseminen voi esimerkiksi kuluttaa organisaatioiden resursseja sekä monimutkaistaa prosesseja ja järjestelmiä turhaan. Tarpeettomat hallintakeinot voivat myös aiheuttaa tyytymättömyyttä työntekijöissä, jos tietyt menettelytavat eivät perustu todellisiin riskeihin.

7.3 Riskien arviointi, käsittely ja tunnistaminen

ISO/IEC 27001:2022 -standardin siirtymäprossissa on hyvä tarkastaa riskien arvioinnin ajantasaisuus. Jos organisaatio hyödyntää riskien arvioinnissa ISO/IEC 27005 -standardia ohjeistuksena, on hyvä muistaa, että tämä standardi sai myös päivityksen vuonna 2022. (Kosling 2024.) Muita riskien arviointia tukevia standardeja ovat ISO 31000 -standardi ja NIST SP 800-30 -standardi.

ISO/IEC 27001:2022 -standardin (2022) kohdan 6.1.2 mukaan organisaatioiden on määriteltävä ja toteutettava tietoturvariskien arviointiprosessi. Lisäksi standardin kohta 8.3 vaatii, että organisaatioilla on oltava käytössä riskien käsittelysuunnitelma. Seuraavassa kuuden kohdan ohjeessa käydään nämä läpi pääpiirteittäin.



Kuva 3. Riskien arvioinnin ja käsittelyn pääkohdat (ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide s.a.)

ISO/IEC 27001:2022 -standardi määrittelee viisi keskeistä elementtiä riskien arviointiprosessille: riskien tunnistaminen, riskien omistajien tunnistaminen, seurausten ja todennäköisyyksien arvioinnin kriteerit, riskilaskennan menetelmät ja riskien hyväksymiskriteerit. Riskien arvioinnissa on monta vaihtoehtoa, mutta metodologian valinta on tärkeää, jotta se sopii organisaation omiin tarpeisiin. Standardi ei määritä kuitenkaan tarkasti, miten kunkin elementin toteuttaminen pitää tapahtua. Tämä tarkoittaa, että organisaatio voi itse päättää sopivammat menetelmät kunkin elementin käsittelyyn omien tarpeidensa ja olosuhteidensa mukaan. ISO/IEC 27001:2022 -standardin riskienhallinnan aloittamiseksi organisaatiot tarvitsevat yhtenäiset ja selkeät säännöt riskienhallintaprosessien toteuttamiseksi. (ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide s.a.)

Riskien arvioinnin toteuttaminen koostuu kaikkien omaisuuserien, niiden uhkien sekä haavoittuvuuksien listaamisesta. Tämän jälkeen on tärkeää arvioida omaisuuserien, uhkien ja haavoittuvuuksien yhdistelmien vaikutukset. Näiden avulla pystytään laskemaan riskin taso. Riskien käsittelyn toteuttamisessa keskitytään merkittävimpiin riskeihin, sillä kaikki riskit eivät ole organisaatioille yhtä merkittäviä. ISO/IEC 27001:2022 -standardin riskien käsittely koostuu

neljästä vaihtoehdosta: riskin pienentämisestä, riskin välttämisestä, riskin jakamisesta sekä riskin hyväksymisestä. Näistä riskin pienentäminen on yleisin vaihtoehto.

Riskien arvioinnin ja käsittelyn raportoinnissa dokumentoidaan kaikki aiemmin tehdyt toimenpiteet. ISO/IEC 27001:2022 -standardi ei kuitenkaan määritä raportin sisältöä. (ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide s.a.) Standardissa sanotaan kuitenkin, että organisaation tulee ylläpitää dokumentaatioita tietoturvariskien arviointi- ja käsittelyprosesseista sekä tietoturvariskien arviointien tuloksista (ISO/IEC 27001:2022). Raportti sisältää kuitenkin kaikki tunnistetut riskit, niiden vaikutukset ja todennäköisyydet, riskitasot, riskien omistajat, hyväksymättömät riskit sekä kunkin hyväksymättömän riskin käsittelyvaihtoehdot (ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide s.a.).

Soveltuvuuslausuntoa käydään enemmän läpi opinnäytetyön seuraavassa luvussa (7.4). Pääpiirteittäin tämä dokumentti sisältää yksityiskohtaisen luettelon käytössä olevista hallintakeinoista, niiden käyttöönottoperusteista sekä käyttötavoista. Soveltuvuuslausunto on myös keskeinen osa sertifioinnin tarkastusprosessia. Riskien käsittelysuunnitelmassa siirrytään teoreettisesta lähestymistavasta käytännön toimiin. Aiemmin teoreettisesti käsittelyt asiat muuttuvat nyt konkreettisiksi toimenpiteiksi. Riskien käsittelysuunnitelma selventää, kuka vastaa minkäkin turvatoimen toteutuksesta ja millaisella aikataululla. (ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide s.a.)

Tämä kappale perustuu ISO/IEC 31010:2019 -standardin (2019) sisältöön. ISO/IEC 31010:2019 -standardi tarjoaa laajasti ohjeita riskien arviointimenetelmistä. Se myös toimii tukena ISO 31000:2018 -riskienhallintastandardille. ISO/IEC 31010-standardi keskittyy erityisesti erilaisten menetelmien esittelemiseen, joita voidaan käyttää riskien tunnistamiseen, analysointiin ja arviointiin. Tämä standardi auttaa organisaatioita valitsemaan sopivimmat menetelmät heidän riskienhallintatarpeisiinsa. ISO/IEC 31010-standardin riskien arviointimenetelmät auttavat ymmärtämään olemassa olevia riskejä, tukevat riskienhallintaprosessia sekä helpottavat päätöksentekoa riskien vertailussa ja

arvioimisessa. Standardin mukaan erilaisia riskien tunnistamismenetelmiä ovat muun muassa erilaiset empiiriset- ja näyttöperusteiset menetelmät, skenaarioanalyysi sekä tarkistusluettelot. Standardissa kuvaillaan myös sidosryhmien osallistamisesta mikä on keskeinen osa ISO/IEC 27001:2022 -standardia. Standardista voidaan tiivistää, että sidosryhmien tunnistaminen ja osallistaminen on keskeistä riskien arvioinnissa, sillä he tarjoavat arvokasta tietoa ja näkemyksiä. Standardin mukaan heidän osallistumisensa edistää ymmärrystä toimintaympäristöstä, parantaa riskien tunnistamista ja ymmärtämistä. Standardi sisältää myös menetelmiä, joilla pyritään saamaan selville asiantuntijoiden ja sidosryhmien näkemyksiä.

7.4 Soveltuvuuslausunto

Soveltuvuuslausunto (SoA) kuvaa organisaation lähestymistapaa Liite A:n hallintakeinojen toteuttamiseen. Soveltuvuuslausunto on dokumentti, joka sisältää ne hallintakeinot, jotka organisaatio aikoo ottaa käyttöön ISO/IEC 27001:2022 -standardin vaatimusten täyttämiseksi. Tämä on pakollinen vaihe jokaiselle organisaatiolle, joka suunnittelee ISO/IEC 27001:2022 -sertifikaatin hankkimista. Soveltuvuuslausunnon tulisi pitää sisällään lista kaikista hallintakeinoista, joita organisaatio käyttää vastatakseen tietoturvariskien käsittelyvaihtoehtoihin. Sen lisäksi soveltuvuuslausunnon tulee sisältää perustelut hallintakeinoille eli miksi kukin listattu hallintakeino on valittu mukaan. Näiden lisäksi sen tulee sisältää todiste siitä, että hallintakeinot on otettu käyttöön suunnitelman mukaan. Viimeisenä soveltuvuuslausunto tulee sisältää selvitys siitä, miksi jotkin hallintakeinot on päätetty jättää pois. (Edwards 2024.)

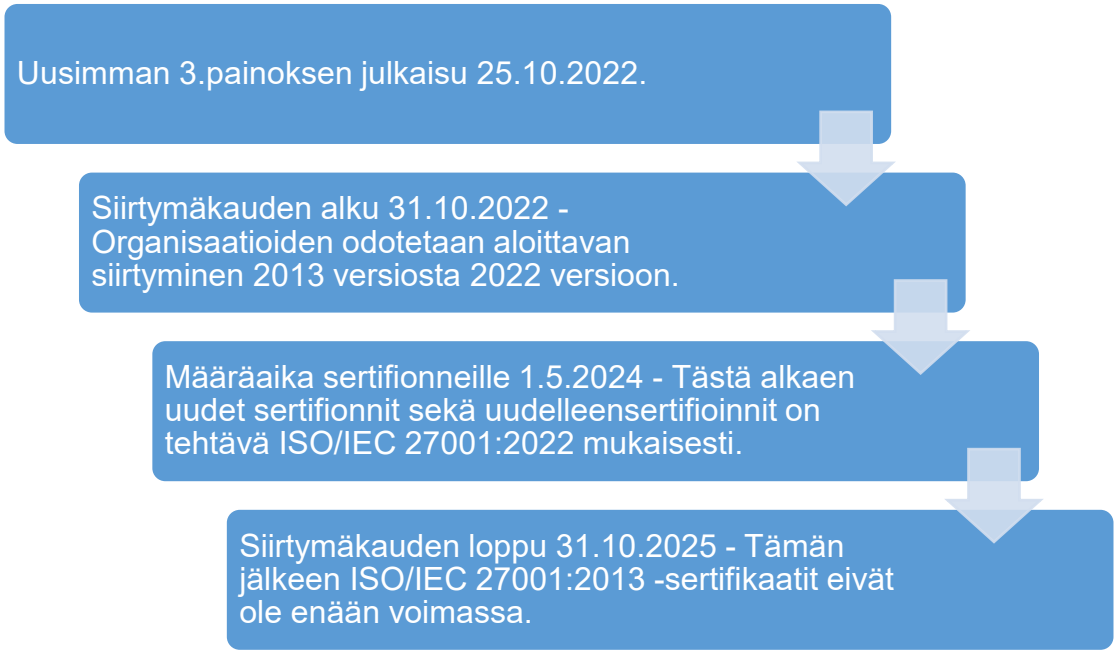
Soveltuvuuslausunto on myös yksi ensimmäisistä dokumenteista, johon auditoija tyypillisesti kiinnittää huomiota. Mikäli auditoija havaitsee, että organisaatio ei ole päivittänyt soveltuvuuslausuntoaan ISO/IEC 27001:2022 -standardin mukaisten uusien vaatimusten ja hallintakeinojen osalta, se viittaa siihen, että siirtymäprosessi uuteen standardiin ei ole vielä käynnistynyt. (Armstrong & Harrison 2024.)

Mikäli organisaation sovellettavuuslausunto (SoA) on laadittu ISO/IEC 27001:2013 -standardin mukaisesti, on suositeltavaa hyödyntää ISO/IEC

27002:2022 -standardin Liite B muutostaulukkoa. Tämä auttaa tekemään vertailuja ja arvioimaan, miten vanhat hallintakeinot vastaavat uuden version vaatimuksia. Muutostaulukosta löytyy vastaavuudet kullekin hallintakeinolle, joka auttaa myös ymmärtämään muutoksia. On tärkeää huomata, että kaikki kohdat eivät mene yksi yhteen. Tämä johtuu siitä, että joitakin hallintakeinoja on yhdistetty tai jaettu useampaan osaan. Tämän lisäksi osa uusista hallintakeinoista on johdettu vanhoista hallintakeinoista. (Nykänen 2022.) Vaikka muutostaulukko ei tarjoa täydellisiä vastaavuuksia kaikille hallintakeinoille, se voi silti merkittävästi helpottaa päivitysprosessia ja auttaa arvioimaan, mitä hallintakeinoja on syytä tarkastella lisää.

8 SIIRTYMÄPROSESSI

ISO/IEC 27001:2022 -standardin päivitys tuo mukanaan muutoksia ja parannuksia tietoturvan hallintakäytäntöihin. Jotta organisaatiot voivat onnistuneesti sopeutua näihin muutoksiin, niiden on toteutettava huolellista suunnittelua. (Protiviti s.a.) Aikataulu ISO/IEC 27001:2022 -standardin käyttöönotolle on seuraavanlainen (kuva 4).



Kuva 4. Aikataulutus perustuu International Accreditation Forumin viralliseen dokumenttiin (2023)

Organisaatioiden on siis siirryttävä uusimpaan ISO/IEC 27001:2022 -standardiin kolmivuotisen siirtymäkauden aikana, joka päättyy 31.10.2025 (International Accreditation Forum 2023, 8). Tämä siis tarkoittaa, että ISO/IEC 27001:2013 -sertifikaatit eivät ole enää voimassa tämän jälkeen. Organisaatioiden on suunniteltava ja toteutettava siirtyminen valmiiksi ennen siirtymäkauden loppumista. Tämä siirtymäkausi antaa organisaatioille mahdollisuuden varmistaa, että niiden tietoturvallisuuden hallintajärjestelmä täyttää uusimmat vaatimukset. Organisaation siirtyminen uuteen ISO/IEC 27001:2022 -standardiin edellyttää systemaattista lähestymistapaa, joka alkaa organisaation sisäisestä valmistautumisesta. (NQA s.a.)

Kaikkien organisaatioiden tulee suorittaa siirtymäauditointi varmistaakseen, että tietoturvallisuuden hallintajärjestelmät täyttävät uuden version vaatimukset. Siirtymäauditoinnissa arvioidaan, miten hyvin organisaation tietoturvallisuuden hallintajärjestelmä vastaa uusia vaatimuksia. (NQA s.a.) Tämä voi sisältää prosessien, riskienhallinnan menetelmien ja politiikkojen tarkastelua ja päivittämistä (Protiviti s.a.). Kappaleen loppuosa perustuu International Accreditation Forumin (2023) julkaisemaan Transition Requirements for ISO/IEC 27001:2022-dokumenttiin. Tässä dokumentissa määritellään siirtymävaatimukset organisaatioille, jotka ovat jo sertifioituja ISO/IEC 27001:2013 -standardin mukaan. Dokumentin mukaan siirtymätarkastus voidaan suorittaa samanaikaisesti valvontatarkastuksen, uusintatarkastuksen tai erillisen tarkastuksen yhteydessä. Siirtymätarkastuksen ei tulisi perustua pelkästään asiakirjojen tarkastukseen, erityisesti kun tarkastellaan teknologisia hallintakeinoja. Siirtymätarkastuksen tulee sisältää, mutta ei rajoittua seuraaviin asioihin (taulukko 5).

Taulukko 5. Siirtymätarkastuksessa käytävät kohdat (International Accreditation Forum 2023)

Siirtymätarkastuksessa tarkasteltavat kohdat
Gap-analyysi ISO/IEC 27001:2022 -standardin ja asiakkaan tietoturvallisuuden hallintajärjestelmän muutostarpeiden arvioimiseksi.
Soveltuvuuslausunnon päivittäminen.
Tarvittaessa riskien käsittelysuunnitelman päivittäminen.
Uusien tai muuttuneiden hallintakeinojen valinta ja niiden toteutuksen tehokkuuden arviointi.

Jos auditoinnissa havaitaan puutteita, organisaation on toimitettava korjaava toimenpide, joka on hyväksyttävä ennen päivitetyn ISO/IEC 27001:2022-sertifikaatin myöntämistä (NQA s.a.). Organisaatioiden on siis varmistettava, että niiden tietoturvallisuuden hallintajärjestelmät vastaavat uuden standardin vaatimuksia. Tämä saattaa vaatia päivityksiä ja muutoksia nykyisiin käytäntöihin.

Alla oleva taulukko 6 esittelee, kuinka organisaatiot voivat päivittää tietoturvallisuuden hallintajärjestelmänsä vastaamaan ISO/IEC 27001:2022 -standardin vaatimuksia.

Taulukko 6. ISMS:n siirtymäprosessi

Vaihe	Kuvaus
1. Gap-analyysi	• Saadaan kuva uuden standardin muutostarpeista. • Tarkastetaan riskianalyysi, prosessit, SoA, politiikat ja toimintaohjeet.
2. Toimintasuunnitelma	• Määritellään tarvittavat toimenpiteet. • Luodaan kullekin toimenpiteelle toteutussuunnitelma. • Määritetään vastuuhenkilöt, asetetaan aikataulut, seurataan edistymistä ja suunnitellaan toteutus.
3. Riskien arvioinnin päivittäminen	• Oleellinen sillä Liite A hallintakeinoihin on tullut muutoksia. • Sisältää riskianalyysin päivittämisen.
4. Riskien käsittelysuunnitelman mukauttaminen	• Varmistetaan, että yhtään hallintakeinoa ei jätetä pois.
5. Hallintakeinojen mukauttaminen	• Tehdään riskilähtöinen kartoitus uusista ja muuttuneista hallintakeinoista. • Selvitetään, miten hallintakeinoja sovelletaan ja mitä niiden toteuttaminen käytännössä vaatii. • ISO/IEC 27002:2022 Liite B.
6. SoA:n päivitys	• Päivitetään soveltuvuuslausunto vastaamaan uusia hallintakeinoja.
7. Sisäinen auditointi	• Varmistetaan ISMS:n vaatimuksenmukaisuus päivitettyä versiota vasten. • Huolehditaan vaadittujen muutontoimenpiteiden siirtymä organisaatioon. • Kiinnitetään erityistä huomiota Liitteen A uudistettuihin hallintakeinoihin, riskien käsittelyyn ja riskianalyysiin.
8. Johdon katselmus	• Ylimmän johdon tulee arvioida muutosten vaikutus ISMS:ssä. • Ylin johto arvioi esimerkiksi riskienhallinnan ja sisäisen auditoinnin tulosten perusteella. • Ylimmän johdon tulee tehdä myös tarvittavat päätökset jatkotoimista.
9. Siirtymäarvioinnin toteutus	• Voidaan tehdä erillisenä siirtymäarviointina, seuranta-arvioinnin yhteydessä tai osana uudelleensertifiointia.

Kyseinen taulukko perustuu alun perin Kiwa Inspectan (2023b) suosittelemaan seitsemän askeleen siirtymäprosessiin. Ohjeistukseen on sisällytetty elementtejä myös BSI Groupin (s.a.) siirtymäohjeesta. Tämä tekee siitä tehokkaan työkalun, joka tukee organisaation tietoturvallisuuden hallintajärjestelmän päivitysprosessia ja auttaa täyttämään ISO/IEC 27001:2022 -standardin vaatimukset. Seuraavaksi käydään yksityiskohtaisesti läpi ohjeistuksen vaiheet.

Kiwa Inspectan (2023b) mukaan gap-analyysi on olennainen osa organisaatioiden siirtymäprosessin suunnittelua. Opinnäytetyön 7 luvun tutkimusosiosta voidaan päätellä, että on tärkeää selvittää ja ymmärtää uuden ISO/IEC 27001:2022 -standardin vaatimukset. Tämä sisältää kaikkien muutosten, lisäysten ja poistojen läpikäynnin verrattuna ISO/IEC 27001:2013 -versioon. Tässä vaiheessa on syytä arvioida nykyistä tietoturvallisuuden hallintajärjestelmää, mikä tarkoittaa olemassa olevien politiikkojen, prosessien, riskianalyysin, soveltuvuuslausunnon ja sisäisen auditoinnin dokumenttien tarkastelua (Kiwa Inspecta 2023b). Tämän jälkeen organisaatioiden on hyvä verrata nykyistä tietoturvallisuuden hallintajärjestelmää uuden standardin vaatimuksiin, tunnistaa puutteet ja kuvata tarvittavat muutokset (Crawley 2024).

Gap-analyysin avulla tunnistettujen puutteiden korjaamiseksi on tärkeää luoda toimintasuunnitelma. (Kiwa Inspecta 2023b). Jokaiselle toimenpiteelle on hyvä laatia yksityiskohtainen suunnitelma, joka sisältää toimenpiteen tavoitteet, toteutustavan, aikataulun, edistymisen seurannan, vastuut ja tarvittavat resurssit (ISO/IEC 27001: 2022, 11; Kiwa Inspecta 2023b). On tärkeää määritellä realistinen aikataulu kullekin toimenpiteelle sekä ottaa huomioon toimenpiteiden laajuus ja vaikutukset muihin toimintoihin (ISO/IEC 27001: 2022, 11). Kuten 7 luvun sisällöstä käy ilmi, on myös tärkeää huomioida ja integroida uudet rakenteelliset vaatimukset, kuten ISO/IEC 27001:2022 -standardin vaatimus 6.3, joka keskittyy ISMS:n muutosten suunnitelmalliseen toteutukseen.

On tärkeää tarkastella nykyistä riskianalyysiä ja arvioida, kuinka hyvin se vastaa päivitettyä Liite A:ta (Kiwa Inspecta 2023b). Kun hallintakeinot muuttuvat, organisaatioiden tulee uudelleenarvioida riskejä. Tähän on kaksi lähestymistapaa: ensimmäinen vaihtoehto hyödyntää olemassa olevaa riskien arviointia

merkityksellisten hallintakeinojen tunnistamiseksi. Toinen vaihtoehto on suorittaa kokonaan uusi riskien arviointi ja tunnistaa Liite A:sta relevantit hallintakeinot. Molemmissa tapauksissa on tarpeen päivittää riskien käsittelysuunnitelmat heijastamaan uusia riskejä. (Protiviti s.a.)

Riskien käsittelysuunnitelman mukauttamisessa on tärkeää ymmärtää, mitä muutoksia on tehty Liite A:n hallintakeinoihin. Organisaatioiden tulee tarkastaa nykyinen käsittelysuunnitelma ja vertaa sitä päivitettyyn Liite A:han. (Kiwa Inspecta 2023b.) International Accreditation Forumin (2023) mukaan, jos organisaatio havaitsee puuttuvia hallintakeinoja, sen tulee päivittää riskien käsittelysuunnitelma sisällyttämään lisätyt hallintakeinot ja toteuttaa ne. Samassa dokumentissa mainitaan myös, että siirtymäauditointi voi tarvittaessa sisältää riskien käsittelysuunnitelman päivittämisen. Tästä voidaan päätellä, että on olennaista etsiä puutteita ja kohtia, joissa nykyinen suunnitelma ei ole linjassa uusimpien hallintakeinojen kanssa. On myös tärkeää varmistaa, että jokainen muutos on huolellisesti suunniteltu (ISO/IEC 27001: 2022, 11).

Kun hallintakeinoja on päivitetty liitteessä A, on tärkeää tehdä riskilähtöinen kartoitus niiden vaikutuksista organisaation riskienhallintaan. Tässä vaiheessa tulee tutkia uusia ja muuttuneita hallintakeinoja sekä määrittää, miten niitä sovelletaan käytännössä ja mitä niiden toteuttaminen vaatii. ISO/IEC 27002:2022 -standardin Liite B tarjoaa hyödyllisen työkalun tässä tutkimuksessa, sillä sen avulla voidaan helposti suorittaa vertailu vanhan ja uuden version hallintakeinojen välillä. (Kiwa Inspecta 2023b.) Näin ollen ISO/IEC 27002:2022 -standardi auttaa ymmärtämään muutosten laajuutta ja niiden mahdollisia vaikutuksia.

Siirtymäprosessissa tulee myös päivittää soveltuvuuslausunto vastaamaan uusia muutoksia (Kiwa Inspecta 2023b). Soveltuvuuslausuntoon tulee listata kaikki tarpeelliset hallintakeinot sekä dokumentoida, miksi valitut hallintakeinot ovat käytössä (Edwards 2024). Voidaan siis päätellä, että organisaatioiden tulee arvioida, miten uudet hallintakeinot vaikuttavat nykyiseen turvallisuusympäristöön ja ottaa tarvittavat hallintakeinot käyttöön arvion mukaan. On selvää, että tämä sisältää tarkastelun, mitkä hallintakeinot ovat edelleen relevantteja,

mitkä ovat poistuneet ja mitä uusia hallintakeinoja on lisätty. Näin ollen päivitetty soveltuvuuslausunto auttaa varmistamaan ja osoittamaan, että kaikki käytössä olevat hallintakeinot ovat ajan tasalla ja tehokkaasti dokumentoituja.

Sisäisen auditoinnin tarkoituksena on varmistaa, että organisaation tietoturvallisuuden hallintajärjestelmä täyttää uudistetun standardin vaatimukset. Auditointiprosessissa tarkastellaan erityisesti, miten uusi versio on otettu käyttöön. Erityistä huomiota kiinnitetään Liite A:n päivitettyihin hallintakeinoihin, riskianalyysiin ja riskien käsittelyyn. (Kiwa Inspecta 2023b.) On tärkeää tarkastaa, että kaikki muutokset ovat asianmukaisesti suunniteltu, dokumentoitu ja että niitä seurataan ja arvioidaan säännöllisesti (ISO/IEC 27001: 2022).

Johdon katselmus on myös olennainen osa siirtymäprosessia. Ylimmän johdon tulee arvioida uuden standardin mukaisten muutosten vaikutusta tietoturvallisuuden hallintajärjestelmään. Tämä katselmus perustuu muun muassa riskienhallinnan ja sisäisen auditoinnin tuloksiin. (Kiwa Inspecta 2023b.) Johdon on tärkeää ymmärtää, miten tehtyjen muutosten vaikutukset heijastuvat koko organisaation tietoturvaan ja päättää mahdollisista jatkotoimenpiteistä (ISO/IEC 27001: 2022, 15). Voidaan siis päätellä, että johdon katselmus on tärkeä osa jatkuvan parannusprosessin ylläpitämistä ja se varmistaa, että tietoturvallisuuden hallintajärjestelmä pysyy ajan tasalla ja toimii tehokkaasti.

Siirtymäarviointi voidaan toteuttaa erillisenä siirtymäarviointina, osana säännöllistä seuranta-arviointia tai uudelleensertifiointiprosessin yhteydessä. On tärkeää huomioida, että ISO/IEC 27001:2013 -version voimassaolo päättyy 31.10.2025. Tähän päivämäärään mennessä kaikkien sertifioitujen tietoturvallisuuden hallintajärjestelmien tulee olla päivitetty uuteen versioon. Esimerkiksi Kiwa Inspecta ei suorita sertifiointi- ja uudelleensertifiointiarviointeja vanhaa versiota vasten 30.4.2024 jälkeen. Heidän mukaansa siirtymäarvioinnit tulee suorittaa viimeistään 30.6.2025, jotta aikaa jää riittävästi mahdollisten poikkeamien korjaamiseen. (Kiwa Inspecta 2023b.)

9 KYSELYTUTKIMUS

Kyselytutkimus kohdistetaan valituille tietoturva-asiantuntijoille, joiden asiantuntemus on keskeistä arvioitaessa ISO/IEC 27001:2022 -standardin uusimpia muutoksia. Kyselyn tulokset tarjoavat johtopäätöksiä, jotka osoittavat, mitkä aihealueet vaativat syvempää tarkastelua opinnäytetyössä. Analyysin jälkeen tutkimuksessa keskitytään valittuihin teemoihin, joiden pohjalta kehitetään suosituksia ja laajennetaan teoreettista ymmärrystä aiheesta. Näin pyritään lisäämään opinnäytetyön hyödyllisyyttä. Kyselyn päätavoitteena on tunnistaa, mitkä uudistukset asiantuntijoiden mukaan ovat keskeisimpiä.

9.1 Kyselyn toteutus

Tavoitteena on suunnitella kysely niin, että se on riittävän lyhyt ja ytimekäs kannustamaan asiantuntijoita vastaamaan kyselyyn. Kyselyn pituuden optimointi on keskeinen strategia, sillä lyhyemmät kyselyt parantavat usein vastausprosenttia (Lindgren 2016). Vastausprosentin parantamiseksi kyselyn avoimet kysymykset ovat vapaaehtoisia.

Kyselyn suunnittelussa hyödynnetään laajaa laadullista aineistoa, joka koostuu ISO/IEC 27001:2022 -standardin dokumentista, tämän opinnäytetyön teoreettisesta viitekehyksestä sekä erityisesti luvun 7 tutkimustuloksista. Tietojen syvällinen ymmärrys mahdollistaa tarkasti suunnitellun rakentamisen. Kysely toteutetaan sähköisenä lomakkeena käyttäen Google Forms -palvelua. Kysely koostuu avoimista kysymyksistä, yhdestä monivalintakysymyksestä sekä Likert-asteikolla mitattavista kysymyksistä. Avoimet kysymykset tarjoavat mahdollisuuden perusteellisiin vastauksiin ja syvälliseen näkemykseen aiheesta, kun taas monivalintakysymys antaa selkeitä tilastollisia tietoja keskeisestä aiheesta. Likert-asteikon kysymykset puolestaan mittaavat vastaajien mielipiteiden voimakkuutta eri väittämiin nähden (Vainikainen s.a.). Kysely sisältää kysymyksiä standardin päivityksen merkityksestä, siirtymäprosessin haasteista ja riskienhallinnan tärkeydestä. Kyselyn vastauksia käytetään hallintakeinojen syvällisessä tarkastelussa ja suositusten kehittämisessä. Vastaajille lähetetään kutsulinkki Microsoft Teams -palvelun kautta, mikä on suunniteltu lisäämään vastausprosenttia ja parantamaan kyselyn luotettavuutta. Kyselyn toimivuus on varmistettu asiantuntija-arvioinnilla.

9.2 Kyselyn vastaukset

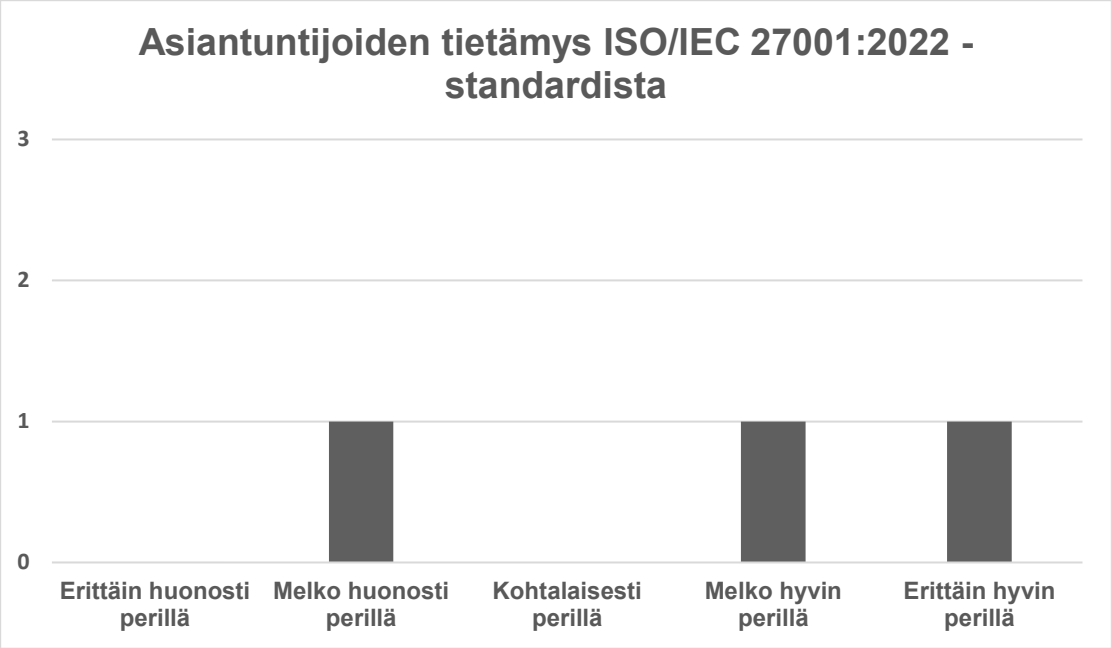
Kyselyyn valittiin kuusi tietoturva-asiantuntijaa, joista kolme vastasi kyselyyn. Tämä rajoittaa tutkimussuunnitelman mukaista määrällistä analyysiä. Siksi tutkimuksessa on päätetty hyödyntää myös laadullista sisällönanalyysiä, joka keskittyy etenkin avoimien vastausten syvälliseen tarkasteluun. Analyysissä eritellään vastauksien keskeiset teemat ja niiden merkitykset, mikä tarjoaa arvokasta tietoa suositusten kehittämiseen.

Jo muutaman kokeneen asiantuntijan vastaukset ovat hyödyllisiä, sillä ne auttavat rajaamaan kyselyn jälkeistä tutkimusosuutta. Tämän vuoksi vastaajien määrä suhteessa otantaan ei ole merkittävä haitta tutkimuksessa. Kyselyn analyysissä tarkastellaan vastauksien sisältöä yksityiskohtaisesti. Kyselyn tarkoituksena on ymmärtää vastaajien näkökulmia ja kokemuksia standardin uusista vaatimuksista.

Vaikka tulokset perustuvat vain kolmen asiantuntijan näkemyksiin, ne tarjoavat silti arvokasta tietoa siitä, miten asiantuntijat näkevät standardin muutokset. Tämä tieto on hyödyllistä, kun kehitetään suosituksia ISO/IEC 27001:2022 -standardin mukaisesti. Lisäksi tämä tilanne korostaa tarvetta jatkotutkimuksille ja uusille lähestymistavoille kyselyn suunnittelussa ja toteutuksessa, jotta voidaan varmistaa laajempi osallistuminen ja kattavampi aineistonkeruu tulevaisuudessa.

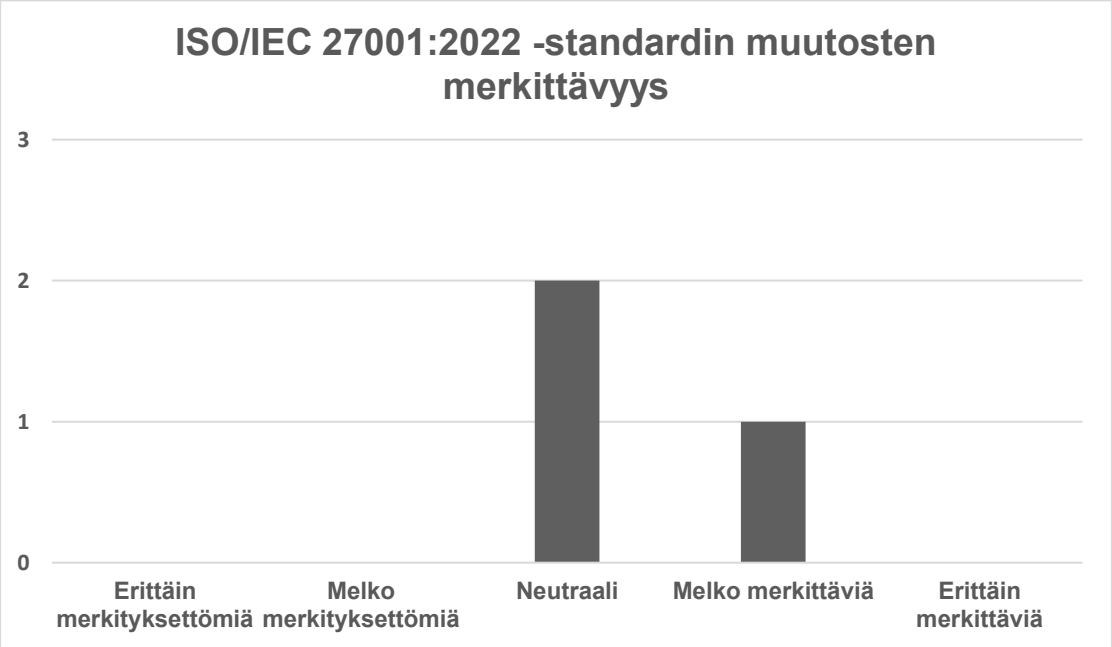
9.2.1 Standardin yleinen ymmärrys ja vaikutukset

Kyselyn ensimmäiseen kysymykseen, jossa tiedustellaan vastaajien tietoisuutta ISO/IEC 27001:2022 -standardin vaatimuksista ja muutoksista, vastaajat ilmoittavat seuraavasti.



Kuva 5. Asiantuntijoiden tietämys ISO/IEC 27001:2022 -standardista

Tämä viittaa siihen, että ISO/IEC 27001:2022 -standardin tuntemuksessa on vaihtelua. Kaksi kolmesta asiantuntijasta kokee kuitenkin olevansa hyvin perillä asiasta. Toiseen kysymykseen, jossa kartoitetaan vastaajan näkemystä ISO/IEC 27001:2022 -standardin muutosten merkittävyydestä, vastaajat arvioivat muutokset melko neutraaleiksi, kuten seuraava kaavio havainnollistaa.

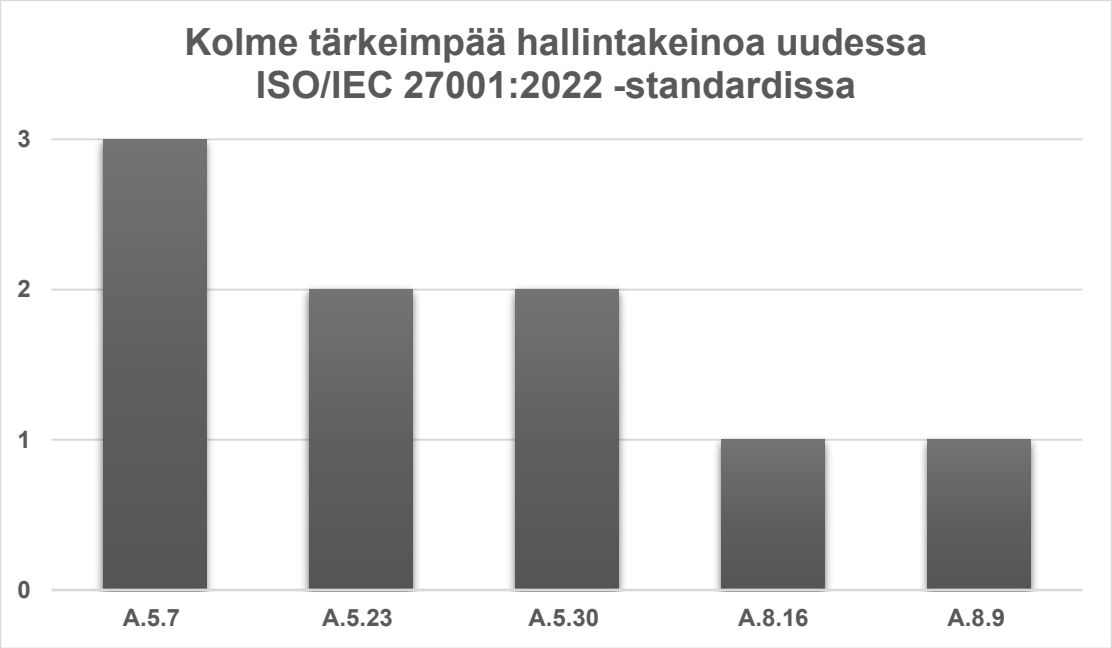


Kuva 6. Standardin muutosten merkittävyys

Kolmesta asiantuntijoista kaksi pitää muutoksia neutraaleina, mikä viittaa siihen, että he eivät näe muutosten vaikuttavan merkittävästi olemassa oleviin käytäntöihin tai eivät koe muutoksia kovin merkittävinä. Yksi asiantuntijoista pitää muutoksia melko merkittävinä, mikä osoittaa, että hän näkee muutokset tärkeinä ja mahdollisesti vaikuttavina.

9.2.2 Keskeiset uudistukset ja niiden vaikutukset

Kyselyssä pyydettiin vastaajia nimeämään kolme tärkeintä uutta hallintakeinoa ISO/IEC 27001:2022 -standardissa. Seuraava kaavio kuvastaa hallintakeinoja, joita asiantuntijat pitivät tärkeimpinä.



Kuva 7. Asiantuntijoiden mielestä tärkeimmät hallintakeinot ISO/IEC 27001:2022 -standardissa

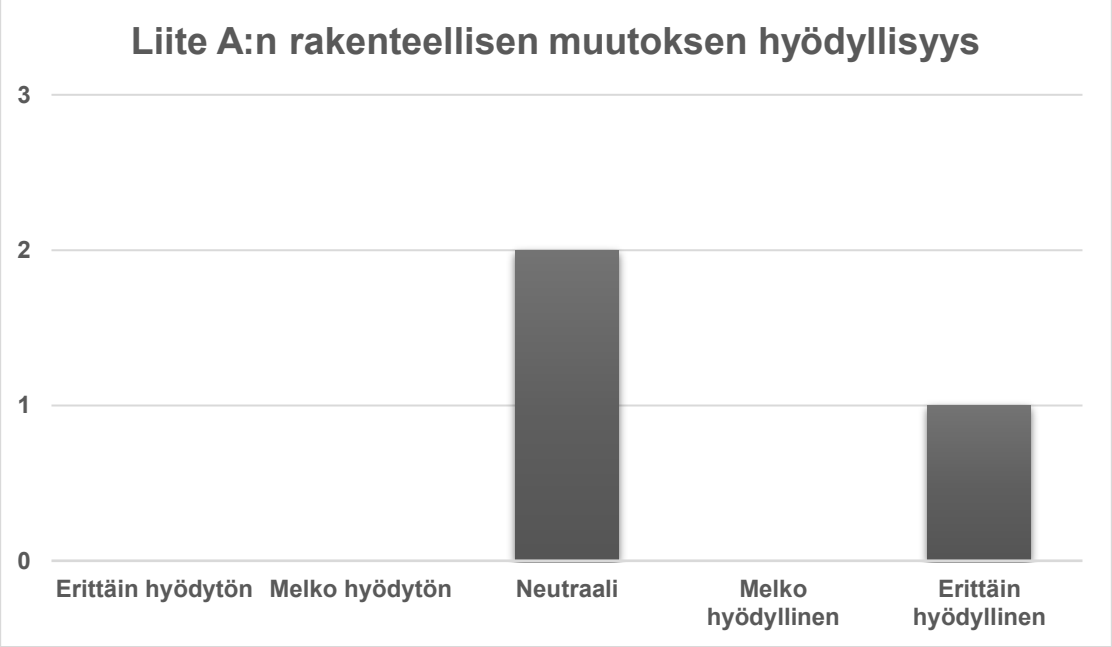
Vastaajista kaikki kolme vastaavat tärkeimmäksi hallintakeinoksi uhkatiedon seurannan (A.5.7), mikä korostaa jatkuvan tietoturvauhkien seurannan ja analysoinnin tärkeyttä. Tämä kuvastaa organisaatioiden tarvetta ennakoivaan ja reaaliaikaiseen tietoturvallisuusstrategiaan. Pilvipalvelujen tietoturvallisuus (A.23) sekä tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa saivat kumpikin kaksi mainintaa, mikä heijastaa näiden alueiden merkityksen tärkeyttä digitalisoituvassa liiketoimintaympäristössä. Vähemmän mainintoja saivat valvontatoiminnot (A.8.15) ja konfiguraationhallinta (A.8.9).

Opinnäytetyön luvussa 9 tarkastellaan syvällisemmin niitä hallintakeinoja, jotka keräsivät eniten mainintoja kyselyssä.

Lisäksi kysyttäessä, mitä vaikutuksia vastaajien valitsemien hallintakeinojen päivityksillä on organisaation tietoturvaan yleisesti, saatiin kolme erilaista näkökulmaa. Ensimmäinen vastaus korostaa, että päivitykset kehittävät organisaation toimintaa. Tämä viittaa siihen, että uudistukset edistävät tietoturvan prosesseja ja parantavat organisaation kykyä vastata tietoturvauhkiin tehokkaammin. Toinen vastaaja nosti esiin, että samanaikaisen NIS2-direktiivin ja ISO/IEC 27001:2022 -standardin päivitysten myötä toimitusketjun tietoturvallisuuden hallinta tulee kehittymään parempaan suuntaan. Tämä johtuu siitä, että organisaatioiden tulee tarkastella tietoturvaa aiempaa laajemmassa kontekstissa, mikä edistää kattavampaa ja syvällisempää tietoturvallisuuden hallintaa. Kolmas vastaus puolestaan kertoo, että päivitykset formalisoivat käytäntöjä, jotka ovat jo pitkälti käytössä. Tämä tarkoittaa, että päivitykset vahvistavat olemassa olevia tietoturvatoimenpiteitä ja auttavat standardoimaan käytäntöjä.

Kun kysyttiin standardin merkittävimmästä uudistuksesta, vastaajilta saatiin kolme erilaista näkökulmaa, jotka valaisevat uudistusten vaikutuksia ja merkitystä. Ensimmäinen näkökulma korostaa, että merkittävin uudistus on vaatimus hallita hallintajärjestelmää koskevat muutokset. Tämä uudistus edellyttää, että organisaatiot ottavat huomioon ja hallitsevat järjestelmällisesti hallintajärjestelmän muutoksia, josta kerrottiin aiemmin tämän tutkimuksen luvussa 7.2. Toinen vastaus korostaa sidosryhmien tarpeiden ja odotusten määrittelyn tärkeyttä. Nämä vastaukset ovat yhdenmukaisia alan muiden ammattilaisten kanssa, jotka pitävät tärkeimpinä uudistuksina vaatimusten kohtia 4.2, 6.3 ja 9.3.2, joissa käsitellään mainittuja aiheita. Tämä yhteys korostaa, kuinka kriittistä on ymmärtää ja vastata sidosryhmien odotuksiin. Lisäksi se tuo esiin muutosten suunnittelun olennaisuuden. Kolmas vastaaja kuvailee uudistusta termillä ”must do”, verraten sitä käyttöjärjestelmien versiopäivityksiin. Tämä näkökulma korostaa, että päivitys on välttämätön toimenpide, joka on suoritettava pysyäkseen ajan tasalla tietoturvastandardissa. Tämä kuvastaa standardin päivityksen välttämättömyyttä ja pakollisuutta organisaation tietoturvan ylläpidossa.

Kysymykseen Liite A:n rakenteellisesta muutoksesta ISO/IEC 27001:2022 -standardissa vastausten jakauma on seuraava: kaksi vastaajaa arvioi muutoksen olevan neutraali, kun taas yksi vastaaja pitää sitä erittäin hyödyllisenä, kuten alla oleva kaavio havainnollistaa.



Kuva 8. Liite A:n rakenteellisen muutosten hyödyllisyys

Tämä jakauma voi kertoa useista asioista. Ensinnäkin se, että kaksi vastaajaa suhtautuu muutokseen neutraalisti, saattaa viitata siihen, että he eivät koe muutoksen vaikuttavan merkittävästi tietoturvakäytäntöihinsä tai että muutos ei tuo mukanaan selkeitä etuja, joita he voisivat hyödyntää. Toisaalta yhden vastaajan käsitys muutoksen hyödyllisyydestä korostaa, että joillekin tietoturva-asiantuntijoille uusi rakenne saattaa tarjota merkittäviä etuja, kuten parempaa järjestelmällisyyttä, selkeämpiä prosesseja tai tehokkaampaa tietoturvariskien hallintaa.

Kysyttäessä syitä aiemman kysymyksen vastauksille, yksi vastaaja kertoo, että muutos selkeyttää rakennetta. Toinen vastaaja mainitsee, ettei osaa kommentoida muutosta tarkemmin, painottaen sen sijaan, että tietoturvallisuuden hallintajärjestelmän käytäntö on hänen mielestään keskeisempää kuin standardin yksittäiset rakenteelliset muutokset. Kolmas vastaaja puolestaan vastaa, ettei tunne Liite A:n rakenteellista uudistusta, mikä osoittaa, että kaikki

asiantuntijat eivät välttämättä ole päivitettyjen standardien muutoksista perillä. Nämä vastaukset auttavat myös selittämään aiemman kaavion vastausten jakaumaa.

9.2.3 Siirtymäprosessin haasteet ja riskienhallinta

Kyselytutkimuksessa selvitettiin myös, kuinka merkittäviä toimenpiteitä siirtyminen ISO/IEC 27001:2013 -standardista uusimpaan ISO/IEC 27001:2022 -standardiin vaatii jo sertifioiduilta organisaatioilta. Vastausten perusteella mielipiteet jakautuvat seuraavasti.

Kuva 9. ISO/IEC 27001:2022 -standardin siirtymän toimenpiteiden merkittävyys

Tuloksista voidaan tulkita, että siirtyminen uuteen ISO/IEC 27001:2022 -standardiin vaatii organisaatioilta huomattavaa työtä. Kaksi kolmesta vastaajasta kokee, että siirtymä aiheuttaa melko merkittäviä toimenpiteitä. Yksi vastaajista arvioi siirtymän vaikutukset neutraaleiksi. Nämä vastaukset ovat myös yhtenäisiä opinnäytetyön kahdeksanteen lukuun, jonka sisällöstä voidaan päätellä, että siirtymäprosessi vaatii melko merkittäviä toimenpiteitä organisaatioilta.

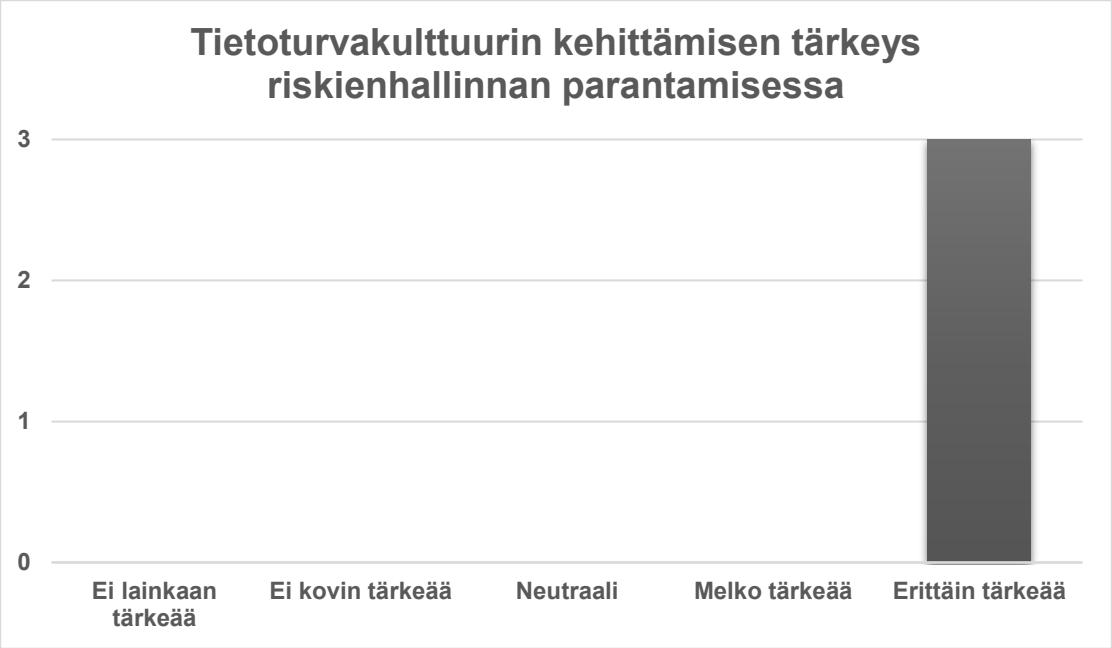
Kysymykseen standardin siirtymäprosessin haasteista vastaajat toivat esiin useita näkökohtia. Yksi vastaajista huomauttaa, että uusien hallintakeinojen käyttöönotto ja omistajuuksien uudelleen määrittely ovat keskeisiä haasteita.

Yhdessä vastauksessa myös mainitaan, että standardin siirtymäprosessi voi olla työläs ja saattaa hetkellisesti ohjata huomion pois muista tietoturvallisuuden kehitystoimista. Kolmas vastaaja mainitsee, että siirtymässä ei ole juuri muita haasteita kuin, että se on aikaa vaativa prosessi. Vastausten perusteella voidaan päätellä, että siirtymä ISO/IEC 27001:2022 -standardiin vaatii melko merkittäviä resursseja ja huolellista suunnittelua jo sertifioiduilta organisaatioilta. Vastauksista myös ilmenee, että prosessi vie paljon aikaa organisaatioilta.

Kysyttäessä, miten organisaatiot voivat osoittaa, että ne ovat toteuttaneet uuden ISO/IEC 27001:2022 -standardin mukaisen riskienhallinnan tehokkaasti, vastaajien antamat vastaukset tarjoavat kattavan näkemyksen tehokkaan riskienhallinnan toteuttamisesta. Vastausten perusteella yksi avainaspekti on riskienhallintaprosessin noudattaminen yhdistettynä tehokkaaseen ja riittävän kattavaan raportointiin. Toinen vastaaja mainitsee, että konkretian merkitys riskienhallinnan tehokkaassa osoittamisessa on äärimmäisen tärkeää. Hänen mielestään, jos riskienhallinta ei ole näkyvä osa päivittäistä toimintaa, se voi viitata siihen, että riskienhallinnan toteuttamisen kynnys tai työmäärä on liian suuri. Hän vielä lisää, että riskienhallinnan tehokkuutta voidaan parantaa tukemalla riskien omistajia tarjoamalla heille ymmärrystä, tukea ja selkeitä rutiineja riskien käsittelyyn. Kyselyn vastauksessa myös mainitaan, että auditoinnin kautta organisaatiot voivat osoittaa, että ne ovat toteuttaneet uuden ISO/IEC 27001:2022 -standardin mukaisen riskienhallinnan tehokkaasti.

9.2.4 Tietoturvakulttuurin kehittäminen ja perehdytys

Kysyttäessä, onko organisaatioiden tietoturvakulttuurin kehittäminen tärkeää riskienhallinnan parantamisessa, kaikki kolme asiantuntijaa vastasivat, että se on erittäin tärkeää. Tämä yksimielisyys korostaa tietoturvakulttuurin keskeistä roolia riskienhallinnan tehokkuudessa. Tätä havainnollistaa myös seuraava kaavio.



Kuva 10. Tietoturvakulttuurin kehittämisen tärkeys riskienhallinnan parantamisessa

Kyselytutkimuksessa myös kysytään, kuinka tärkeänä asiantuntijat pitävät perehdytystä osana organisaatioiden riskienhallintaa. Vastauksien mukaan kaikki asiantuntijat pitävät sitä erittäin tärkeänä. Tämän yksimielisen näkemyksen vahvistaa myös seuraava kaavio.

Kuva 11. Perehdytyksen tärkeys osana organisaatioiden riskienhallintaa

Kyselyn vastauksissa asiantuntijat tuovat esiin useita syitä perehdytyksen tärkeydelle riskienhallinnassa. Asiantuntijat korostavat, että tehokkaan ja vaikuttavan riskienhallinnan saavuttamiseksi on välttämätöntä, että kaikki organisaation työntekijät ymmärtävät miten riskienhallintaprosessi toimii, miksi tiettyjä toimia toteutetaan, sekä mitkä ovat heidän roolinsa ja odotuksensa tietoturvallisessa toimintaympäristössä.

Seuraavassa luvussa syvennytään tarkemmin kolmeen tässä tutkimuksessa korostettuun hallintakeinoon ja niiden vaikutuksiin. Luvussa 11 käsitellään kyselyn johtopäätöksiä yksityiskohtaisemmin.

10 HALLINTAKEINOJEN SUOSITUKSET

Tässä luvussa syvennytään tarkemmin kyselyn vastauksissa mainittuihin hallintakeinoihin, jotka on havaittu tärkeiksi. Alaluvuissa käsitellään seuraavia hallintakeinoja: uhkatiedon seuranta, pilvipalvelujen tietoturvallisuus sekä tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa. Seuraavissa alaluvuissa analysoidaan kunkin hallintakeinon merkitystä, soveltuvuutta ja toteuttamista käytännössä. ISO/IEC 27002:2022 -standardi tarjoaa myös parhaita käytäntöjä ja vaatimuksia kyseisille hallintakeinoille.

10.1 A.5.7 Uhkatiedon seuranta

Hallintakeinon tarkoituksena on varmistaa, että organisaatiot keräävät ja analysoivat aktiivisesti tietoja mahdollisista uhkista. Näin voidaan toteuttaa tarvittavia toimenpiteitä uhkien hallitsemiseksi. Uhkatieto voi sisältää tietoja erilaisista hyökkäystyypeistä, hyökkääjien käyttämistä tekniikoista ja yleisistä hyökkäystrendeistä. Tärkeää on hyödyntää sekä organisaation sisäisiä että ulkoisia tietolähteitä, kuten alan toimittajia ja viranomaisilta saatavia tietoja. (Detailed explanation of 11 new security controls in ISO 27001:2022 s.a.) Saalin (2023) mukaan tämän hallintakeinon lisäys on hyvä parannus nykyisiin käytäntöihin. Tätä tukee myös Nykänen (2022), joka lisää, että 2013-versiossa uhkatiedon vaatimukset eivät olleet näin yksityiskohtaisesti määritelty. Hänen mukaansa aiemmassa versiossa keskityttiin enemmän uhkamallinnukseen sekä hieman toimintaympäristöön liittyvien uhkien varautumiseen.

Pivot Point Securityn (2024a) jakamien kokemuksien mukaan useimmat kolmannen osapuolen tarkastajat näkevät uhkatiedon seurannan vaatimukset kolmen kohdan kautta: haavoittuvuuksien hallinnan, päivitysten hallinnan sekä hälytysten ja seurannan. Tällöin tulee ottaa huomioon uhkien ennakointi, ennakoiva tiedustelu, kyky tunnistaa ja seurata nousevia uhkia sekä tiettyjen uhkien yleistyvyyden tunnistaminen (Pivot Point Security 2024a).

Organisaatioiden on olennaista pitää silmällä omaa toimintaympäristöään sekä sen mukanaan tuomia potentiaalisia uhkia (Nykänen, 2022). Miten tämä toteutetaan, on jätetty kunkin organisaation päätettäväksi. Tavoitteena on hankkia kattava ymmärrys vallitsevista uhkista, jotka voivat vaikuttaa organisaatioon. Tämän prosessin osana on suositeltavaa, että organisaatiot kehittävät tietoturvakäytäntöjään siten, että ne voivat jakaa relevanttia ja organisaation kannalta merkityksellistä uhkatietoa sisäisesti. (Saali 2023.) On myös tärkeää kehittää selkeät prosessit uhkatiedon keräämiseksi ja hyödyntämiseksi. Näiden lisäksi työntekijöiden tietoisuuden lisääminen uhkailmoitusten merkityksestä on avainasemassa. Heidät tulisi kouluttaa siitä, miten ja kenelle uhkatilanteista raportoidaan. (Detailed explanation of 11 new security controls in ISO 27001:2022 s.a.)

Nykänen (2022) kertoo, että A.5.7 hallintakeinossa uhkatieto jaetaan kolmelle eri tasolle: strategiselle, taktiselle ja operationaaliselle tasolle. ISO/IEC 27002 -standardin (2022) mukaan operationaalisten uhkien seuranta keskittyy tarkastelemaan yksityiskohtaisesti erilaisia hyökkäystapoja ja erityisesti sitä, miten nämä hyökkäykset voidaan tunnistaa. Operatiivinen uhkatieto on hyödyllistä etenkin lyhyellä ja keskipitkällä aikavälillä torjuakseen kyberhyökkäyksiä (Flare 2023). Nykänen (2022) täsmentää, että esimerkiksi IOC:n tyyppinen tekninen havainnointi uhkien suhteen sijoittuu operationaaliseen tasoon. IOC-havainnot sisältävät erilaisia merkkejä, jotka viittaavat mahdolliseen tietoturvauhkaan. Näitä ovat esimerkiksi verkkoliikenteen poikkeavuudet, epätavalliset kirjautumisyritykset, järjestelmäasetusten ja tilien käyttöoikeuksien muutokset, epätavalliset DNS-pyynnöt, odottamattomat ohjelmistoasennukset, sekä toistuvat pyynnöt samalle tiedostolle. Nämä indikaattorit voidaan tunnistaa valvomalla jatkuvasti organisaation digitaalisia järjestelmiä. Tietoturva-asi-

antuntijat voivat käyttää tietoturvainformaation ja -tapahtumien hallintajärjestelmää (SIEM) sekä havaitsemis- ja reagointiratkaisuja (XDR), jotka hyödyntävät tekoälyä ja koneoppimista. Myös organisaation muut työntekijät voivat auttaa tunnistamaan epäilyttäviä toimintoja, kuten haitallisia sähköposteja. (Microsoft s.a.)

Taktisten uhkien seuranta keskittyy keräämään tietoa siitä, mitä menetelmiä, työkaluja ja teknologioita hyökkääjät käytävät (ISO/IEC 27002: 2022). Tämä tiedonkeruu on suunnattu ensisijaisesti teknisille asiantuntijoille, ja se auttaa heitä ymmärtämään, kuinka heidän verkkonsa saattaa olla hyökkäysten kohteena käyttäen hyökkääjien uusimpia menetelmiä. Taktinen uhkatieto sisältää myös IOC:ta, kuten IP-osoitteita, URL-osoitteita ja järjestelmälokeja, joita käytetään tulevien tietomurtojen havaitsemiseen. (DNSstuff 2020.) Taktinen uhkatiedustelu on erityisen hyödyllistä lyhyen aikavälin tietojen tarjoamisessa organisaatiolle (SecurityScorecard 2023).

Strateginen uhkatieto tarjoaa korkean tason tiedustelutietoa maailmanlaajuisesta uhkamaisemasta ja organisaation asemasta siinä. Strateginen uhkatieto tarjoaa päätöksentekijöille, kuten toimitusjohtajille ja muille johtajille, käsityksen heidän organisaationsa kohtaamista kyberuhkista. Tämä auttaa johtoa ymmärtämään paremmin, millaisia kyberuhkia heidän organisaationsa mahdollisesti kohtaa. Strateginen uhkatieto käsittelee muun muassa globaaleja geopoliittisia tilanteita, kyberturvallisuuden trendejä tietyillä toimialoilla, sekä syitä ja tapoja, joilla organisaation omaisuuserät saattavat joutua hyökkäyksen kohteeksi. Organisaation sidosryhmät hyödyntävät tätä tietoa yhdistääkseen organisaation laajemmat riskienhallintatoimet ja investoinnit kyberuhkien torjuntaan, jotta voidaan ennaltaehkäistä tulevia uhkia ja varmistaa organisaation turvallisuus. (IBM s.a.) Voutilainen & Kari (2020, 3) laajentaa strategista uhkatiedustelua kuvailemalla, että strateginen kyberuhkatiedustelu tarjoaa kattavaa ja pitkävälin näkemystä uhkaympäristöön, joka voi auttaa organisaatioita ymmärtämään ja hallitsemaan tulevia riskejä tehokkaammin. He mainitsevat samalla, että tekoälyä ja koneoppimista voidaan ottaa käyttöön strategisessa kyberuhkatiedustelussa. Heidän mukaansa tekoälyyn perustuvat työkalut voivat

auttaa analysoimaan suuria tietomääriä nopeammin ja tehokkaammin kuin ihmiset yksinään. (Voutilainen & Kari 2020, 3.) Strateginen uhkatiedustelu on hyödyllistä pitkän aikavälin näkökulmasta (SecurityScorecard 2023).

Loppu luku perustuu IBM:n (s.a.) sivustolla olevaan aineistoon. Uhan tiedustelun elinkaari kuvaa prosessia, jossa tietoturvatiimit tuottavat, jakavat ja jatkuvasti parantavat uhkatietojaan. Vaikka yksityiskohdat voivat vaihdella organisaatiosta toiseen, useimmat noudattavat jonkinlaista seuraavaa kuusivaiheista prosessia:

Taulukko 7. Uhkatietoelinkaaren vaiheet (IBM s.a.)

Vaihe	Kuvaus
Suunnittelu	Tarpeiden ja vaatimusten määrittäminen yhteistyössä sidosryhmien kanssa.
Uhkatiedon kerääminen	Raakatiedon kerääminen eri lähteistä vastaamaan sidosryhmien kysymyksiin.
Käsittely	Tiedon standardointi ja yhdistäminen analyysin helpottamiseksi.
Analyysi	Trendien ja mallien tunnistaminen ja hyödyllisen uhkatiedon tuottaminen.
Levitys	Analysoitujen tietojen jakaminen ja toimenpiteiden suositteleminen.
Palaute	Saadun palautteen arviointi ja parannusten määrittäminen.

Uhkatietoelinkaaren suunnittelussa tietoturva-analyytikot työskentelevät yhdessä organisaation sidosryhmien, kuten johtajien, IT- sekä tietoturvatiimin jäsenten kanssa asettaakseen tiedustelutarpeet. Nämä sisältävät tyypillisesti tietoturvaa koskevat kysymykset, joihin sidosryhmät haluavat tai tarvitsevat vastauksia. Esimerkiksi tietoturvajohtaja saattaa haluta tietää, vaikuttaako uusi kiristyshaittaohjelma organisaatioon.

Tämän jälkeen tietoturvatiimi kerää raakadataa, joka voi auttaa vastaamaan sidosryhmien kysymyksiin. Esimerkiksi, jos tiimi tutkii uutta kiristyshaittaohjelmaa, se voi kerätä tietoa kyseisen haittaohjelmaryhmän taustoista, heidän aiemmin kohteekseen ottamistaan organisaatioista ja hyökkäyskeinoista, joita he ovat hyödyntäneet aiemmissa iskuissaan. Uhkatietoja voidaan kerätä monista lähteistä, kuten uhkatietosyötteistä, tietoturvafoorumeista sekä sisäisistä turvallisuuslokeista.

Uhkatiedon keräämisen jälkeen analyytikot kokoavat, standardoivat ja yhdistävät keräämänsä raakadatan helpottaakseen analyysiä. Tämä prosessi voi pitää sisällään virheellisten hälytysten karsimista tai uhkatiedon soveltamista erilaisiin analyysikehyksiin, kuten MITRE ATT&CK-malliin, joka liittyy aiempiin turvallisuuspoikkeamiin. Monet uhkatiedustelutyökalut automatisoivat tämän käsittelyvaiheen käyttämällä tekoälyä ja koneoppimista. Nämä työkalut yhdistävät uhkatietoja useista eri lähteistä ja tunnistavat alkuvaiheessa datassa ilmeneviä trendejä ja kaavoja.

Analyysivaiheessa raakauhkadatasta tulee todellista uhkatietoa. Tässä vaiheessa analyytikot testaavat ja vahvistavat havaitsemiaan suuntauksia ja malleja, joita he voivat käyttää vastatakseen sidosryhmien turvallisuusvaatimuksiin. Analyysin jälkeen tietoturvatiimi jakaa havaintonsa ja suositukset asianmukaisille sidosryhmille. Toimenpiteitä voidaan toteuttaa näiden suositusten perusteella.

Lopuksi sidosryhmät ja analyytikot arvioivat uusimman uhkatiedustelukierroksen tuloksia ja määrittävät, täyttikö se asetetut vaatimukset. Mahdolliset uudet kysymykset tai tunnistetut tiedon puutteet ohjaavat seuraavaa kierrosta.

Näin ollen voidaan päätellä, että kyseinen elinkaariajattelu mahdollistaa tietoturvatiimien ennakoivan potentiaalisia tulevia haasteita vastaan ja voi mahdollistaa reagoimaan tunnettuihin uhkiin. Tämä ennakoiva lähestymistapa on keskeinen osa riskienhallintaa ja tietoturvan parantamista, mikä on suoraan linjassa ISO/IEC 27001:2022 -standardin kanssa.

10.2 A.5.23 Pilvipalvelujen tietoturvallisuus

Kyseessä on ennaltaehkäisevä hallintakeino, jonka tarkoituksena on hallita ja määritellä pilvipalveluiden käytön tietoturvallisuutta (ISO/IEC 27002: 2022). Tämä hallintakeino keskittyy pilvipalvelujen parantamiseen asettamalla niille tietyt turvallisuusvaatimukset. Tavoitteena on varmistaa, että organisaatiot käyttävät pilvipalveluita turvallisesti alusta loppuun. Tämä pitää sisällän palvelun valinnan, käytön, ylläpidon sekä käytöstä poistamisen. Vaikka monet pilvipalvelut tarjoavat jo turvallisuusominaisuuksia, joskus voi olla tarpeen jopa vaihtaa palveluntarjoajaa, mikäli nykyinen ei täytä vaadittavia turvallisuusstandardeja. (Detailed explanation of 11 new security controls in ISO 27001:2022 s.a.)

Pilvipalveluiden tietoturvallisuuden hallinnassa korostuu organisaation tarpeiden jatkuva arviointi ja elinkaaren hallinta. Tämä tarkoittaa, ettei pilvipalveluiden käyttöönotto ole vain yksittäinen tapahtuma vaan prosessi, joka vaatii säännöllistä tarkastelua ja mukauttamista organisaation muuttuviin tarpeisiin. Tämä prosessi käsittää tarpeiden määrittelyn, palvelun valinnan, sen integroinnin nykyisiin järjestelmiin, ylläpidon, seurannan ja jatkuvan kehittämisen. Tietoturvaa tulee siis päivittää ja ylläpitää koko pilvipalvelun elinkaaren ajan. (Saali 2023.)

SFS-webinaarin mukaan A.5.23 hallintakeino liittyy läheisesti ISO/IEC 27017 -standardiin, joka auttaa organisaatioita tunnistamaan pilvipalveluiden käyttöön liittyvät tietoturvallisuuden vaatimukset, hallinnoimaan pilvipalveluihin liittyviä tietoturvariskejä sekä määrittelemään pilvipalveluiden käytölle asetettavat edellytykset. ISO/IEC 27017 -standardi (2015) tarjoaa erityistä ohjeistusta pilvipalveluiden turvallisuuden hallintaan. Tämä hallintakeino ei SFS:n mukaan yleensä aiheuta suuria ongelmia organisaatoille, mutta on tärkeää tunnistaa ne erikoisuudet, jotka liittyvät pilvipalveluiden turvallisuuteen. (Nykänen 2022.)

Organisaatioiden tulee kehittää prosesseja, jotka määrittelevät miten pilvipalveluiden turvallisuusvaatimukset asetetaan ja miten palveluntarjoajat valitaan. Työntekijöiden tietoisuuden lisääminen ja kouluttaminen pilvipalveluiden tur-

vallisuusriskeistä ja niiden hallinnasta on myös avainasemassa. (Detailed explanation of 11 new security controls in ISO 27001:2022 s.a.) Pilvipalveluiden käyttö voi sisältää jaetun vastuun tietoturvasta ja yhteistyön pilvipalvelutarjoajan ja pilvipalvelun asiakasorganisaation välillä. On olennaista, että molempien vastuut määritellään ja toteutetaan asianmukaisesti. ISO/IEC 27017:2015 sisältää tietoa tietoturvasta ja julkisista pilvipalveluista. Henkilötietojen suojaukseen julkisissa pilvissä liittyvät erityspiirteet on kuvattu standardissa ISO/IEC 27018:2019. (Ahmed 2023.)

Organisaatioiden tulee luoda selkeät politiikat pilvipalveluiden käyttöön, määritellä tietoturvariskien hallintatavat ja viestiä kohdennetut toimintaperiaatteet sidosryhmille. Pilvipalveluiden käyttöprosessit, kuten hankinta, käyttö, hallinta ja lopettaminen tulee suunnitella organisaation tietoturvavaatimusten mukaisesti. Vastuiden selkeä määrittely ja niiden asianmukainen toteuttaminen pilvipalvelun tarjoajan ja pilvipalvelun asiakkaan kesken on tärkeää. (ISO/IEC 27002: 2022.)

ISO/IEC 27002 (2022) kuvailee kattavasti mitä hallintakeinossa organisaation olisi määriteltävä ja tehtävä kyseisessä hallintakeinossa. A.5.23 hallintakeinossa organisaatioiden on muun muassa käytävä läpi jokaisen pilvipalvelujen pilvipalvelusopimukset palvelun tuottajien kanssa. Kyseisissä pilvipalvelusopimuksissa käydään esimerkiksi CIA-mallin mukaisia asioita sekä tietojen käsittelyyn liittyviä vaatimuksia. Organisaatioiden on myös tunnistettava pilvipalvelun käyttöön liittyviä riskejä. Standardissa käydään myös läpi, mitä kaikkea pilvipalvelun tuottajan ja pilvipalvelun asiakkaana toimivan organisaation sopimus tulee pitää sisällään. Näitä ovat esimerkiksi haittaohjelmien torjumiseen, organisaatioiden arkaluonteiseen tietoihin sekä tietoturvavaatimuksiin liittyvät asiat.

ENISA:n (2023) raportti huomauttaa, että palvelujen sekä datan jatkuva ja väistämätön siirtyminen pilveen vaatii tarkkaa harkintaa pilvessä tapahtuvien tietovuotohyökkäysten suhteen. Raportin mukaan pilvipalvelujen virheellinen konfigurointi on yksi merkittävimmistä syistä tietovuodoille.

10.3 A.5.30 Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa

Tässä hallintakeinossa organisaatioiden tulee suunnitella, ylläpitää, testata ja toteuttaa tieto- ja viestintätekniikan valmiuksia (ISO/IEC 27001: 2022). ISO/IEC 27001:2022 -standardissa tämä hallintakeino on määritelty selkeämmäksi kokonaisuudeksi (Nykänen 2022). Tämän hallintakeinon tavoitteena on varmistaa, että yrityksen tieto- ja viestintäteknologia on aina valmis kohtaamaan mahdolliset häiriöt, jotta kriittiset tiedot ja resurssit ovat käytettävissä, kun niitä eniten tarvitaan (Detailed explanation of 11 new security controls in ISO 27001:2022 s.a.).

Tämä hallintakeino on osa laajempaa, yleistä vaatimustasoa ICT-järjestelmien hallinnassa. SFS:n mukaan on siis tärkeää huolellisesti pohtia, kuinka erilaisten tietojen ja omaisuuserien saatavuus voidaan taata häiriötilanteissa. On olennaista määrittää, kuinka nopeasti organisaation tulisi pystyä palauttamaan toimintansa häiriötilanteen jälkeen. Lisäksi tulee tunnistaa ne järjestelmät, jotka ovat ensisijaisesti palautettava häiriötilanteessa. (Nykänen 2022.) On keskeistä ymmärtää, että uusi A.5.30 hallintakeino linkittyy suoraan liiketoiminnan ja sen jatkuvuuden suunnitteluun. Tässä tietoturvan jatkuvuus integroidaan osaksi laajempaa liiketoiminnan kontekstia. Tämä tarkoittaa, että tietoturvan tarpeet ja vaatimukset määrittyvät liiketoiminnan ja sen sidosryhmien kautta. Tämä auttaa varmistamaan, että tietoturvasuunnittelu heijastaa todellisia liiketoiminnan ja sen sidosryhmien tarpeita. Tämä vähentää riskiä siitä, että tietoturvatoimet ovat liiketoiminnan kannalta irrelevantteja tai riittämättömiä. (Saali 2023.)

Kyseinen hallintakeino on erityisen tärkeä, jos organisaatio ei ole investoinut ratkaisuihin, jotka mahdollistavat järjestelmien palautuvuuden ja redundanssin. On olennaista kehittää prosesseja teknologian jatkuvaan ylläpitoon sekä menettelyjä katastrofien jälkeiseen palautumiseen ja liiketoiminnan jatkuvuuden suunnitelmien testaamiseen. On keskeistä tiedottaa työntekijöitä potentiaalisista häiriöistä ja kouluttaa heitä ylläpitämään ja valmistautumaan ICT-häiriöihin, jotta liiketoiminta voi jatkua sujuvasti. (Detailed explanation of 11 new security controls in ISO 27001:2022 s.a.)

Uudessa A.5.30 hallintakeinossa on samankaltaisuuksia ISO/IEC 27001:2013 -standardin A.17 hallintakeinon kanssa. Uusi hallintakeino on kuitenkin hieman erilainen ja tarjoaa määritellymmän yhteyden tietoturvan ja laajemman liiketoiminnan välillä. (Morrison 2023b.) Morrisonin mukaan ei ole yhtä kaikille sopivaa lähestymistapaa, vaan organisaatiot voivat ottaa käyttöön liiketoiminnan jatkuvuuden lähestymistavan, joka sopii heidän liiketoimintaansa. Liiketoiminnan vaikutusanalyysi (BIA) on tämän prosessin kriittisin osa, jota usein laiminlyödään organisaatioissa. On välttämätöntä tunnistaa yrityksen kriittiset toiminnot. Tämän jälkeen on tärkeää varmistaa, että organisaatiolla on riittävät kyvyt toimintojen nopeaan palauttamiseen, erityisesti niissä liiketoimintaprosesseissa, jotka ovat alttiita suurille saatavuusriskeille. Tällöin on olennaista, että organisaatiot laativat ja priorisoivat jatkuvuussuunnitelmat näille kriittisille prosesseille. (Morrison 2023b.)

Liiketoiminnan vaikutusanalyysi on keskeinen osa yrityksen häiriöitilanteiden hallintaa. BIA:n tuloksena muodostetaan kaksi keskeistä tavoitetta: palautumisaikatavoite (RTO) ja palautuspistetavoite (RPO), jotka ovat elintärkeitä yrityksen toipumiskyvylle häiriöitilanteissa. RTO määrittää sen enimmäisaikajänteen, jonka liiketoimintaprosessi voi olla keskeytyneenä ilman merkittäviä haittavaikutuksia yritykselle. Sen määrittäminen vaatii ymmärrystä siitä, kuinka kriittinen kyseinen järjestelmä on liiketoiminnan kannalta. RTO:n asettaminen edellyttää investointeja teknologiaan, prosesseihin ja henkilöstöön, jotta liiketoiminta voi jatkua mahdollisimman vähin häiriöin. Palautuspistetavoite keskittyy tietohävikin hallintaan häiriötilanteessa. Se määrittää maksimaalisen sallitun datan menetyksen, jonka yritys voi kestää ilman vakavia seurauksia. RPO on erityisen tärkeä tietointensiivisille yrityksille, joissa datan menetys voi johtaa merkittäviin liiketoiminnallisiin ja taloudellisiin seurauksiin. RPO määrittää, kuinka usein dataa tulisi varmuuskopioida ja kuinka kauan yritys voi sietää menettää dataa ilman, että se vaikuttaa liiketoimintaan kriittisesti. (Morrison 2023b.)

11 TULOKSET

Opinnäytetyön tarkoituksena oli syventyä ISO/IEC 27001:2022 -standardin aiheuttamiin muutoksiin ja tarjota Elisa Oyj:lle suosituksia, jotka edistävät sen

tietoturvallisuuden kehitystä ja tukevat siirtymää uuteen standardiin. Tutkimuskysymyksiin vastaaminen osoittautui suoraviivaiseksi, mikä johtui selkeästi määritellyistä tavoitteista. Opinnäytetyön tavoitteena oli selvittää, mitkä ovat keskeisimmät erot ISO/IEC 27001:2013- ja ISO/IEC 27001:2022 -standardien välillä, mitä organisaatioiden tulee ottaa huomioon siirtymäprosessissa sekä mitä muutoksia organisaatioiden tulee huomioida uuden standardin vaatimusten täyttämiseksi.

11.1 Tutkimuskysymyksistä johdetut tulokset

Onnistunut siirtymäprosessi uusimpaan standardiin vaatii suunnitelmaa, jota on hyvä lähestyä järjestelmällisesti vaihe vaiheelta (taulukko 6). On siis oleellista ymmärtää, mitä siirtymäprosessi pitää sisällään. Organisaatioiden on hyvä pitää mielessä siirtymäaikataulu (kuva 4) sekä vaihtoehdot siirtymätarkastuksen suorittamiselle. Siirtymätarkastus voidaan suorittaa samanaikaisesti valvontatarkastuksen, uusintatarkastuksen tai erillisen tarkastuksen yhteydessä. Siirtymätarkastuksen kannalta kriittisin ajankohta on 31.10.2025, sillä sen jälkeen ISO/IEC 27001:2013 -version voimassaolo päättyy. Organisaatioiden on hyvä pitää myös mielessä, mitä siirtymätarkastuksessa käydään läpi (taulukko 5). Siirtymäprosessi nähdään myös aikaa vievänä, sillä kyselytutkimuksessa kaksi kolmesta vastaajasta kokee, että siirtymä aiheuttaa melko merkittäviä toimenpiteitä. Yksi vastaajista arvioi siirtymän vaikutukset neutraaleiksi. Avoimissa kysymyksissä kaksi kolmesta myös mainitsi, että siirtymäprosessi on aikaa vievä prosessi.

Jotta siirtymäprosessi voisi onnistua, organisaatioiden tulee ymmärtää ISO/IEC 27001:2013- ja ISO/IEC 27001:2022 -standardien keskeiset eroavaisuudet. Vaatimusosion kohdat 4–10 ovat pysyneet suurimmalta osin samankaltaisina. Vaatimusosion muutokset koostuvat pienistä sanamuutoksista, täydennyksistä, tarkennuksista sekä useammasta lisäyksestä (taulukko 1).

Opinnäytetyön luvussa 7.2 käytyjen uusien vaatimusten vaikutusten lisäksi kyselytutkimuksessa asiantuntijoilta kysyttiin, että mitkä heidän mielestään ovat standardin merkittävimmät uudistukset. Seuraava taulukko havainnollistaa asiantuntijoiden vastauksia.

Taulukko 8. Asiantuntijakyselyn tulokset merkittävimmistä päivityksistä

Merkittävin uudistus	Selitys
Vaatimus 6.3	• Asiantuntija näki merkittävimpänä uudistuksena hallita ISMS koskevia muutoksia.
Sidosryhmien tarpeet	• Toinen vastaaja koki merkittävimpänä sidosryhmien tarpeiden ja odotusten määrittämisen.
-	• Kolmas vastaaja näki standardin päivityksen välttämättömänä toimenpiteenä, joka on suoritettava pysyäkseen ajan tasalla tietoturvastandardissa.

Vaatimusten lisäksi standardin Liite A on kokenut muutoksia. Niistä oleellisimpia ovat 14 hallintoaluetavoitteen muuttaminen 4 hallintateemaan, 57 hallintakeinon yhdistäminen 24 hallintakeinoon sekä 11 uutta hallintakeinoa (taulukko 2). Kyselytutkimuksessa asiantuntijat näkivät uhkatiedon seurannan (A.5.7), pilvipalvelujen tietoturvallisuuden (A.5.23) ja tieto- ja viestintätekniikan valmiuden liiketoiminnan suunnittelussa (A.5.30) tärkeimmiksi uusiksi hallintakeinoiksi (kuva 7). Alla oleva taulukko havainnollistaa keskeiset havainnot näistä hallintakeinoista.

Taulukko 9. Asiantuntijakyselyssä mainittujen hallintakeinojen keskeiset vaikutukset

Hallintakeino	Vaikutukset
Uhkatiedon seuranta (A.5.7)	• Jakautuu strategiselle, taktiselle ja operationaaliselle tasolle. • Tarkoituksena varmistaa, että organisaatiot keräävät ja analysoivat aktiivisesti tietoja mahdollisista uhista. • Tarkoituksena toteuttaa toimenpiteitä uhkien hallitsemiseksi. • Uhkatieto voi sisältää tietoa hyökkäystyypeistä, hyökkääjien käyttämistä tekniikoista ja yleisistä hyökkäystrendeistä. • Tärkeää hyödyntää sisäisiä ja ulkoisia tietolähteitä. • Haavoittuvuuksien hallinta, päivitysten hallinta ja hälytysten ja seuranta ovat tärkeitä elementtejä tässä hallintakeinossa. • Uhkatiedon jakaminen sisäisesti.
Pilvipalvelujen tietoturvallisuus (A.5.23)	• Ehkäisevä hallintakeino. • Tarkoituksena hallita ja määritellä pilvipalveluiden käytön tietoturvallisuutta. • Tavoitteena varmistaa, että organisaatiot käyttävät pilvipalveluita turvallisesti alusta loppuun. • Pitää sisällään palvelun valinnan, käytön, ylläpidon sekä käytöstä poistamisen. • Tarpeiden jatkuva arviointi ja elinkaari korostuvat tämän hallintakeinoa hallinnassa. • Tietoturvaa tulee päivittää ja ylläpitää koko pilvipalvelun elinkaaren ajan. • Liittyy läheisesti ISO/IEC 27017 -standardiin. • Tarvitaan selkeät politiikat pilvipalveluiden käyttöön • Määriteltävä tietoturvariskien hallintatavat
Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa (A.5.30)	• Tavoitteena varmistetaan organisaation valmius kohtaamaan mahdollisia häiriöitä. • Varmistetaan kriittisten tietojen ja resurssien saatavuus. • Organisaatioiden tulee ylläpitää, suunnitella, testata ja toteuttaa tietoa- ja viestintätekniikan valmiutta. • Tämä hallintakeino linkittyy suoraan liiketoiminnan ja sen jatkuvuuden suunnitteluun. • Tietoturvan tarpeet ja vaatimukset määrittyvät liiketoiminnan ja sen sidosryhmien kautta. • Vaikutusanalyysin merkitys. • Palautumisaikatavoite ja palautuspistetavoite ovat elintärkeitä yrityksen toipumiskyvylle häiriöitilanteissa.

Organisaatioiden tulee siis arvioida riskejä ja tunnistaa uudesta Liite A:sta ne hallintakeinot, jotka ovat olennaisia riskien hallitsemiseksi. Uudet hallintakeinot

voivat vaatia myös riskien käsittelysuunnitelman päivittämistä. On välttämätöntä myös huolehtia, että organisaatiot päivittävät tietoturvallisuuden hallintajärjestelmänsä vastaamaan uusia vaatimuksia, jotta siirtyminen ISO/IEC 27001:2022 -standardiin on mahdollista. Uusien vaatimusten ja hallintakeinojen keskeiset muutokset sekä niiden vaikutukset ovat käyty läpi opinnäytetyön luvussa 7. Siirtymäprosessissa organisaatioiden on hyvä pitää mielessä myös seuraavat standardit, jotka tukevat siirtymässä uusimpaan ISO/IEC 27001:2022 -standardiin.

Taulukko 10. Standardit, jotka tukevat ISO/IEC 27001:2022 -standardin siirtymää

Standardi	Tehtävä
ISO/IEC 27002:2022	• Tarjoaa kattavan ohjeistuksen hallintakeinojen käytännön toteutuksesta ja valinnasta.
ISO/IEC 27005:2022	• Auttaa riskienhallintaprosessin suunnittelussa, toteutuksessa, ylläpidossa ja jatkuvassa parantamisessa.
ISO/IEC 27017:2015	• Tarjoaa ohjeistusta pilvipalveluiden turvallisuuden hallintaa. Hyödyllinen ISO/IEC 27001:2022 -standardin hallintakeinossa A.5.23.
ISO/IEC 27018:2019	• Suunnattu henkilötietojen suojaamiseen julkisissa pilvipalveluissa. Tukee etenkin ISO/IEC 27001:2022 -standardin hallintakeinossa A.5.23.
ISO 31000:2018	• Tukee ISO/IEC 27001:2022 -standardia riskien arviointi- ja käsittelyprosesseissa.
ISO/IEC 31010:2019	• Tarjoaa ohjeita riskien arviointimenetelmistä.

On hyvä myös muistaa, että Liite A:n hallintakeinoista osa hallintakeinoista ovat yhdistelmiä vanhoista, joten on tärkeää tarkastella kaikkia päivitetyn Liite A:n hallintakeinoja yksitellen. Hallintakeinojen valinnassa ja suunnittelussa kannattaa hyödyntää ISO/IEC 27002:2022 -standardin attribuutteja ja Liite B:tä. Liite B:n avulla nähdään selkeästi, miten uudet ja vanhat hallintakeinot vastaavat toisiaan.

11.2 Johtopäätökset

Tutkimuksen keskeinen kysymys oli, mitä uusia vaatimuksia ja muutoksia Elisan tulee ottaa huomioon ISO/IEC 27001:2022 -standardin siirtymäprosessissa. Tutkimusongelma ratkaistiin käyttämällä monipuolisia aineistonkeruu- ja analyysimenetelmiä, jotka mahdollistivat perusteellisen ymmärryksen aiheesta. Tutkimus hyödynsi sekä laadullisia että määrällisiä menetelmiä, kuten sisällönanalyysiä ja kyselytutkimusta. Nämä menetelmät tuottivat tärkeää tietoa ja asiantuntijanäkemyksiä, jotka ohjasivat suositeltujen toimenpiteiden kehittämistä.

Tutkimus osoitti, että ISO/IEC 27001:2022 -standardin tuomat uudet vaatimukset ja hallintakeinot vaativat organisaatioilta entistä kokonaisvaltaisempaa lähestymistapaa tietoturvallisuuteen. Standardin noudattaminen on tärkeää digitaalisten teknologioiden ja kyberuhkien nopeasti kehittyvässä maailmassa, missä organisaatioiden kyky hallita potentiaalisia riskejä on kriittinen.

Opinnäytetyön tuloksena syntyi konkreettisia ohjeistuksia ja laaja kattaus asiantuntijanäkemyksiä, jotka tukevat siirtymäprosessia ja auttavat organisaatioita valmistautumaan uusimpaan ISO/IEC 27001:2022 -standardiin. Lisäksi kyselytulokset tarjosivat uusia näkökulmia ja vahvistivat aiemmin havaittuja ilmiöitä.

12 POHDINTA

Opinnäytetyössä tuotettiin laaja-alaista ja merkityksellistä tietoa, joka oli mahdollista kerätyn aineiston laajuuden ja perusteellisen analyysin ansiosta. Tämän ansioista oli mahdollista muodostaa kattavia näkökulmia ja kehittää laadukkaita ohjeistuksia. Mielestäni tutkimusasetelman teoreettinen perustelu, tutkimusosioiden kattavuus ja tutkimuskysymyksiin vastaaminen onnistuivat hyvin, mikä tekee työstä laadukkaan ja selkeän kokonaisuuden.

Opinnäytetyön aikana havaittiin myös kehitettäviä kohtia. Aiheen tarkempi rajaus olisi saattanut mahdollistaa syvällisemmän ja kohdennetumman tiedon

tuottamisen, erityisesti suurille organisaatioille, kuten Elisalle. Vaikka tutkimuksen laaja-alaisuus tarjosi monipuolisen näkemyksen siirtymäprosessista ja ISO/IEC 27001:2022 -standardin muutoksista, aiheen vielä tiiviimpi rajaus olisi voinut lisätä tutkimuksen käytännön soveltuvuutta ja hyödyllisyyttä.

Myös primääriaineiston hankinta olisi myös voitu toteuttaa toisin. Kyselytutkimuksen vastaajamäärän vähäisyys viittaa siihen, että esimerkiksi teemahaastattelut olisivat voineet tarjota syvällisempiä näkemyksiä tutkittavasta aiheesta. Kyselyn valintaan vaikuttivat ajankäytölliset syyt sekä kyselytutkimuksen päätavoite, joka oli selvittää, mitkä hallintakeinot ovat asiantuntijoiden mielestä olennaisimpia. Päätavoitteeseen kysely sopi mielestäni erinomaisesti. Monet kyselytutkimuksen vastaukset myös vahvistivat 7 ja 8 lukujen sekundääriaineistoja. Lähes kaikki tutkimuksen materiaalit perustuivat alan ammattilaisten näkemyksiin, mikä tekee tutkimustuloksista merkityksellisiä.

12.1 Luotettavuus

Opinnäytetyön sekundääri- ja primääriaineisto koostui monipuolisista ja luotettavista lähteistä. Sekundääriaineisto sisälsi standardeja, sertifiointielinten ohjeita, alan tutkimuksia ja webinaareja, yritysten julkaisemia oppaita, raportteja ja kirjallisuutta. Luotettavuutta lisää se, että tutkimuksen perustelut ovat alan ammattilaisten laatimia, jotka työskentelevät ISO/IEC 27001:2022 -standardin parissa. Lähteiden määrä lisää luotettavuutta, koska se mahdollistaa useamman alan ammattilaisen näkemyksen aiheesta.

Vaikka kyselytutkimuksen pieni vastausprosentti heikentää tulosten yleistettävyyttä, tämä ei merkittävästi vaikuttanut tutkimuksen toteutukseen, koska kyselyn tulokset keskittyivät pääasiassa hallintakeinojen rajaukseen luvun 10 tutkimusosiossa. Lisäksi kyselyn vastaukset vertailtiin sekundääriaineiston kanssa, ja tässä vertailussa löytyi useita yhtäläisyyksiä. Tämä korostaa tutkimuksen validiteettia.

Opinnäytetyö tarjoaa erityisesti hyötyä niille organisaatioille, jotka suunnittelevat siirtymistä uuteen ISO/IEC 27001:2022 -standardiin. Tätä tukee myös

opinnäytetyön toimeksiantaja, joka on todennut työn hyödylliseksi heidän sisäisessä ISO/IEC 27001:2022 -standardin siirtymäprojektissa. Toimeksiantajan mukaan tarkat kuvaukset vaatimusten muutoksista, kuten kohdan 7.2 vaatimusten muutokset, olivat arvokkaita. Ne tarjosivat hyvän vertailun ja näkemyksiä, joita hekin voivat hyödyntää. Siirtymäprosessin kuvaus oli heille myös hyödyllinen ja vahvisti heidän näkemyksiään asiasta. Opinnäytetyössä havaittiin useita hyödyllisiä kohtia, jotka vaativat toimeksiantajalta pohtimista, mitä voidaan ottaa käyttöön ja mitkä asiat vaativat muutosta. Toimeksiantajan positiiviset kommentit sekä konkreettiset hyödyt tukevat opinnäytetyön luotettavuutta ja hyödyllisyyttä.

12.2 Tulosten yhteys teoriaan

Tutkimustulokset tukevat teoreettista viitekehystä, joka keskittyy tietoturvan perusperiaatteiden, kuten CIA-kolmikon ymmärtämiseen ja soveltamiseen. CIA-kolmikko on olennainen osa tietoturvan hallintajärjestelmän teoreettista perustaa. ISO/IEC 27001:2022 -standardin mukaisesti toteutettu tietoturvallisuuden hallintajärjestelmä auttaa organisaatioita hallitsemaan riskejä ja varmistamaan tiedon luottamuksellisuuden, eheyden ja saatavuuden. Tutkimustulokset korostavat, että organisaatioiden tulee päivittää tietoturvallisuuden hallintajärjestelmiään vastaamaan uusia ISO/IEC 27001:2022 -standardin vaatimuksia. Tämä käsittää esimerkiksi hallintakeinojen tarkistamisen ja päivittämisen uuden standardin mukaisesti, mikä on välttämätöntä riskien tehokkaalle hallinnalle. Päivitysprosessi edellyttää, että organisaatiot arvioivat olemassa olevia tietoturvakäytäntöjään ja mukauttavat ne uusiempien vaatimusten mukaisiksi, joka varmistaa tietoturvan ajantasaisuuden ja tehokkuuden. Näin ollen tutkimuksen havainnot ovat läheisesti yhteydessä tiedon luottamuksellisuuden, eheyden ja saatavuuden säilymisen kanssa.

Teoreettisessa viitekehyksessä käsitellään myös tietoturvallisuuden hallintajärjestelmää sekä ISO/IEC 27000 -standardisarjaa. Nämä ovat olennainen osa tutkimustuloksia. Tietoturvallisuuden hallintajärjestelmä muodostaa koko opinnäytetyön tulosten perustan. ISO/IEC 27000 -standardisarjan standardeja hyödynnetään tutkimustuloksissa, sillä ne tarjoavat ohjeistusta ja tukea ISO/IEC 27001:2022 -standardin siirtymäprosessissa ja tietoturvallisuuden

hallintajärjestelmän kehittämisessä. Myös teoreettisessa viitekehyksessä mainittu PDCA-malli on erittäin keskeinen osa ISO/IEC 27001:2022 -standardin uutta vaatimusta, joka koskee muutosten suunnittelua. Opinnäytetyössä on todettu, että organisaatioiden tulisi soveltaa sitä kaikissa tilanteissa, joissa tietoturvallisuuden hallintajärjestelmää muutetaan.

Teoriaosiossa käsitellään myös riskienhallintaa ja kyberuhkia. Riskienhallinta on oleellinen osa tutkimistuloksia, sillä organisaatioiden tulee tarkastaa ja päivittää muun muassa riskien arviointi ja -käsittelysuunnitelma standardin siirtymäprosessissa. Sillä tutkimusosiossa käsitellään, kuinka riskien arviointi ja -käsittelysuunnitelmaa tulee tarkastaa ja päivittää standardin siirtymäprosessissa. Muuttuneen Liite A:n takia organisaatioiden tulee uudelleenarvioida hallintakeinojaan, jotka on suunniteltu auttamaan organisaatioita hallitsemaan tietoturvallisuuteen liittyviä riskejä. Teoreettisessa viitekehyksessä käsitellyt kyberuhat ovat olennaisia tutkimuksen kannalta, ja näitä uhkia tarkastellaan syvällisesti uuden hallintakeinon, uhkatiedon seurannan (A.5.7) yhteydessä.

Vaikka CIA-AAA-malli ja Parkerin kuusikko eivät ole suoraan mukana tutkimustuloksissa, ne voivat silti tarjota hyödyllisen viitekehyksen tietoturvallisuuden hallintajärjestelmän kehittämisessä. Soveltamalla näitä malleja voidaan kehittää kattavampia tietoturvakäytäntöjä, jotka tukevat riskienhallintaa ja organisaation tietoturvallisuutta.

12.3 Jatkokehitys

Tutkimuksen aineistonkeruuvaiheessa korostui tietoturvakulttuurin keskeinen rooli työpaikkojen riskienhallinnassa. Esimerkiksi Trim & Lee (2014) Crawley (2022) tuovat esille tietoturvakulttuurin merkityksen työpaikkojen riskienhallinnassa. Vaikka aihe herätti mielenkiintoa ja sen syvempi käsittely olisi tuonut lisäarvoa opinnäytetyöhön, tutkimuksen rajaus pakotti jättämään aiheen tutkimuksen ulkopuolelle. Kyselyssä esitin asiantuntijoille kysymyksiä tietoturvakulttuurin kehittämisen ja perehdytyksen merkityksestä. Kaikki asiantuntijat pitivät näitä aiheita erittäin tärkeinä, mikä korostaa aiheen tärkeyttä. Kuten aiemmin pohdinnassa todettiin, syvällisemmät haastattelut voisivat olla hyvä

tapa kerätä primääriaineistoa tulevissa tutkimuksissa, jolloin saataisiin vielä kattavammin erilaisia näkemyksiä aiheesta.

Tutkimuksen rajauksen seurauksena osa hallintakeinoista jäi laajemman analyysin ulkopuolelle. Tämä osoittaa, että jatkossa on tarpeen keskittyä näihin hallintakeinoihin, jotta voidaan saada kattava kuva niiden vaikutuksista ja soveltuvuudesta organisaation riskienhallinnan vahvistamiseen.

Yhteenvetona opinnäytetyöstä voidaan todeta, että tutkimus osoittaa, että ISO/IEC 27001:2022 -standardi tuo uusia muutoksia, jotka vaativat organisaatioilta resursseja ja huolellista suunnittelua. Tutkimuksen tulokset tarjoavat arvokasta tietoa ja ohjeistusta standardin siirtymäprosessiin, joiden avulla organisaatiot voivat vahvistaa tietoturvallisuuden hallintajärjestelmäänsä ja vastata tehokkaammin uuden standardin vaatimuksiin.

LÄHTEET

Aaltonen, J. 2023. Maailman johtava tietoturvastandardi ISO/IEC 27001 päivittyi: Elmo saavutti vaatimukset ensimmäisenä Suomessa. Verkkolehti. Saatavissa: https://www.sttinfo.fi/tiedote/69996299/maailman-johtava-tietoturvastandardi-isoiec-27001-paivittyi-elmo-saavutti-vaatimukset-ensimmaisena-suomessa?publisherId=69817957 [viitattu 23.4.2024].

Ahmed, H. 2023. A Guide to the Updated ISO/IEC 27002:2022 Standard, Part 1. Artikkeli. Saatavissa: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-7/a-guide-to-the-updated-iso-iec-27002-2022-standard-part-1 [viitattu 25.4.2024].

Armstrong, W. 2023. Transitioning to ISO 27001:2022. How to Best Meet the New Requirements. Blogi. Saatavissa: https://www.urmconsulting.com/blog/transitioning-to-iso-27001-2022 [viitattu 25.4.2024].

Armstrong, W & Harrison, T. 2024. Lessons Learnt from Early ISO 27001:2022 Transitions. Blogi. Saatavissa: https://www.urmconsulting.com/blog/lessons-learnt-from-early-iso-27001-2022-transitions [viitattu 25.4.2024].

Badman, A. 2023. Types of cyberthreats. Blogi. Saatavissa: https://www.ibm.com/blog/types-of-cyberthreats/ [viitattu 1.5.2024].

Barker, S. s.a. ISO 27001 Clause 6.3 Planning of Changes – Ultimate Certification Guide. WWW-dokumentti. Saatavissa: https://hightable.io/iso-27001-clause-6-3-planning-of-changes-new-control/ [viitattu 25.4.2024].

BSI s.a. ISO/IEC 27001 Transition Guide. PDF-dokumentti. Saatavissa: https://www.bsigroup.com/globalassets/localfiles/en-id/iso27001/iso-iec-27001-transition-guide.pdf [viitattu 24.4.2024].

Calder, A. & Gerrard, L. 2013. ISO27001/ISO27002: A Pocket Guide. IT Governance Ltd. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 13.3.2024].

Calder, A. 2023. Webinar | ISO 27001:2022 – Transition Policies and Staff Awareness Training. Videoleike. Saatavissa: https://www.youtube.com/watch?v=Ih6S8dZK-aQ [viitattu 19.4.2024].

Crawley, K. 2022. 8 Steps to Better Security. A Simple Cyber Resilience Guide for Business. New Jersey: John Wiley & Sons.

Detailed explanation of 11 new security controls in ISO 27001:2022. s.a. Advisera. WWW-dokumentti. Saatavissa: https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/ [viitattu 21.4.2024].

Digitalisaatiolla kestävä tulevaisuus. s.a. Elisa Oyj. WWW-dokumentti. Saatavissa: https://elisa.fi/yhtiotieto/ [viitattu 23.4.2024].

Edwards, M. 2024. ISO 27001:2022 Annex A Explained. WWW-dokumentti. Saatavissa: https://www.isms.online/iso-27001/annex-a/ [viitattu 25.4.2024].

ENISA. 2023. ENISA Threat Landscape 2023. PDF-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 [viitattu 27.4.2024].

Flare. 2023. Operational Threat Intelligence: The Definitive Guide. Blogi. Saatavissa: https://flare.io/learn/resources/blog/operational-threat-intelligence [viitattu 25.4.2024].

Fortinet s.a. AAA Security. WWW-dokumentti. Saatavissa: https://www.fortinet.com/resources/cyberglossary/aaa-security [viitattu 24.4.2024].

Gracy, M. 2024. ISO 27001 Gap Analysis: What is it And How to Get Started. Blogi. Saatavissa: https://sprinto.com/blog/iso-27001-gap-analysis/ [viitattu 24.4.2024].

Harvey, A. 2024. The Ultimate Guide to ISO 27002. WWW-dokumentti. Saatavissa: https://www.isms.online/iso-27002/ [viitattu 25.4.2024].

Hashemi-Pour, C. & Chai, W. 2023. CIA triad (confidentiality, integrity and availability). TechTarget. WWW-dokumentti. Saatavissa: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA [viitattu 13.3.2024].

IAS Certification. 2024. ISO 27001:2013 vs. 2022: Exploring Key Differences. WWW-dokumentti. Saatavissa: https://www.iascertification.com/iso-27001-2013-vs-iso-27001-2022-exploring-key-differences/ [viitattu 10.4.2024].

IBM. 2023. Cost of a Data Breach Report 2023. PDF-dokumentti. Saatavissa: https://www.ibm.com/reports/data-breach [viitattu 27.4.2024].

IBM. 2024. X-Force Threat Intelligence Index 2024. PDF-dokumentti. Saatavissa: https://www.ibm.com/reports/threat-intelligence [viitattu 27.4.2024].

IBM s.a. What is threat intelligence? WWW-dokumentti. Saatavissa: https://www.ibm.com/topics/threat-intelligence [viitattu 21.4.2024].

International Accreditation Forum. 2023. Transition Requirements for ISO/IEC 27001:2022. (IAF MD 26:2023). PDF-dokumentti. Saatavissa: https://iaf.nu/iaf_system/uploads/documents/IAF_MD26_Issue_2_15012023.pdf [viitattu 14.4.2024].

ISO 27001 Controls Explained: A Guide to Annex A. s.a. Secureframe. WWW-dokumentti. Saatavissa: https://secureframe.com/hub/iso-27001/controls [viitattu 24.4.2024].

ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide. s.a. Advisera. WWW-dokumentti. Saatavissa: https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/ [viitattu 24.4.2024].

ISO 31000:2018. 2018. Riskienhallinta. Ohjeet. Suomen Standardisoimisliitto SFS.

ISO 31000 – Risk management. s.a. ISO. WWW-dokumentti. Saatavissa: https://www.iso.org/iso-31000-risk-management.html [viitattu 14.3.2024].

ISO/IEC 27000:2020. 2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Suomen Standardisoimisliitto SFS.

ISO/IEC 27001:2013. 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto SFS.

ISO/IEC 27001:2022. 2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmän vaatimukset. Suomen Standardisoimisliitto SFS.

ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection. Information security management systems. Requirements. s.a. ISO. WWW-dokumentti. Saatavissa: https://www.iso.org/standard/27001 [viitattu 14.4.2024].

ISO/IEC 27002:2022. 2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Suomen Standardisoimisliitto SFS.

ISO/IEC 27005:2022. 2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Ohjeita tietoturvariskien hallintaan. Suomen Standardisoimisliitto SFS.

ISO/IEC 27017:2021. 2021. Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015). Suomen Standardisoimisliitto SFS.

ISO/IEC 27018:2020. 2020. Informaatioteknologia. Turvallisuustekniikat. Menettelyohjeet henkilötietojen suojaamiseen henkilötietoja käsittelevissä julkisissa pilvipalveluissa. Suomen Standardisoimisliitto SFS.

ISO/IEC 31010:2019. 2019. Riskienhallinta. Riskien arviointimenetelmät. Suomen Standardisoimisliitto SFS.

ISO/IEC CD 27028 – Information security, cyber security and privacy protection. s.a. ISO. WWW-dokumentti. Saatavissa: https://www.iso.org/standard/61007.html [viitattu 29.4.2024].

IT Governance Ltd. 2013. Comparing ISO 27001:2005 to ISO 27001:2013. PDF-dokumentti. Saatavissa: https://www.itgovernance.co.uk/download/27001-update-reference-sheet.pdf [viitattu 18.3.2024].

Jakkal, V. 2022. Cybersecurity threats are always changing---staying on top of them is vital, getting ahead of them is paramount. Blogi. Saatavissa: https://www.microsoft.com/en-us/security/blog/2022/02/09/cybersecurity-

threats-are-always-changing-staying-on-top-of-them-is-vital-getting-ahead-of-them-is-paramount/ [viitattu 11.4.2024].

Juhila, K. s.a. Laadullinen tutkimus ja teoria. Tietoarkisto. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/laadullinen-tutkimus-ja-teoria/ [viitattu 18.3.2024].

Kananen, J. 2014a. Verkkotutkimus opinnäytetyönä. Laadullisen ja määrällisen verkkotutkimuksen opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2014b. Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona. Opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kiwa Inspecta. 2023a. Key Changes to ISO/IEC 27001:2022. WWW-dokumentti. Saatavissa: https://www.kiwa.com/en/media/news/2023/changes--to-isoiec-270012022/ [viitattu 23.4.2024].

Kiwa Inspecta. 2023b. Uusi standardiversio ISO/IEC 27001:2022 – Kiwa Inspecta palveluksessasi. WWW-dokumentti. Saatavissa: https://www.kiwa.com/fi/fi/uutiset/uusi-standardiversio-isoiec-270012022-kiwa-inspecta-palveluksessasi/ [viitattu 24.4.2024].

Kosling, K. 2024. A Guide to Transitioning to ISO 27001:2022. Blogi. Saatavissa: https://www.itgovernanceusa.com/blog/what-you-need-to-know-about-iso-270012022 [viitattu 25.4.2024].

Kosutic, D. 2022. ISO 27001 2013 vs. 2022 revision – What has changed? Blogi. Saatavissa: https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/ [viitattu 1.5.2024].

Lahnalahti, J. 2022. Uudistetut tietoturvallisuuden hallintakeinot standardissa ISO/IEC 27002:2022. Käyttö ja vaikutukset arviointeihin. Videoleike. Saatavissa: https://sfs.fi/tietoturvallisuuden-hallintakeinojen-standardi-on-uudistettu-mita-on-muuttunut/ [viitattu 24.4.2024].

Lindgren, S. 2016. 5 vinkkiä kyselyidesi vastausprosentin kasvattamiseen. Blogi. Saatavissa: https://surveypal.fi/blogi/5-vinkkia-kyselyidesi-vastausprosentin-kasvattamiseen/ [viitattu 28.4.2024].

Lähdesmäki, T., Hurme, P., Koskimaa, R., Mikkola, L., Himberg, T. 2009. Kohteen tulkinta. Menetelmäpolkuja humanisteille. Jyväskylän yliopisto, humanistinen tiedekunta. WWW-dokumentti. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/ongelmanasettelu/kohteen-tulkitseminen [viitattu 13.4.2024].

Lähdesmäki, T., Hurme, P., Koskimaa, R., Mikkola, L., Himberg, T. 2015. Määrällinen Tutkimus. Menetelmäpolkuja humanisteille. Jyväskylän yliopisto,

humanistinen tiedekunta. WWW-dokumentti. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimus-strategiat/maarallinen-tutkimus [viitattu 13.4.2024].

Manimbo, D. s.a. What are the “Attributes” in ISO 27002? Blogi. Saatavissa: https://www.schellman.com/blog/iso-certifications/iso-27002-attributes [viitattu 29.4.2024].

Microsoft s.a. What are indicators of compromise (IOCs)? WWW-dokumentti. Saatavissa: https://www.microsoft.com/en-us/security/business/security-101/what-are-indicators-of-compromise-ioc [viitattu 21.4.2024].

Morrison, D. 2023a. ISO 27001:2022 Changes. What changed between the 2013 and 2022 versions? WWW-dokumentti. Saatavissa: https://morrisec.com.au/iso-27001-2022-changes/ [viitattu 25.4.2024].

Morrison, D. 2023b. ISO 27001:2022 – 5.30 ICT Readiness for Business Continuity. How to develop cyber resilience for your business. WWW-dokumentti. Saatavissa: https://morrisec.com.au/iso-27001-2022-5-3-ict-readiness-business-continuity/ [viitattu 25.4.2024].

Mäki-Maukola, E. 2023. ISO 27000 -tietoturvastandardisarja osana nykypäivän yritysten tietoturvallisuuden hallintaa. Jyväskylän yliopisto. Kyberturvallisuus. Pro gradu -tutkielma. WWW-dokumentti. Saatavissa: http://urn.fi/URN:NBN:fi:jyu-202302211818 [viitattu 12.3.2024].

NIST s.a. Cyber Threat. WWW-dokumentti. Saatavissa: https://csrc.nist.gov/glossary/term/cyber_threat [viitattu 1.5.2024].

NQA s.a. ISO 27001:2022 Transition Guidance for Clients. WWW-dokumentti. Saatavissa: https://www.nqa.com/en-gb/transitions/iso-27001-2022 [viitattu 24.4.2024].

Nykänen, R. 2022. Uusi ISO/IEC 27002 – mitä on muuttunut? Videoleike. Saatavissa: https://sfs.fi/tietoturvallisuuden-hallintakeinojen-standardi-on-uudistettu-mita-on-muuttunut/ [viitattu 21.4.2024].

PECB. 2023. ISO/IEC 27001:2022 Transition. WWW-dokumentti. Saatavissa: https://pecb.com/whitepaper/isoiec-270012022-transition [viitattu 25.4.2024].

PECB. 2024. ISO/IEC 27001 - What are the main changes in 2022? Artikkeli. Saatavissa: https://pecb.com/article/isoiec-27001---what-are-the-main-changes-in-2022 [viitattu 1.5.2024].

Pender-Bey, G. s.a. The Parkerian Hexad. The CIA Triad Model Expanded. PDF-dokumentti. Saatavissa: https://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf [viitattu 24.4.2024].

Pinnell, T. s.a. ISO 27002:2022 – A guide to the changes. PDF-dokumentti. Saatavissa: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-Webinar-A-guide-to-the-changes-to-ISO-27002.pdf [viitattu 29.4.2024].

Pivot Point Security. 2024a. Understanding the ISO 27001:2022 Update. WWW-dokumentti. Saatavissa: https://www.pivotpointsecurity.com/understanding-the-iso-270012022-update/ [viitattu 25.4.2024].

Pivot Point Security. 2024b. The Value of Attributes in the New ISO 27002:2022. WWW-dokumentti. Saatavissa: https://www.pivotpointsecurity.com/the-value-of-attributes-in-the-new-iso-270022022/ [viitattu 29.4.2024].

Protiviti s.a. ISO 27001:2022 – Key Changes and Approaches to Transition. PDF-dokumentti. Saatavissa: https://www.protiviti.com/sites/default/files/2023-02/iso-270001-2022-key-changes-protiviti.pdf [viitattu 14.4.2024].

Päivärinta, E. 2020. Tietoturvan riskitason määrittäminen Android-laitteissa sovellusten ohjelmointirajapintaa käyttäen. Oulun yliopisto, Tietotekniikan tutkinto-ohjelma. Diplomityö. WWW-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi:oulu-202003171271 [viitattu 12.3.2024].

Saali, J. 2023. ISO 27001:2022 Mitkä ovat uuden version keskeiset muutokset? Videoleike. Saatavissa: https://www.arter.fi/iso-270012022-mitka-ovat-uuden-version-keskeiset-muutokset/ [viitattu 21.4.2024].

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. Menetelmäopetuksen tietovaranto KvaliMOTV. Kvalitatiivisten menetelmien verkko-oppikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. PDF-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/tietoarkisto/julkaisut/kvalimotv.pdf [viitattu 18.3.2024].

SecurityScorecard. 2023. What is Threat Intelligence in Cybersecurity? A Comprehensive Overview. Blogi. Saatavissa: https://securityscorecard.com/blog/what-is-threat-intelligence-in-cybersecurity/ [viitattu 25.4.2024].

Siltainsuu, J. 2017. Kyberrikollisuus modernissa tietoyhteiskunnassa. Kandidaatintutkielma. Jyväskylän yliopisto, Tietojenkäsittelytieteiden laitos. WWW-dokumentti. Saatavissa: http://urn.fi/URN:NBN:fi:jyu-201901041066 [viitattu 11.4.2024].

Skulmoski, G. J. 2022. Shields Up: Cybersecurity Project Management. Business Expert Press. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 13.3.2024].

The History of ISO 27001. s.a. Secureframe. WWW-dokumentti. Saatavissa: https://secureframe.com/hub/iso-27001/history [viitattu 18.3.2024].

Trim, L. & Lee, Y. 2014. Cyber Security Management. A Governance, Risk and Compliance Framework. Englanti: Gower.

Vainikainen, J. s.a. Likert-asteikko kyselyssä. Blogi. Saatavissa: https://www.zef.fi/fi/blogi/likert-asteikko [viitattu 28.4.2024].

Vastuullisuusriskien hallinta. s.a. Elisa Oyj. WWW-dokumentti. Saatavissa: https://elisa.fi/yhtiotieto/vastuullisuus/ethics-ja-compliance/riskienhallinta/ [viitattu 23.4.2024].

Verizon. 2023. Summary of Findings. 2023 Data Breach Investigations Report. WWW-dokumentti. Saatavissa: https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/ [viitattu 27.4.2024].

Vilkka, H. 2021. Tutki ja kehitä. 5. päivitetty painos. Keuruu: PS-kustannus.

Vilkka, H. & Mankki, V. 2024. Johdatus monimenetelmätutkimukseen. Jyväskylä: Santalahti.

Voutilainen, J. & Kari, M. 2020. Strategic cyber threat intelligence : Building the situational picture with emerging technologies. Jyväskylän yliopisto. WWW-dokumentti. Saatavissa: http://urn.fi/URN:NBN:fi:jyu-202102041423 [viitattu 21.4.2024].

Vuori, J. 2021. Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/laadullinen-sisallonanalyysi/ [viitattu 11.4.2024].

What is information security? s.a. IBM. WWW-dokumentti. Saatavissa: https://www.ibm.com/topics/information-security [viitattu 23.4.2024].

What is risk management? s.a. IBM. WWW-dokumentti. Saatavissa: https://www.ibm.com/topics/risk-management [viitattu 20.3.2024].

Why is ISO 27001 Important? s.a. Secureframe. WWW-dokumentti. Saatavissa: https://secureframe.com/hub/iso-27001/why-is-iso-27001-important [viitattu 18.3.2024].

Yrityksen tietoturva. s.a. Elisa Oyj. WWW-dokumentti. Saatavissa: https://yrityksille.elisa.fi/tietoturva [viitattu 23.4.2024].

ISO/IEC 27001:2022 -standardin päivityksen vaikutusten arviointi

Tämä kysely on osa laajempaa tutkimusta, joka keskittyy ymmärtämään ISO/IEC 27001:2022 -standardin päivityksen vaikutuksia. Kyselyn tarkoituksena on selvittää, miten standardin uudet vaatimukset ja muutokset vaikuttavat organisaatioiden riskienhallintaan ja tietoturvakulttuuriin.

Kyselyn vastauksista saatava tieto auttaa tunnistamaan keskeisiä asioita, jotka vaativat tarkempaa tutkimusta ja pohdintaa. Saatuja tietoja hyödynnetään opinnäytetyössä ja ne tukevat työn tavoitteiden saavuttamista.

Vastausten avulla voidaan:

- Tunnistaa keskeiset haasteet ja mahdollisuudet, joita uusi standardi tuo mukanaan.
- Tarjota syvällisempää tietoa standardin vaikutuksista.
- Kehittää suosituksia standardin onnistuneeseen implementointiin.

Vastaamiseen kuluu arviolta 10-15 minuuttia. Kaikki vastaukset käsitellään luottamuksellisesti ja anonyymisti.

Kiitos jo etukäteen vastauksistanne!

ISO 27001:2022 -standardin muutokset

Kuinka hyvin koet olevasi perillä uuden ISO/IEC 27001:2022 -standardin vaatimuksista ja muutoksista? *

1. Erittäin huonosti perillä
2. Melko huonosti perillä
3. Kohtalaisesti perillä
4. Melko hyvin perillä
5. Erittäin hyvin perillä

	1	2	3	4	5	
Erittäin huonosti perillä	○	○	○	○	○	Erittäin hyvin perillä

Kuinka merkittäviksi koet ISO/IEC 27001:2022 -standardin muutokset? *

1. Erittäin merkityksettömiä
2. Melko merkityksettömiä
3. Neutraali
4. Melko merkittäviä
5. Erittäin merkittäviä

	1	2	3	4	5	
Erittäin merkityksettömiä	○	○	○	○	○	Erittäin merkittäviä

Mitkä **kolme** uutta hallintakeinoa ISO/IEC 27001:2022 -standardissa ovat mielestänne tärkeimpiä? *

	A.5.7 Uhkatiedon seuranta	A.5.23 Pilvipalvelujen tietoturvallisuus	A.5.30 Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa	A.7.4 Fyysisen turvallisuuden valvonta	A. Konfiguraa
1	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐

Mitä vaikutuksia arvioitte valitsemienne hallintakeinojen päivitysten tuovan organisaatioiden tietoturvaan yleisesti?

Oma vastauksesi

Mikä on mielestänne standardin merkittävin uudistus?

Oma vastauksesi

Onko mielestäsi Liite A:n rakenteellinen muutos ISO/IEC 27001:2022 -standardissa hyödyllinen uudistus? *

1. Erittäin hyödytön
2. Melko hyödytön
3. Neutraali
4. Melko hyödyllinen
5. Erittäin hyödyllinen

	1	2	3	4	5	
Erittäin hyödytön	○	○	○	○	○	Erittäin hyödyllinen

Miksi?

Oma vastauksesi

Kuinka merkittäviä toimenpiteitä siirtyminen ISO/IEC 27001:2013 -standardista ISO/IEC 27001:2022 -standardiin vaatii jo sertifioiduilta organisaatioilta? *

1. Ei lainkaan merkittäviä
2. Vähän merkittäviä
3. Neutraali
4. Melko merkittäviä
5. Erittäin merkittäviä

	1	2	3	4	5	
Ei lainkaan merkittäviä	○	○	○	○	○	Erittäin merkittäviä

Yleisesti ottaen, mitä haasteita näette standardin siirtymäprosessissa?

Oma vastauksesi

Riskienhallinta

Miten organisaatiot voivat osoittaa, että ne ovat toteuttaneet uuden ISO/IEC 27001:2022 -standardin mukaisen riskienhallinnan tehokkaasti?

Oma vastauksesi

Onko organisaatioiden tietoturvakulttuurin kehittäminen mielestäsi tärkeää riskienhallinnan parantamisessa? *

1. Ei lainkaan tärkeää
2. Ei kovin tärkeää
3. Neutraali
4. Melko tärkeää
5. Erittäin tärkeää

	1	2	3	4	5	
Ei lainkaan tärkeää	○	○	○	○	○	Erittäin tärkeää

Kuinka tärkeänä pidät perehdytystä osana organisaatioiden riskienhallintaa?

1. Ei lainkaan tärkeää
2. Ei kovin tärkeää
3. Neutraali
4. Melko tärkeää
5. Erittäin tärkeää

	1	2	3	4	5	
Ei lainkaan tärkeää	○	○	○	○	○	Erittäin tärkeää

Miksi perehdytys on tärkeää?

Oma vastauksesi