Tampereen ammattikorkeakoulu

ISO/IEC 27001:2022-standardin tuomat muutokset organisaatiossa

Iina Antila

OPINNÄYTETYÖ
Toukokuu 2023

Tietotekniikan tutkinto-ohjelma
Tietoverkkotekniikka ja tietoliikenne

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Tietoverkkotekniikka ja tietoliikenne

ANTILA, IINA:
ISO/IEC 27001:2022-standardin tuomat muutokset organisaatiossa

Opinnäytetyö 38 sivua, josta liitteitä 5 sivua
Toukokuu 2023

International Organization for Standardisation (ISO) ja International Electrotechnical Commission (IEC) ovat yhdessä julkaisseet ISO/IEC 27001-standardin uuden version 25. lokakuuta 2022. ISO/IEC 27001:2022 standardi auttaa organisaatioita tiedostamaan, tunnistamaan ja hallitsemaan riskejä ennakoivasti tietoturvallisuuden hallintajärjestelmän muodossa.

Opinnäytetyö käsittelee standardin keskeisimpiä muutoksia vuoden 2013 versioon verrattuna. Standardin muutoksia käsitellään ISO27001-sertifioituneen yrityksen näkökulmasta. Opinnäytetyössä esitellään standardin keskeisimmät muutokset, jotka sertifioituneiden yritysten tulisi ottaa huomioon ennen uutta auditointia. Tavoitteena opinnäytetyössä oli luoda avustava työkalu toimeksiantajalle muutoksen tueksi. Osana opinnäytetyötä kartoitettiin kyselyn avulla ISO 27001 -sertifioitujen yritysten ja organisaatioiden valmiuksia ja asenteita kyseisen standardin uudistuksiin sekä uudelleensertifiointiin.

Standardin keskeisimmät muutokset ovat standardin liite A:n kontrolleissa. Muutoksia on tapahtunut myös standardin vaatimuksissa. Muutoksista monet ovat kielellisiä sana- ja lauserakenteiden muutoksia, sisällön yhtenäistämistä ja selkeämpää linjausta.

Kyselyn perusteella suurin osa vastanneista organisaatioista on jo aloittanut muutostyöt uudelleensertifiointia varten. Vastausten perusteella organisaatiot näkevät suurimpina haasteina muutostyössä resurssien saatavuuden, tietoturvallisuuden hallintajärjestelmän dokumentaation ja muutoksiin perehtymisen, johon tällä opinnäytetyöllä on tarkoitus vastata.

Opinnäytetyön tavoitteena oli perehtyä muutoksiin ja muodostaa yhteenveto keskeisistä muutoksista. Lopputuloksena opinnäytetyössä luotiin toimeksiantajalle aputyökalu tietoturvallisuuden hallintajärjestelmän dokumentaation ja keskeisten muutoksien hallintaan. Opinnäytetyön tavoite saavutettiin ja sen tulokset esitellään tässä raportissa.

Asiasanat: ISO/IEC 27001, tietoturva, riskienhallinta, tietoturvallisuuden hallintajärjestelmä

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunications Engineering and Networks

ANTILA, IINA:
The Changes Introduced by ISO/IEC 27001:2022 Standard in an Organisation

Bachelor's thesis 37 pages, appendices 5 pages
May 2023

The International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC) jointly published a new version of ISO/IEC 27001 on 25 October 2022. ISO and IEC develop international standards in various areas, including information security and data processing. ISO/IEC 27001:2022 helps organisations proactively identify, recognize, and manage risks in an information security management system.

This thesis focused on key changes in the standard compared to the previous version. The changes from the 2013 version will be examined from the perspective of an organisation that is already ISO 27001 certified, highlighting considerations before undergoing a new audit. The objective was to create a supportive tool to assist the client in managing the transition. As part of the thesis, the capacity and attitudes of ISO 27001-certified companies and organisations were mapped to the revisions and recertification of that standard.

The main changes to the standard are in the Annex A's controls, along with changes in the requirements. Many changes involve linguistic structures, harmonisation, and clearer alignment.

According to the survey findings, organisations have initiated recertification. Challenges identified include resource availability, documentation of the IT security management system, and comprehensive examination of the changes addressed in this thesis.

Key words: ISO/IEC 27001, information security, risk management, information security management system

SISÄLLYS

LYHENTEET JA TERMIT

ISO	International Organisation for Standardisation
IEC	International Electrotechnical Commission
Standardi	Yleisesti hyväksyttyä laatutason määrittely
SFS	Suomen Standardisoimisliitto
SoA	Statement of Applicability, soveltuvuuslauseke
ISMS	Information Security Management System, tietoturvallisuuden hallintajärjestelmä
Sertifikaatti	Virallinen todistus vaatimusten täyttämisestä tai tietyn standardin noudattamisesta
Kontrolli	Toimenpide tai mekanismi, jolla varmistetaan haluttu tulos tai tavoitteen saavuttaminen
Liite A	Annex A, sisältää standardin tärkeimmät ohjaustoimenpiteet
PDCA	Plan, Do, Check, Act. Jatkuvan parantamisen prosessimalli
Auditointi	Toiminnan tarkastaminen sovittujen standardien mukaan
Akkreditointi	Akkreditointi on virallinen tunnustus toiminnan pätevyydestä.

1 JOHDANTO

Kyberrikollisuus lisääntyy ja uusia uhkia tunnistetaan organisaatioissa ympäri maailmaa jatkuvasti. Check Point Softwaren vuoden 2023 kyberturvallisuusraportti kertoo, että maailmanlaajuiset kyberhyökkäykset lisääntyivät 38 % vuonna 2022 vuoteen 2021 verrattuna (Check Point 2023). Kyberriskien hallinta on noussut välttämättömäksi osaksi organisaatioiden toimintaa.

ISO/IEC 27001 on maailmanlaajuisesti tunnettu ja tunnustettu tietoturvallisuusstandardi. ISO:n (2013) mukaan standardi antaa organisaatioille puitteet ja ohjeet tietoturvallisuuden hallintaan ja parantamiseen. Standardin tavoitteena on varmistaa, että organisaatioilla on asianmukaiset tietoturvaprosessit ja -järjestelmät, jotka auttavat suojaamaan tietoja ja tietojärjestelmiä mahdollisilta tietoturvauhilta. Organisaatiot, jotka haluavat saada ISO-standardin mukaisen sertifikaatin, voivat sertifioitua riippumattoman sertifiointielimen kautta. ISO/IEC 27001 -sertifikaatilla organisaatio voi osoittaa sitoutumista tietoturvan hallintaan kolmansille osapuolille ja sidosryhmille. Tällä osoituksella organisaatio todennäköisesti lisää luottamusta kaikessa vuorovaikutuksessa (Krypsys 2023a).

Sertifiointi itsessään ei takaa organisaatioiden toiminnan ja prosessien tietoturvallisuutta. Siksi on tärkeää, että standardin esittämät vaatimukset ja tietoturvakontrollit suunnitellaan jalkautettavan organisaatiossa käytännössä. Standardin esittämien riskien ja niiden hallintakeinojen linkittämistä suoraan organisaation liiketoimintaan voidaan pitää tärkeänä.

1.1 Opinnäytetyön tarkoitus, tavoitteet ja kyselytutkimus

Opinnäytetyön tarkoituksena oli kerätä yhteen standardin uudistuneen version keskeisimmät muutokset vanhaan versioon nähden, tehdä yhteenveto keskeisistä muutoksista ja rakentaa kerätystä tiedosta aputyökalu toimeksiantajaorganisaatiolle. Opinnäytetyössä tutkittiin kyselytutkimuksen avulla myös muiden eri toimialojen sertifioituneiden organisaatioiden valmiuksia ja asenteita kyseisen standardin uudistuksiin sekä uudelleensertifiointiin.

Kysely osoitettiin 32:lle eri toimialojen organisaatioille, jotka ovat ISO/IEC 27001 -sertifioituneita. Kyselyyn valittiin organisaatiot Kiwa Inspectan sertifikaattihaun avulla. Sertifikaattihaku antoi yleistä tietoa sertifioituneesta organisaatiosta. Kutsu kyselyyn osallistumisesta lähetettiin sähköpostitse suoraan organisaation yhteyshenkilölle, jonka yhteystiedot löytyivät organisaation verkkosivuilta.

Kyselyssä taustaksi kartoitettiin organisaation tilannetta sertifikaatin nykytilanteeseen, muutoksiin valmistautumisen ja koettujen haasteiden suhteen. Kyselyn tarkoituksena oli kartoittaa yleisesti standardiuudistukseen liittyviä suurimpia haasteita ja niiden taustatekijöitä. Kyselyyn vastanneita organisaatioita on yhteensä yhdeksän.

1.2 Toimeksiantaja

Opinnäytetyön toimeksiantaja oli Netum Oy, jolla on yli 20 vuoden kokemus vaativista IT-hankkeista. Netum Oy:n tavoitteena on olla alan luotetuin kumppani ja halutuin työyhteisö vastuullisessa ja turvallisessa digimuutoksessa. (Netum Oy, 2023a.)

Netum on noin kolmensadan työntekijän IT-palvelutalo, jolla on toimipisteet Tampereella, Helsingissä, Turussa, Porissa, Jyväskylässä, Hämeenlinnassa ja Kuopiossa. Netumin liikevaihto vuonna 2022 oli 29.1 miljoonaa euroa. Netum Group Oyj on listattu Nasdaq Helsingin First North -markkinapaikalle. (Netum Oy 2023b.)

Yksi Netumin vahvuuksista on matala organisaatio, joka pystyy yhdistelemään palveluja ja tarjoamaan asiakaskohtaisia ratkaisuja. Netum Oy tarjoaa digipalveluiden kehittämistä ja ylläpitoa, kyberturvallisuuspalveluita, data- ja integraatiopalveluja, tietovarasto- ja analytiikkaratkaisuja, tietojärjestelmien kehittämis-, tuki- ja ylläpitopalveluita sekä johdon konsultointia (Netum Oy 2023c).

2 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ

Verkottunut ja edelleen digitalisoituva yhteiskuntamme on haavoittuva. Kaikki peruspalvelut toimivat pitkälti tietotekniikan ohjaamina, joten pienilläkin häiriöillä voi olla vakavia kerrannaisvaikutuksia. (Järvinen, P. 2018. 14.) Yritysten ja organisaatioiden tietomäärät ovat valtavia. Palveluiden ja tuotteiden saatavuus riippuu tietovirroista ja -verkoista, joten tietojen turvallisuus on sekä yksityishenkilöiden että organisaatioiden huolenaihe.

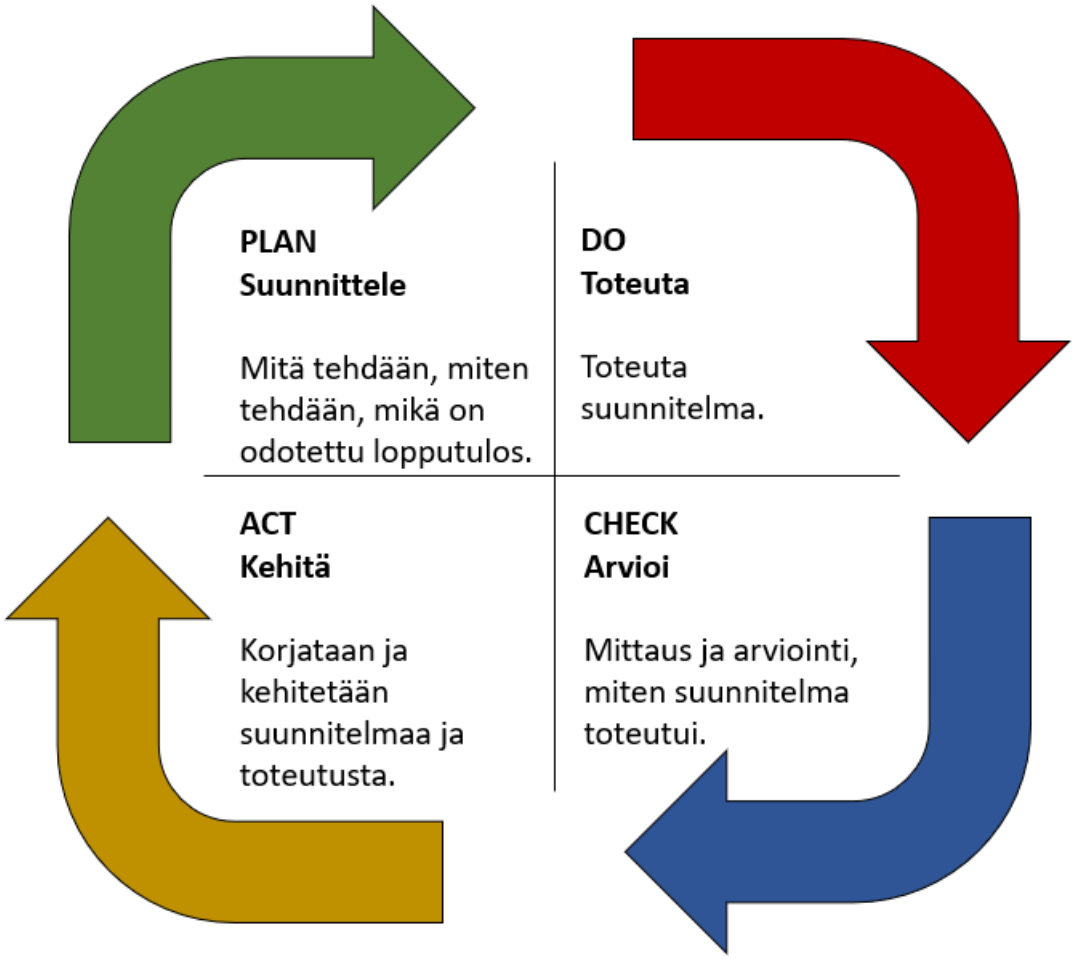
Tietoturva on kokonaisvaltaista tietojen suojelemista. Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden ylläpitämistä. Tietoturva Pron (2019) mukaan tietoturvallisuuden tavoitteena on varmistaa, että tiedot ovat ainoastaan niiden käytettävissä, joilla on niihin oikeus, silloin kun he niitä tarvitsevat. Lisäksi pyritään varmistamaan, että tiedot ovat oikeassa muodossa eivätkä ole muuttuneet matkalla. Tahalliset ja tahattomat toimet organisaation tietoverkoissa, prosesseissa ja käytännöissä voivat aiheuttaa monenlaisia riskejä tietoturvallisuudelle kaikilla yhteiskunnan tasoilla.

Tietoturvallisuuden hallintajärjestelmä on viitekehys, jota organisaatiot voivat soveltaa omaan strategiaansa. Tietoturvallisuuden hallintajärjestelmä on systemaattinen ja dokumentoitu toimintamalli prosessien, omaisuuksien ja riskien sekä niiden hallintakeinojen tunnistamisesta, johtamisesta ja hallinnasta. Hallinnalla tarkoitetaan valvontaa ja liiketoimintatavoitteiden saavuttamiseen tarvittavien päätösten tekemistä riskiperusteisesti siten, että organisaation tieto-omaisuus suojataan (Lahnalahti 2022). Hallinnan lähtökohtana on tunnistaa organisaation toiminta ja siihen liittyvät liiketoimintariskit.

2.1 PDCA-malli

ISO 27001-standardissa ja tietoturvallisuuden hallintajärjestelmän kehittämisessä hyödynnetään PDCA-prosessimallia. PDCA tulee sanoista Plan (suunnittele), Do (toteuta), Check (arvioi) ja Act (kehitä).

PDCA-mallissa toimintaa ja kehitystyötä arvioidaan, mitataan ja kehitetään jatkuvasti. Tavoitteiden seuraaminen, tarkistaminen ja kehittäminen nähdään jatkuvana prosessina, jossa jokaisen kierroksen jälkeen päästään lähemmäksi asetettua tavoitetta. (Aalto-yliopisto 2022.) Kuten ISO 27001-standardi, myös PDCA-malli edellyttää organisaatiolta jatkuvaa tietoturvallisuuden kehittämistä (kuvio 1).

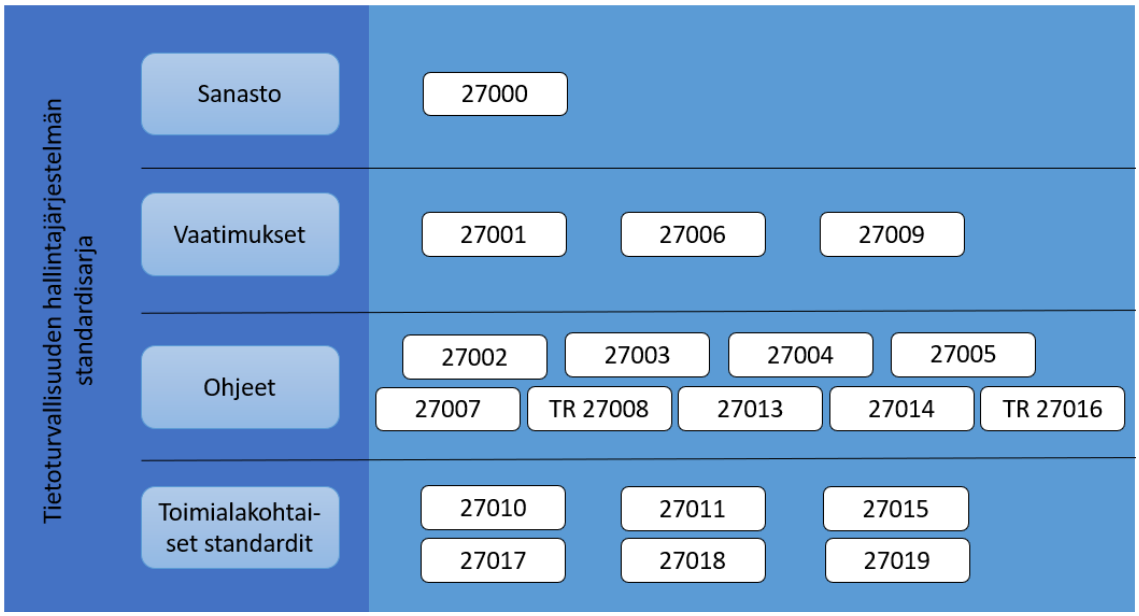


KUVIO 1. PDCA-malli sovellettuna tietoturvallisuuden hallintajärjestelmän toteutuksessa.

3 ISO/IEC 27000-standardisarja

ISO/IEC 27000 on kansainvälisen standardointijärjestön ISO:n (International Organisation for Standardisation) ja kansainvälisen sähköalan standardointiorganisaation IEC:n (International Electrotechnical Commission) luoma ja hallinnoima standardisarja. Suomessa standardin suomenkielisestä kehittämisestä ja ylläpidosta vastaa Suomen Standardoimisliitto SFS (ISO n.d.). Sarja sisältää joukon standardeja, joille kaikille keskeistä on tietoturvallisuuden hallinta. ISO/IEC 27000-sarjan tavoitteena on tarjota ja luoda hyviä toimintatapoja tietoturvan hallintajärjestelmän käyttöönottoon, ylläpitoon ja hallinnointiin. (GlobalSuite Solutions 2022.)

Standardisarjaa täydennetään useilla erilaisilla yksittäisillä standardeilla ja ohjeilla (The ISO 27000 Directory 2021). ISO/IEC 27000 tarjoaa yleiskuvauksen tietoturvallisuuden hallintajärjestelmästä, sekä siihen liittyvästä sanastosta ja termeistä. Tietoturvallisuuteen liittyvä erikoissanasto muuttuu ja päivittyy jatkuvasti. Ydinterminologialla voi olla useita merkityksiä ja tulkintoja riippuen kontekstista. Tämä itsessään on riski, jota standardi muodollisilla määrittelyillä pyrkii minimoimaan. Tietoturvallisuuden yleiskuvaus käsittelee tietoturvan riskien, hallintakeinojen ja hallintajärjestelmien keinot. (IsecT Oy 2023.) Kuvio 2 esittää ISO27001-sarjan standardit kokonaisuutena.



KUVIO 2. ISO/IEC 27000 standardiperhe.

Tässä opinnäytetyössä käsitellään tarkemmin ISO/IEC 27001-standardia, johon liittyy läheisesti myös 27002- ja 27005-standardit. Kyseiset standardit ovat uudistuneet vuonna 2022.

3.1 ISO/IEC 27001 standardi

ISO/IEC 27001 (informaatioteknologia, turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät, vaatimukset) standardi esittelee tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset. Vaatimukset ovat yleisluontoisia ja niitä voi soveltaa kaikentyyppiset ja -kokoiset organisaatiot. Standardi sisältää myös tietoturvariskien arviointia ja käsittelyä koskevat vaatimukset. (SFS n.d.a.)

3.2 ISO/IEC 27002 standardi

ISO/IEC 27002 (tietoturvallisuus, kyberturvallisuus ja tietosuoja, tietoturvallisuuden hallintakeinot) standardi on tarkoitettu käytettäväksi yhdessä ISO/IEC 27001 standardin kanssa tietoturvallisuuden hallintajärjestelmän toteuttamisprosessissa. Se sisältää ohjeistuksia yleisellä tasolla hyväksyttyjen tietoturvallisuuden hallintakeinojen toteuttamiseksi. Standardissa huomioidaan toimialaa tai organisaatiota koskevat tietoturvan riskiympäristöt, joten sitä voidaan hyödyntää myös tietoturvallisuuden hallintaohjeiden kehittämisessä. (SFS n.d.b.)

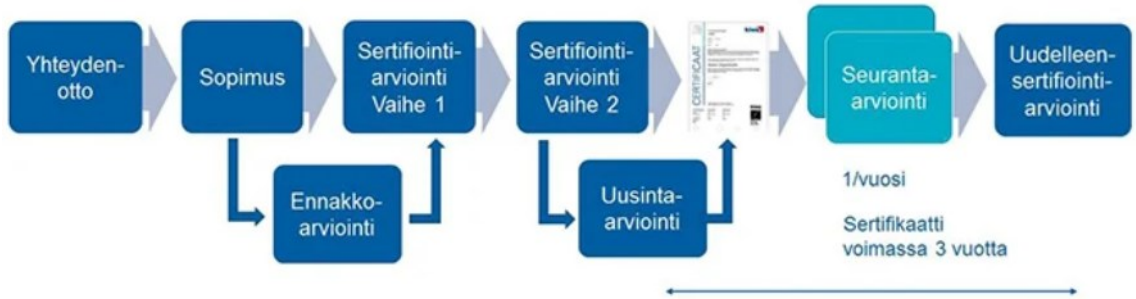
3.3 ISO/IEC 27005 standardi

ISO/IEC 27005 (informaatioteknologia, turvallisuustekniikat, tietoturvariskien hallinta) standardi esittelee ohjeita tietoturvariskien hallintaan. Sitä voidaan soveltaa kaikentyyppisille organisaatioille. (SFS n.d.c.)

3.4 Sertifioituminen ja auditointi

Organisaatio voi osoittaa tietoturvansa tason muun muassa sertifikaatilla. Sertifikaatilla viitataan esimerkiksi prosessin, komponentin tai organisaation tiettyjen ominaisuuksien varmistamiseen. Sertifioitumista edeltää auditointiprosessi, jossa kolmas puolueeton osapuoli arvioi sertifikaatin vaatimusten täyttymistä. (Kiwa Inspecta n.d.a.) ISO/IEC 27001-standardia vasten auditoitu sertifikaatti on kansainvälisesti tunnettu ja arvostettu.

Organisaation luotua tietoturvallisuuden hallintajärjestelmän se ottaa yhteyttä sertifiointeja suorittavaan, kolmanteen osapuoleen. Kolmannen osapuolen tulee olla akkreditoitunut, jolla varmistetaan, että sertifiointikäytännöt ovat hyväksyttäviä ja yhdenmukaisia. (Kiwa n.d.b) Hallintajärjestelmän sertifiointimenettelyt on kuvattu kuviossa 3.



KUVIO 3. Hallintajärjestelmän sertifiointimenettely. (Lähde: Kiwa Inspecta)

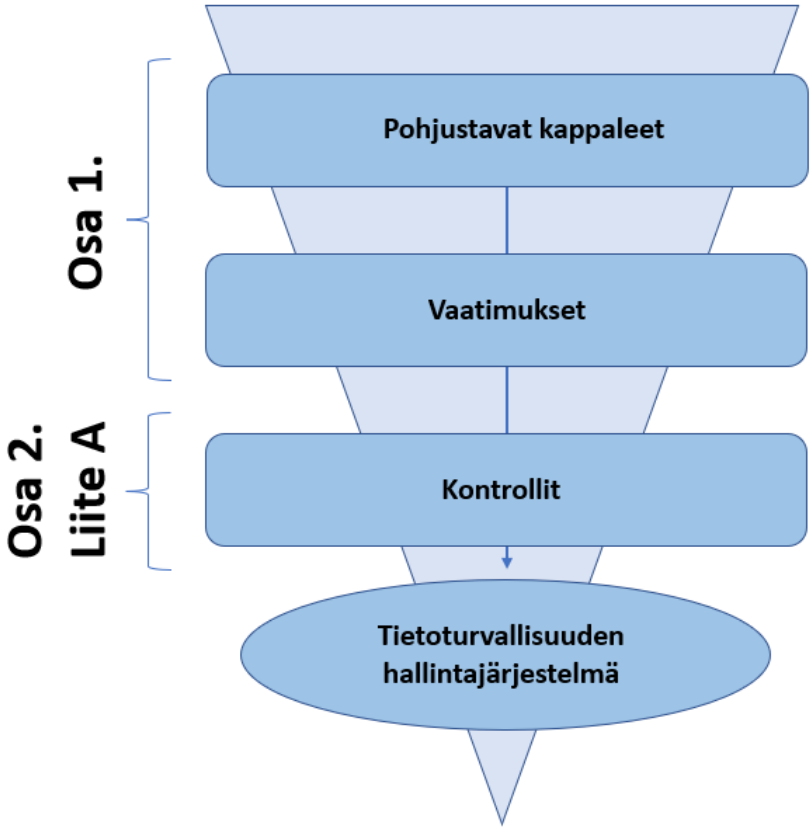
Sertifikaatti on voimassa kolme vuotta, kun auditoitua järjestelmää noudatetaan. Sertifikaatin ylläpitämiseksi tehdään vuosittain määräaikaisarviointeja, joissa vierailujen aikana tarkastetaan, että hallintajärjestelmä täyttää edelleen standardin vaatimukset. Kolmen vuoden jälkeen suoritetaan uudelleensertifiointi, joka on pitkälti samanlainen arviointiprosessi kuin sertifikaatin myöntäminen. (Bureau Veritas n.d.)

4 KESKEISIMMÄT MUUTOKSET

ISO/IEC 27001 päivitettiin uuteen versioon, joka julkaistiin lokakuussa 2022. Standardin päivitykset vastaavat jatkuvasti muuttuvaa teknologian ja tietoturvallisuuden verkottunutta maailmaa. Suurin muutos on tapahtunut standardin liite A:ssa ja sen kontrolleissa. (ISMS.online 2023a.)

4.1 Standardin rakenne

ISO/IEC 27001-standardi koostuu kahdesta osasta (kuvio 4). Ensimmäinen osa sisältää pohjustavat kappaleet ja vaatimukset. Toinen osa on liite A, jossa luetellaan joukko luokiteltuja valvontatoimenpiteitä, eli kontrolleja, joita organisaatiot käyttävät osoittaakseen noudattavansa standardia.



KUVIO 4. Standardin rakenne.

Pohjustavat kappaleet ovat johdantoa ja sisältävät yleistä tietoa standardista. Vaatimukset asettavat tavoitteet ja periaatteet tietoturvallisuuden hallintajärjestelmän luomiseen, hallintaan, ylläpitoon ja kehittämiseen. Standardin vaatimukset kertovat, mitä hallintajärjestelmän tulee sisältää, jotta se olisi asianmukainen tietoturvallisuuden dokumentoinnin ja hallinnan kannalta. Sertifioinnin kannalta on välttämätöntä, että vaatimukset implementoidaan osaksi organisaation prosesseja, dokumentteja ja käytäntöjä. (Standard Fusion 2021.) Organisaation tulee dokumentoida ja pystyä esittämään sertifikaatin auditoijalle tiedot siitä, miten vaatimukset ovat toteutettu.

Standardin liite A sisältää itse kontrollit, jotka numeroidaan A-alkuisesti (esimerkiksi A.5.11). Kontrollit ovat toimenpiteitä, jotka organisaation tulee määritellä ja niiden toteutumista tulee valvoa. Esimerkiksi millaisia vaatimuksia asetetaan salasanalle tai mitä ohjelmistoja organisaation laitteille voidaan asentaa, ja kuka sen tekee. Toisin kuin vaatimusten kohdalla, organisaation ei ole pakko toteuttaa jokaista kontrollia, sillä kaikki vaatimukset eivät välttämättä ole relevantteja tai sovellettavissa kaikissa organisaatioissa. (Cysense 2022.) Kontrollien osalta organisaation tulee kuitenkin pystyä perustelemaan, miksi kyseinen kontrolli ei ole relevantti. Kaikki kontrollit ja toimenpiteet mitä organisaatio tekee tietoturvansa hallinnoimiseksi, tulisi linkittyä organisaation riskienhallintaan.

4.2 Soveltuvuuslauseke

Soveltuvuuslauseke, eli SoA (Statement of Applicability), on tietoturvallisuuden hallintajärjestelmän ja sertifikaatin kannalta yksi olennaisimmista ja pakollisista dokumenteista. Soveltuvuuslauseke kertoo, mitä liite A:n kontrolleja ja tietoturvatoimenpiteitä organisaatio soveltaa ja miten ne toteutetaan. SoA voi sisältää myös organisaation omia kontrolleja ja toimenpiteitä, jotka katsotaan tarpeellisiksi. (GlobalSuite Solutions 2022.) SoA:n tulee sisältää myös lisätietoja kustakin kontrollista ja tietoa asiaankuuluvista asiakirjoista (IT Governance 2022).

4.3 Kontrollit

Liite A:n kontrollit jaettiin aiemmin 14:sta eri kategoriaan. Uudessa versiossa kontrollit on jaettu neljään kategoriaan, jotka esitellään tarkemmin taulukossa 1 (ISMS.online 2023b).

TAULUKKO 1. ISO/IEC 27001:2022 kontrollien luokittelu

Kategoria	Kontrollit	Kontrollien lukumäärä
Organisaatio	A.5.1 – A.5.37	37
Ihmiset	A.6.1 – A.6.8	8
Fyysinen	A.7.1 – A.7.13	14
Teknologinen	A.8.1 – A.8.34	34

ISO/IEC 27001 sisälsi aiemmin 114 kontrollia. Uudelleenjärjestelyjen ja hiomisen jälkeen kontrolleja on 93. Yleisellä tasolla muutokset kontrolleihin ovat:

- 11 uutta kontrollia otettiin käyttöön
- 58 kontrollia yhdistettiin
- 24 kontrollia nimettiin uudelleen

Uudet kontrollit ovat:

A.5.7 Uhkatiedon seuranta: Kontrolli edellyttää organisaatioita keräämään ja analysoimaan uhkatietoja helpottaakseen tietoon perustuvia toimia haittojen ehkäisemiseksi. Näin uhkien vaikutusta voidaan vähentää ja pysytään ajan tasalla tuoreimmista tiedotteista tietojen suojaamiseksi. Tämä on yksi merkittävimmistä kontrolleista, joka kertoo yleistyneen ajatuksen siitä, että uhkat kehittyvät jatkuvasti ja vaativat seurantaa.

A.5.23 Pilvipalveluiden tietoturvallisuus: Pilvipalvelut ovat yleistyneet organisaatioissa kaikilla tasoilla. Kontrolli hahmottelee prosessit, joita tarvitaan pilvipalvelujen hankinnassa, käytössä, hallinnassa ja niistä poistumisessa.

A.5.30 Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa: Kontrolli tunnustaa ICT-ympäristön ja -palveluiden tärkeän roolin liiketoiminnan jatkuvuuden ylläpitämisessä häiriön tai kriittisen tapahtuman aikana. Kontrolli määrittelee organisaation toipumisaikatavoitteen ja liiketoimintavaikutusten analyysin. Ennen liiketoiminnan keskeytystä, sen aikana ja sen jälkeen tavoitteena on säilyttää tiedon eheys ja saatavuus.

A.7.4 Fyysisen turvallisuuden valvonta: Kontrolli edellyttää, että organisaatiolla on käytössä asianmukaiset valvontalaitteet luvattoman fyysisen pääsyn varalta. Tarkoituksena on havaita ja estää ulkoisten ja sisäisten tunkeilijoiden pääsy rajoitetulle fyysiselle alueelle.

A.8.9 Konfiguraationhallinta: Konfiguraatiot joko yksittäisenä konfigurointitiedostona tai kokoelmana toisiinsa linkitettyjä määrityksiä määräävät, kuinka laitteistoa, ohjelmistoja ja verkkoja hallitaan. Konfiguraatioiden oikeellisuuden varmistaminen on oleellista, jotta varmistutaan siitä, että verkko toimii kuten pitääkin. Konfiguraatiot tulee myös suojata hyväksymättömiltä ja sopimattomilta muutoksilta. Konfiguraatioita tulee myös seurata ja katselmoida säännöllisesti.

A.8.10 Tietojen poistaminen: Organisaatioiden tulee poistaa työntekijöitä, käyttäjiä, asiakkaita ja organisaatioita koskevat tallennetut tiedot, kun niitä ei enää tarvita. Tämä koskee kaikkiin järjestelmiin, laitteisiin tai mihin tahansa muuhun tallennusvälineeseen varastoitua tietoa.

A.8.11 Tietojen peittäminen: Tietojen peittämisellä tarkoitetaan arkaluonteisten tietojen, kuten henkilökohtaisten tunnistetietojen tai pääsynhallintaa koskevien tietojen peittämistä. Tietojen peiton tulee olla toimintaperiaatteiden ja liiketoiminnallisten vaatimusten mukaista lainsäädäntö huomioiden.

A.8.12 Tietovuotojen estäminen: Tietovuoto voi olla sisäisen tai ulkoisen henkilöstön, järjestelmien tai haitallisten tahojen luvatonta pääsyä, tietojen siirtämistä tai poimimista organisaation tietojärjestelmistä. Tietovuoto on yleinen riski organisaatiossa, jossa käsitellään suuria tietomääriä. Kaikkia tietovuotojen estämistoimia on sovellettava kaikissa organisaation osissa.

A.8.16 Valvontatoiminnot: Organisaation on valvottava verkkoja, järjestelmiä ja sovelluksia poikkeavan käyttäytymisen varalta. Valvonnan tarkoitus on ennakoida tapaukset ennen niiden tapahtumista ja koordinoida reagointitoimia.

A.8.23 Verkkosuodatus: Organisaation verkkoihin ja tietojärjestelmiin voi kohdistua haittaohjelmahyökkäyksen riski, jos työntekijät vierailevat saastuneilla sivustoilla. Hyökkääjä voi myös lähettää esimerkiksi tietojenkalasteluviestejä työntekijöiden työsähköposteihin, joiden sisältämät linkit ja tiedostot johtavat saastuneelle sivustolle. Kontrollin mukaan organisaation on otettava käyttöön asianmukaiset verkkosuodatustoiminnot, joilla rajoitetaan ja valvotaan pääsyä ulkoisille verkkosivuille ja siten hallitaan turvallisuusuhkia.

A.8.28 Turvallinen ohjelmointi: Kontrollin mukaan organisaation tulee noudattaa turvallisen ohjelmoinnin periaatteita. Huonot koodauskäytännöt, kuten virheellinen validointi ja heikkojen avaimien luominen voivat altistaa organisaation kyberhyökkäyksille ja tietovarojen vaarantumisen.

4.4 Vaatimukset

Standardin uudessa versiossa vaatimusten määrä on pysynyt samana, mutta niihin on tullut tarkennuksia, sanamuutoksia ja lisäyksiä (A-LIGN, n.d.). Mukana on muutama kokonaan uusi vaatimus ja alakohta, jotka ovat kuitenkin lähtökohtaisesti tarkennuksia edellisestä versiosta. Standardien versioita vertailemalla nähdään, että kaiken kaikkiaan vaatimusten osalta muutokset, jotka ilmenevät taulukosta 2, ovat vähäisiä ISO/IEC 27001:2013 verrattuna (SFS-ISO/IEC 27001 2013, 8–12; SFS-ISO/IEC 27001 2022, 6–14).

Taulukko 2. Vaatimusten keskeiset muutokset 2022.

Vaatimus	**Muutos**
4.2	Lisätty alakohta, joka edellyttää määrittelemään tarkemmin vaatimukset, joita tietoturvan hallintajärjestelmässä vastataan.
4.4	Lisätty täydennys, jolla selvennetään prosessien ja niiden vuorovaikutuksien mukaanotto tietoturvallisuuden hallintajärjestelmässä. Lisäksi vaatimuksessa puhutaan ”kansainvälisen standardin” sijaan ”asiakirjasta”.
6.2	Muutokset ovat pieniä, mutta selventäviä. Vaatimus esittää, että tietoturvatavoitteita tulee seurata ja ne on oltava saatavilla dokumentoituna tietona. Vaatimuksen alaosat ovat tarkentuneet, jonka myötä numerointi ja järjestys on muuttunut.
6.3	Kokonaan uusi vaatimus. Tällä vaatimuksella halutaan tarkentaa muutosten hallintaa ja sitä, että kaikki muutokset tietoturvallisuuden hallintajärjestelmään tehdään suunnitellusti.
8.1	Muutokset ovat selventäviä toiminnan suunnittelun ja valvonnan osalta.
5.3	Pienet kielelliset muutokset tarkentavat, että tietoturvaan liittyvistä rooleista tulee viestiä organisaation sisällä.
7.4	Tiivistyy alakohtien osalta. Uusi alakohta ”kuinka viestitään” yhdistää viestintäprosessit ja sen, kuka viestii.
9.2	Sisältö ei ole muuttunut. Muutokset ovat sanamuodollisia ja vaatimuksen sisältö jaetaan nyt omiksi alakohdikseen **9.2.1** ja **9.2.2.**
9.3	Muutokset ovat sanamuodollisia selvennyksiä. Yhden vaatimuksen sijaan tämä vaatimus on jaettu selkeyden vuoksi kolmeen alakohtaan **9.3.1**, **9.3.2** ja **9.3.3**.
10.1, 10.2	Vaatimukset ovat sisällöltään samanlaiset, mutta luetellaan nyt eri järjestyksessä (10.1 Jatkuva parantaminen, 10.2 Poikkeamat ja korjaavat toimenpiteet).

5 TYÖKALU MUUTOKSIEN YHTEENVEDOSTA

Standardin muutosten yhteenvedon tekemiseksi opinnäytetyöhön toimeksiantajaorganisaatiossa järjestettiin suunnittelupalaveri. Keskustelun aikana todettiin, että muutokset voitaisiin käsitellä taulukko-muodossa, joka yhdistäisi tietoa standardin vanhasta ja uudesta versiosta. Taulukon tärkeiksi ominaisuuksiksi nostettiin mahdollisuus luokitella tietoja, selkeys ja mahdollisuus kerätä yksityiskohtaistakin tietoa. Näistä syistä ryhdyttiin toteuttamaan työkalua Microsoft Excel -ohjelmistolla, jolla koettiin olevan hyvä mahdollisuus toteuttaa kriteerejä.

Työkalussa standardin vaatimukset ja kontrollit jaetaan omille välilehdilleen. Vaatimusten osalta taulukon tietoa voi luokitella vaatimuksen tunnisteen, kategorian, päivityksen ja dokumentin mukaan. Tämä helpottaa linkittämään vaatimukset eri dokumentteihin, kiinnittämään huomiota uudistuneisiin vaatimuksiin ja etsimään tietoa yksityiskohtaisesti.

Kontrollit-välilehdellä taulukko mahdollistaa myös kontrollien haun ja jaottelun kontrollien tunnisteen, kategorian ja päivityksen avulla. Taulukko luokittelee uudet kontrollit myös vanhojen kontrollien mukaan sen perusteella, mistä vanhoista kontrolleista uusi tunniste muodostuu. Taulukkoon on tuotu myös keskeisiä linkityksiä toimeksiantajaorganisaation dokumentaatioon.

Organisaation aloittaessa dokumentaation osalta varsinaisen muutostyön voivat muutospolut olla hyvin erilaisia ja poiketa toisistaan merkittävästi. Riippuen organisaation nykyisestä dokumentaatiosta, sitoutumisesta ja vaatimusten linkityksestä liiketoimintaan työmäärä voi vaihdella paljon.

6 KYSELYTUTKIMUS

Opinnäytetyössä toteutettiin kyselytutkimus, joka auttoi muodostamaan johtopäätöksiä opinnäytetyön aiheesta kokonaisuutena. Kyselyn tarkoituksena oli tutkia eri toimialojen sertifioituneiden organisaatioiden valmiuksia, keinoja ja asenteita uudistuksiin ja uudelleensertifiointiin liittyen. Tutkimusmenetelmä oli kvantitatiivinen ja kvalitatiivinen. Kvantitatiivinen menetelmä auttaa ymmärtämään kyselyn vastauksia numeroiden ja prosenttien kautta (Jyväskylän yliopisto, 2015). Kvalitatiivisen menetelmän avulla on mahdollista ymmärtää tutkimuskohdetta laajemmin kokonaisuutena (Tilastokeskus n.d).

Kysely päätettiin toteuttaa sähköisesti Microsoft Forms -työkalulla sen helppouden ja nopeuden ansiosta. Kyselyyn valitut organisaatiot löytyivät Kiwa Inspectan sertifikaattihaulla ja näiden organisaatioiden yhteystiedot yritysten verkkosivuilta. Kutsu osallistua kyselyyn lähetettiin suoraan yhteyshenkilön sähköpostiin. Vastausaika oli 3.-15.5.2023. Tänä aikana kyselyyn saatiin 9 vastausta 32:sta. Kyselyn vastausprosentti oli 28,13 %.

Suurimmat haasteet kyselyn toteuttamisessa olivat kyselyn arkaluontoinen aihe ja suhteellisen lyhyt vastausaika, jonka takia kyselyn osalta ei lähetetty muistutusviestejä. Kyselyssä oli sekä avoimia että suljettuja kysymyksiä. Suljettujen kysymyksien vastaukset olivat toisensa poissulkevia.

6.1 Kysymykset ja tulokset

Tässä kappaleessa käsitellään kyselytutkimuksen kysymyksiä ja niiden vastauksia. Vastaukset esitellään jokaisen kysymyksen osalta erillisinä kohtina. Vastauksia esitellään myös havainnollistaen kuvioiden ja taulukoiden avulla.

Kysymys 1: Minä vuonna edustamasi organisaatio on sertifioitunut?

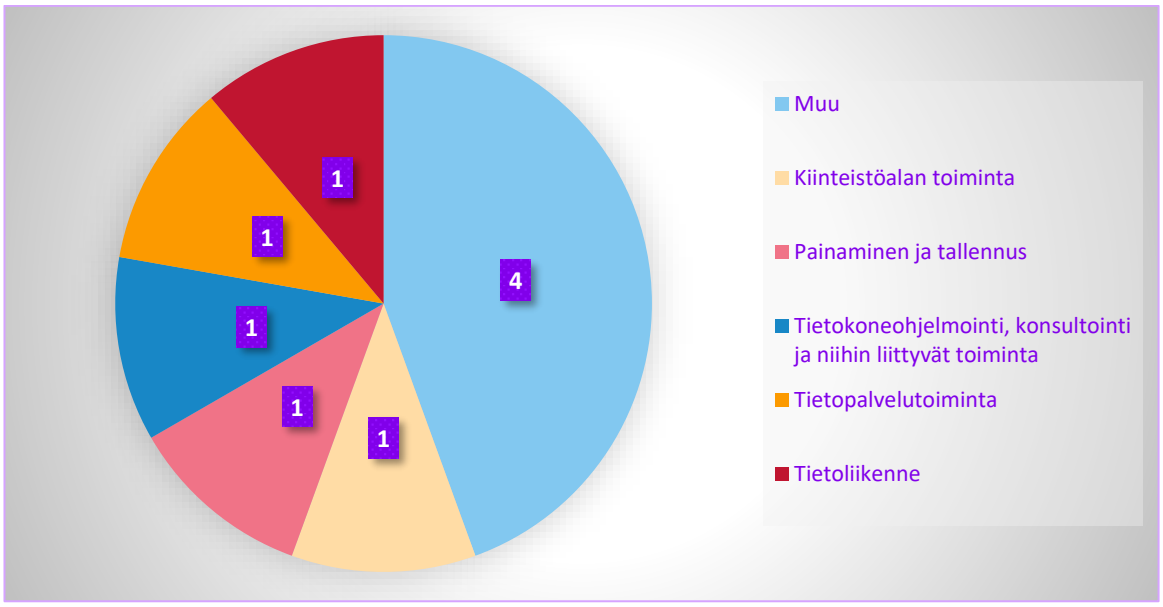
Kysymyksellä kartoitetaan vastanneiden organisaatioiden sertifioitumisen vuotta, joka antaa tietoa siitä, kuinka kauan sertifioitu tietoturvallisuuden hallintajärjestelmä on ollut käytössä. Vastausten perusteella (taulukko 3) nähdään, että suurin osa sertifioinneista on tapahtunut alle viisi vuotta sitten.

TAULUKKO 3. Organisaatioiden sertifioitumisen vuosi

Sertifioitumisvuosi	Organisaatioiden lukumäärä
2013	2
2017	1
2020	2
2022	3

Kysymys 2: Mikä on organisaation toimiala?

Kysymyksellä selvitetään vastanneiden organisaatioiden toimialaa. Osallistumiskutsuja kyselyyn lähetettiin usealle eri toimialalle ja vastauksia saatiin jonkin verran vaihdellen (kuvio 5). Edustetuin kategoria on ”muu”-toimiala.

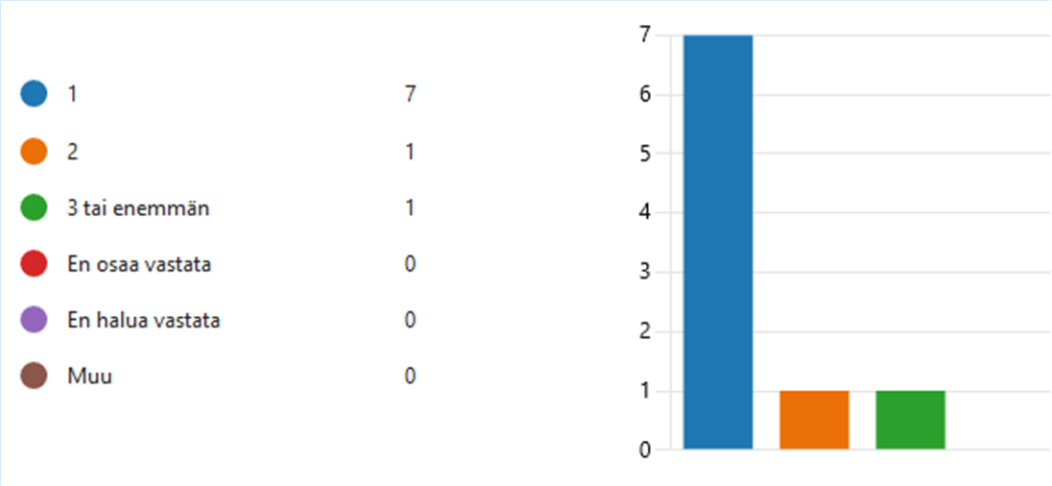


KUVIO 5. Organisaatioiden toimialat

Kysymys 3: Kuinka monta eri tietoturvapäällikköä on työskennellyt organisaatiossa sertifikaatin voimassaolon aikana tietoturvallisuuden hallintajärjestelmän parissa?

Tämän kysymyksen yhteydessä tarkennettiin, mitä tietoturvapäälliköllä tarkoitetaan. Kysymyksessä tietoturvapäälliköllä tarkoitettiin roolia, jonka tehtävä on suunnitella, kehittää ja johtaa organisaation tietoturvallisuuden hallintaa, mukaan lukien riskienhallinta, auditointi, raportointi ja yhteistyö organisaation osien ja sidosryhmien kanssa. Kuvio 6 kertoo, että suurimmassa osassa vastanneista organisaatioista on työskennellyt yksi tietoturvapäällikkö, yhdessä organisaatiossa kaksi ja yhdessä kolme tai enemmän.

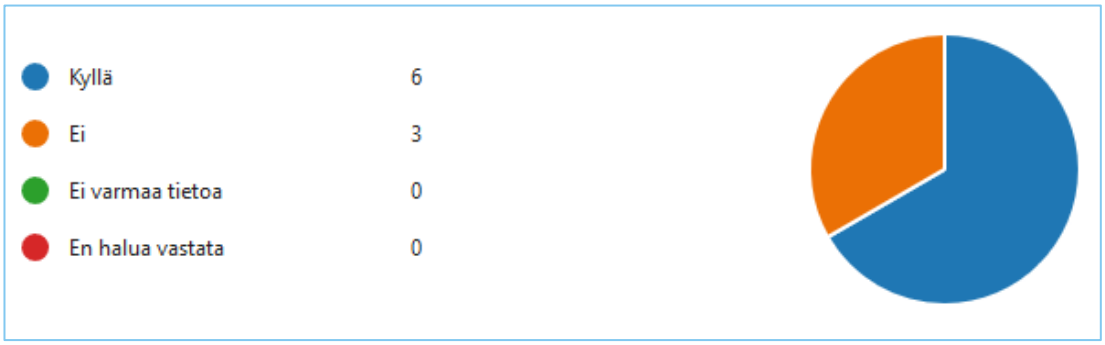
Tällä kysymyksellä voidaan kartoittaa, onko tietoturvallisuuden hallintajärjestelmä, sen ylläpito ja kehitys ollut useamman henkilön vastuulla sertifikaatin voimassaolon aikana.



KUVIO 6. Organisaatiossa työskennelleiden tietoturvapäälliköiden määrä

Kysymys 4: Onko organisaatiossanne aloitettu valmistautuminen uusien ISO/IEC 27001:2022 standardin vaatimusten täyttämiseksi?

Kysymyksellä kartoitetaan, ovatko organisaatiot aloittaneet valmistautumisen standardin uuteen versioon. Kolmasosa vastaajista ei ole vielä aloittanut valmistautumista (kuvio 7).

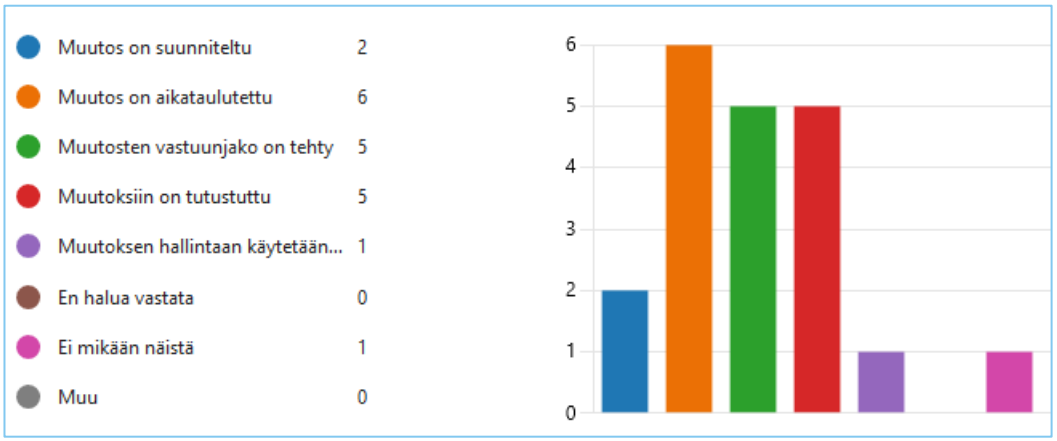


KUVIO 7. Organisaatioiden valmistelujen aloitus standardin muutoksiin

Kysymys 5: Miten organisaationne on suunnitellut muutoksen hallinnan ISO/IEC 27001:2022 standardin uusien vaatimusten osalta?

Kysymyksellä kartoitetaan keinoja organisaation vaatimusten muutosten hallinnan suunnittelussa. Vastausten perusteella (kuvio 8) nähdään, että suurin osa vastanneista organisaatioista on aikatauluttanut muutokset (66,7 %), miettinyt muutosten vastuunjakoa (55,7 %) ja tutustunut muutoksiin (55,7 %).

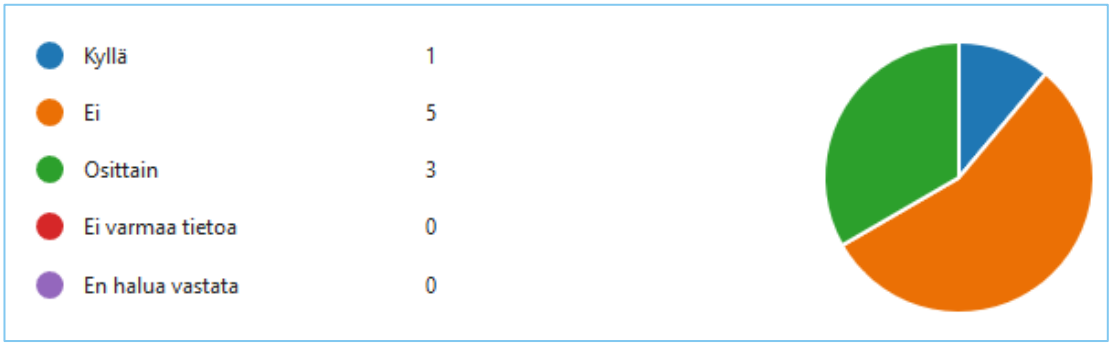
Vastaajista 22,2 % toteaa, että muutoksia on suunniteltu ja yksi vastaajista kertoo muutoksiin käytettävän ulkoista konsulttia tai muuta vastaavaa. Yksi kyselyvastaus on ”ei mikään näistä”, eli ettei muutosten hallinnan keinot löydy näistä vaihtoehdoista.



KUVIO 8. Organisaatioiden muutosten hallinnan suunnittelu

Kysymys 6: Onko organisaatiossanne jo lähdetty toteuttamaan ISO/IEC 27001:2022 standardin myötä uudistuneita vaatimuksia ja kontrolleja?

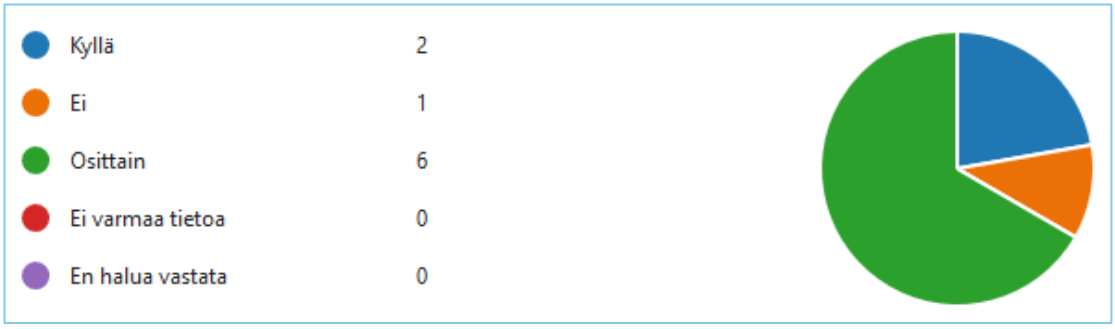
Kysymyksen vastausten (kuvio 9) perusteella nähdään, että suurin osa vastaajista ei ole lähtenyt toteuttamaan standardin uuden version mukaisia uudistuksia organisaation vaatimuksiin ja kontrolleihin. Kolmasosa on aloittanut toteutukset osittain.



KUVIO 9. Organisaation uudistusten toteutus

Kysymys 7: Onko organisaatiossanne varmistettu, että tarvittavat resurssit, kuten taloudelliset, teknologiset ja henkilöstöresurssit ovat käytettävissä ISO27001:2022 standardin muutosten toteuttamiseen?

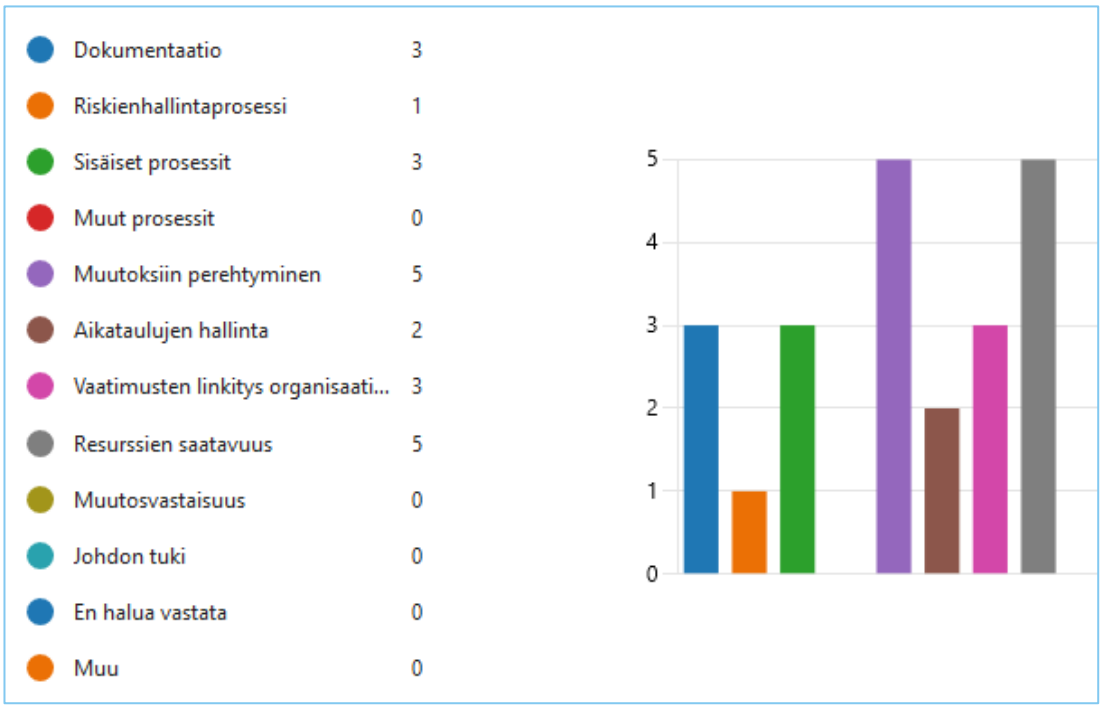
Kysymyksellä kartoitetaan resurssien saatavuuden varmistusta muutoksiin liittyen. Vastauksien perusteella (kuvio 10) suurimassa osassa organisaatioita varmistuksia resursseihin on tehty osittain. Kahdessa varmistuksia on tehty ja yhdessä toistaiseksi ei.



KUVIO 10. Resurssien saatavuuden varmistus organisaatiossa

Kysymys 8: Mitkä ovat organisaationne suurimmat haasteet ISO27001:2022 standardin muutosten implementoinnissa?

Kysymyksellä selvitetään mitä haasteita organisaatiot kokevat muutoksien implementointiin liittyen. Vastausten perusteella (kuvio 11) suurimmaksi haasteeksi nousi muutoksiin perehtyminen ja resurssien saatavuus (viisi vastausta). Toiseksi suurimmaksi haasteeksi koetaan tietoturvallisuuden hallintajärjestelmään liittyvä dokumentaatio, sisäiset prosessit ja vaatimusten linkitys organisaation liiketoimintaan. Muita haasteita ovat riskienhallintaprosessissa ja aikataulujen hallinnassa.



KUVIO 11. Organisaation suurimmat haasteet standardin muutoksien implementoinnissa

Kysymys 9: Kerro halutessasi tarkemmin haasteista organisaatiossa muutokseen liittyen.

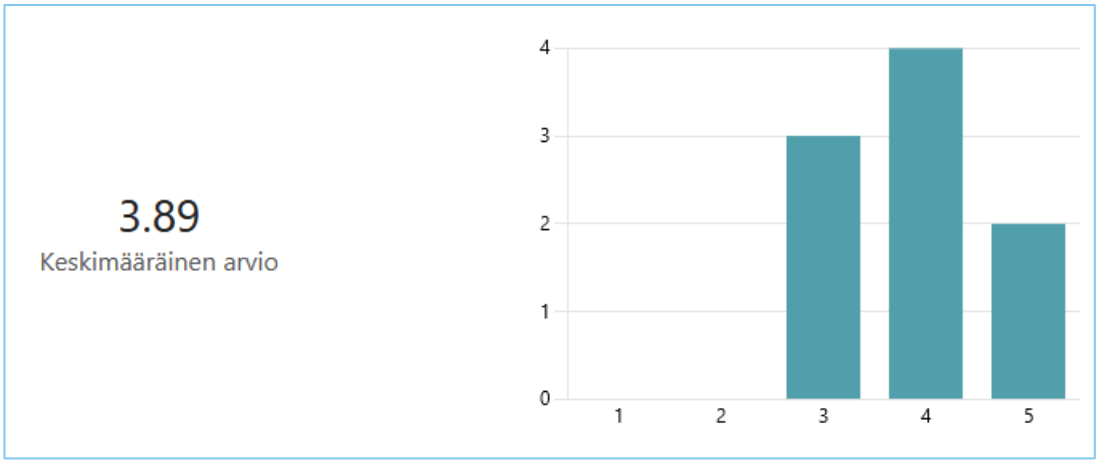
Tämä kysymys toteutettiin avoimena kysymyksenä, johon vastaajat voivat kertoa muista haasteista valmiiden vaihtoehtojen ohella muutoksiin liittyen. Vastauksia tuli yksi.

Avoimessa vastauksessa viitatiin ajan puutteeseen ja siihen, että muutokset melko hyvin tiedossa, etenkin jos on ollut mukana toteuttamassa useamman ISO/IEC 27001-sertifioinnin.

Vastauksen perusteella voidaan todeta, että ajanpuute ylipäänsä tuo haasteita muutosten implementointiin. Helpottava tekijä on, jos standardi ja tietoturvallisuuden hallintajärjestelmä (ISMS, Information Security Management System) ovat ennestään tuttuja.

Kysymys 10: Kuinka hyvin ISO/IEC 27001:2022 standardin päivityksen tuomiin muutoksiin organisaatiossanne suhtaudutaan yleisesti?

Kysymyksellä kartoitetaan yleistä suhtautumista standardin muutoksiin. Vastaus annettiin numeerisena arvona väliltä 1–5, jossa 1 on ”erittäin negatiivisesti” ja 5 on ”erittäin positiivisesti”. Tuloksista nähdään (kuvio 12), että keskimääräinen vastaus on 3,89, eli hyvin positiivisesti.



KUVIO 12. Organisaatioiden suhtautuminen standardin muutoksiin

Kysymys 11: Vapaa sana ja ajatuksia muutoksiin liittyen.
Kysymys esitettiin avoimena kysymyksenä, jolloin vastaajat pystyivät kirjoittamaan vapaasti ajatuksiaan aiheeseen liittyen.

Yhdessä avoimessa vastauksessa kaivattiin isompiakin muutoksia standardiin; maailma muuttuu ja standardien tulisi seurata aikaamme.

Toisessa avoimessa vastauksessa kerrottiin, miten paljon ISO/IEC 27001-sertifiointi on hyödyntänyt vastaajan organisaatiota.

Kolmas vastaaja kertoi muutosten olleen hyviä ja tarpeellisia. Vastaaja viittasi vuoden 2013 version selkeisiin puutteisiin ja vanhentuneisiin tietoihin, joihin päivitetty versio vastaa paremmin.

6.2 Kyselyn tuloksien pohdinta

Kyselyn vastausten perusteella voidaan todeta, ettei organisaation toimialalla tai sertifikaatin voimassaolon pituudella ole merkitystä siihen, millainen suhtautuminen organisaatiolla on standardin uudistuksiin. Otanta kyselyssä on suppea, joka vaikuttaa luotettavan yleiskuvan muodostamiseen organisaatioiden toimialan ja sertifikaatin voimassaolon vaikutuksista.

Lähes kaikki organisaatiot ovat aloittaneet uudistusten implementoinnin ja suurimpana haasteena nähdään muutoksiin perehtyminen ja resurssien saatavuus. Kolmasosa vastauksista osoittaa haasteiksi myös dokumentaation, sisäiset prosessit ja vaatimusten linkityksen liiketoimintaan. Tästä voidaan päätellä, että dokumentaation läpikäynti, päivittäminen ja luominen liitetään sisäisiin prosesseihin ja siihen, että resursseja, kuten aikaa ja henkilökuntaa, ei ole toteutukseen välttämättä riittävästi. Resurssien puutteen takia myös liiketoimintariippuvuuksien löytäminen voi olla työlästä sisäisten prosessien vuoksi. Resurssien ja käytettävän ajan puutteen vuoksi standardin dokumentaatioon perehtyminen, ja sitä kautta muutoksiin perehtyminen voi olla haastavaa. Tämä on vastanneilla organisaatiolla selkeästi tiedossa, sillä suurin osa on osittain varmistanut resurssien

saatavuuden. Eräs vastaaja kertoo, että suurin haaste on ajan puute, vaikka muutokset itsessään ovat melko selkeitä etenkin henkilöille, jotka ovat toteuttaneet useamman ISO/IEC 27001 -sertifioinnin.

Muutoksista on tarjolla tietoa ja useita yhteenvetoja internetin eri lähteissä. Vastaajista 55,6 % (n=9) on tutustunut muutoksiin, mutta muutoksien sisäistäminen vaatii myös tarkempaa organisaatiokohtaista perehtymistä. Uusia vaatimuksia tai kontrolleja ei kuitenkaan ole suurimmaksi osaksi lähdetty vielä toteuttamaan.

Vastaajista 66,7 % (n=9) on aloittanut muutoksien valmistelun aikataulutuksella. Lisäksi muutoksiin on tutustuttu ja 55,6 % (n=9) organisaatioista on myös tehnyt vastuunjaon muutoksiin liittyen. Suurimmassa osassa organisaatioita (77,8 % (n=9)) on työskennellyt yksi tietoturvapäällikkö sertifikaatin voimassaolon aikana tietoturvallisuuden hallintajärjestelmän parissa. Tämä voidaan nähdä positiivisena vaikutuksena, sillä tietoturvapäälliköt tuntevat paitsi organisaation liiketoiminnan ja prosessit, myös tietoturvallisuuden hallintajärjestelmän sertifioinnin alusta alkaen.

Yleisesti ottaen standardin muutoksiin suhtauduttiin positiivisesti. Organisaatiot arvioivat heidän sisäisen suhtautumisensa muutoksiin keskiarvollisesti 3,89/5, eli hyvin positiiviseksi. Sanalliset palautteet muutoksiin liittyen kertovat, että muutokset ovat tarpeellisia, vaikka ei välttämättä riittäviä. Standardin ja sertifioinnin itsessään nähdään myös hyödyttävän yritystä.

Yhteenvetona voidaan todeta, että organisaation toimialasta tai sertifikaatin iästä huolimatta haasteet ovat samat:

- muutoksiin perehtyminen
- organisaation tietoturvallisuuden hallintajärjestelmän dokumentaatio
- resurssien, etenkin ajan puute

Helpottavia tekijöitä on tietoturvapäälliköiden kokemus organisaatiosta, sertifikaatista ja tietoturvallisuuden hallintajärjestelmän ylläpidosta ja kehityksestä organisaatiokohtaisesti. Muutoksien suoraviivaisuus auttaa hahmottamaan tarvitta-

via toimenpiteitä. Vain yksi vastanneista organisaatioista aikoo käyttää muutoksessa ulkopuolista konsulttia. Ulkopuolisen konsultin hyödyntäminen voisi ratkaista suurimmaksi osaksi edellä mainitut haasteet muutokseen liittyen.

Tutkimuskyselyn otanta on suhteellisen pieni, mutta kattaa useamman eri toimialan. Vastanneilla organisaatioilla on myös hyvin hajontaa siinä, milloin sertifikaatti on tullut organisaatiolle voimaan. Tutkimuksen laatua voisi parantaa vielä laajemmalla otannalla, jonka saavuttamisessa auttaisivat pidempi vastausaika sekä muistutusviestit. Kyselyn toteutusta voisi myös harkita, koska verkossa tehtävät kyselyt eivät välttämättä tavoita kohdehenkilöitä niin kattavasti, kuin esimerkiksi henkilökohtainen haastattelu.

Sertifikaatin uudistukset tulee implementoida organisaatioissa lokakuuhun 2025 mennessä, jonka jälkeen voitaisiin tehdä jatkotutkimusta, miten tässä on onnistuttu ja miten implementointi on toteutettu. Samassa yhteydessä voitaisiin tutkia mitä käytännön toimenpiteitä ja strategioita organisaatiot käyttävät muutoksen hallitsemiseksi. Lisäksi voitaisiin tutkia miten uusi standardi vaikuttaa organisaatioiden tietoturvakulttuuriin ja tietoturvakäytäntöihin, sekä miten muutokset on implementoitu.

7 YHTEENVETO

Opinnäytetyön tarkoituksena oli perehtyä ISO/IEC 27001 -standardin vuoden 2022 muutoksiin, niiden vaikutuksiin organisaatiossa ja erilaisiin tapoihin toteuttaa muutos. Lisäksi verkkokyselyn avulla selvitettiin eri alojen organisaatioiden ajatuksia ja asenteita muutoksiin liittyen. Standardista ja sen muutoksista löytyy runsaasti yhteenvetoja ja tietoa internetistä, mikä helpotti tarvittavien lähteiden löytämistä. Lisäksi käytössä oli toimeksiantajan puolesta sekä vuoden 2013 että 2022 versiot, joita pystyttiin tätä työtä varten vertailemaan keskenään.

Opinnäytetyötä varten toteutettu kyselytutkimus osoittautui haastavaksi aiheen arkaluontoisuuden, lyhyen vastausajan ja toteutusmuodon vuoksi. Näistä tekijöistä huolimatta vastausprosentti oli melko hyvä, mutta ei korkea (28,13 %). Korkeamman vastausprosentin voisi saavuttaa pidentämällä vastausaikaa, lähettämällä osallistujille muistutusviestin kyselyyn osallistumisesta ja mahdollisesti toteuttamalla kysely esimerkiksi haastatteluna verkkokyselyn sijaan. Opinnäytetyössä toteutetun kyselytutkimuksen tulokset antoivat kuitenkin toivottua tietoa ja ymmärrystä kyselyn aiheeseen, ja niistä oli muodostettavissa selkeitä johtopäätöksiä.

Jokaisessa ISO/IEC 27001 -sertifioidussa organisaatiossa tietoturvallisuuden hallintajärjestelmä on erilainen ja palvelee nimenomaan kyseisen organisaation tarpeita ja liiketoimintaa. Tärkeintä muutoksien implementoinnissa on tuntea oman organisaationsa toimintamallit, prosessit ja tietoturvallisuuden hallintajärjestelmän dokumentaatio saumattoman siirtymän toteuttamiseksi. Opinnäytetyössä kehitetty aputyökalu tulee toivottavasti olemaan avuksi toimeksiantajan siirtymässä uuteen standardi-versioon ja tietoturvallisuuden hallintajärjestelmän kehittämisessä. Tarvittavien muutoksien suunnitteleminen ja resurssien saatavuus ovat avainasemassa onnistuneessa muutostyössä.

Opinnäytetyö opetti tietoturvallisuuden hallintajärjestelmästä ja ISO/IEC 27001 -standardista kokonaisuutena paljon. Tutkimuskysely vastauksineen antoi hyvää perspektiiviä siihen, kuinka muutokset kohdataan, miten niihin on valmistauduttu ja mikä muutoksissa koetaan haastavimmaksi.

LÄHTEET

ISO/IEC 27001. 2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardoimisliitto SFS. Luettu 20.4.2023. Vaatii käyttöoikeuden. https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stx

Aalto-yliopisto. 2022. Aalto-käsikirja - Jatkuvan kehittämisen periaate PDCA. Verkkosivu. Viitattu 31.3.2023. https://www.aalto.fi/fi/aalto-kasikirja/jatkuvan-kehittamisen-periaate-pdca

A-LIGN. n.d. What's the Difference Between ISO 27001:2013 and ISO 27001:2022? Verkkosivu. Viitattu 5.5.2023. https://www.a-lign.com/articles/blog-whats-the-difference-between-iso-27001-2013-and-iso-27001-2022

Bureau Veritas. n.d. Sertifiointipalvelut. Verkkosivu. Viitattu 30.3.2023. https://www.bureauveritas.fi/palvelumme/sertifiointi

Check Point. n.d. Check Point Software's 2023 Cyber Security Report. Verkkosi-vu. Viitattu 24.5.2023. https://pages.checkpoint.com/cyber-security-report-2023.html

Cysense. 2022. A Structure of The ISO/IEC 27001—Standard That You Need to Know. Verkkosivu. Viitattu 8.5.2023. https://www.cysense.io/blog/a-structure-of-the-iso-27001-standard-that-you-need-to-know

Global Compliance Certification. 2023. What is the difference between ISO 27001:2013 and ISO 27001:2022? Verkkosivu. Viitattu 8.5.2023. https://gccertification.com/iso-270012022/

GlobalSuite Solutions. 2022. What is SoA, Statement of Applicability? Verkkosivu. Viitattu 8.5.2023. https://www.globalsuitesolutions.com/what-is-a-statement-of-applicability-soa-and-how-useful-is-it/

IsecT Oy. 2021. ISO/IEC 27000:2018—Information technology—Security techni-ques—Information security management systems—Overview and vocabulary. Verkkosivu. Viitattu 25.3.2023. https://www.iso27001security.com/html/27000.html

ISMS.online. 2023a. ISO 27001:2022 Annex A Explained Verkkosivu. Viitattu 5.4.2023. https://www.isms.online/iso-27001/annex-a/

ISMS.online. 2023b. ISO 27001:2022 Annex A Explained Verkkosivu. Viitattu 5.4.2023. https://www.isms.online/iso-27001/annex-a/

ISO. 2013. Are you prepared for information security breaches? New ISO/IEC 27001 can help. Verkkosivu. Viitattu 5.5.2023. https://www.iso.org/news/2013/10/Ref1783.html

ISO. n.d. SFS Finland Verkkosivu. Viitattu 31.3.2023. https://www.iso.org/member/1734.html

IT Governance. 2022. Requirements for Achieving ISO 27001 Certification. Verkkosivu. Viitattu 24.5.2023. https://www.itgovernance.co.uk/blog/requirements-for-achieving-iso-27001-certification

Jyväskylän yliopisto. 2015. Määrällinen tutkimus. Verkkosivu. Viitattu 15.5.2023. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/maarallinen-tutkimus

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Jyväskylä: Docendo Oy.

Kiwa Inspecta. n.d.a. Mikä on akkreditointi? Verkkosivu. Viitattu 31.3.2023. https://www.kiwa.com/fi/fi/palvelutyyppi/sertifiointi-ja-arviointi/johtamisjarjestelmat/mika-on-akkreditointi/

Kiwa Inspecta. n.d.b. Mikä sertifikaatti on? Verkkosivu. Viitattu 31.3.2023. https://www.kiwa.com/fi/fi/palvelutyyppi/sertifiointi-ja-arviointi/johtamisjarjestelmat/mika-sertifikaatti-on/

Krypsys. 2023. Why Implement ISO 27001? Verkkosivu. Viitattu 6.5.2023. https://krypsys.com/services/iso-27001-consulting/

SFS. n.d.a. ISO/IEC 27000 Tietoturvallisuuden standardisarja. Verkkosivu. Viitattu 28.3.2023. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

SFS. n.d.b. ISO/IEC 27000 Tietoturvallisuuden standardisarja. Verkkosivu. Viitattu 29.3.2023. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

SFS. n.d.c. ISO/IEC 27000 Tietoturvallisuuden standardisarja. Verkkosivu. Viitattu 29.3.2023. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

Standard Fusion. 2021. ISO 27001 – Mandatory Clauses. Verkkosivu. Viitattu 8.5.2023. https://www.standardfusion.com/blog/iso-27001-mandatory-clauses/

The ISO 27000 Directory. 2021. An Introduction to ISO 27001, ISO 27002....ISO 27008. Verkkosivu. Viitattu 24.3.2023. http://www.27000.org/

Tietoturva pro. 2019. Ajantasaiset laitteet ja ohjelmistot eivät riitä, vaan tietoturvas-ta on tehtävä tapa toimia. Verkkosivu. Viitattu 26.3.2023. https://www.tietoturva.pro/

SFS. 2022. Tietoturvallisuuden hallintakeinojen standardi on uudistettu – mitä on muuttunut? Verkkosivu. Viitattu 29.3.2023. https://sfs.fi/tietoturvallisuuden-hallintakeinojen-standardi-on-uudistettu-mita-on-muuttunut/

Tilastokeskus. n.d. Kvalitatiivinen tutkimus. Verkkosivu. Viitattu 15.5.2023. https://www.stat.fi/meta/kas/kvalit_tutkimus.html

LIITTEET

Liite 1. Kyselylomake 1(4)

ISO27001:2022 tuomat muutokset organisaatiossa

Tällä kyselyllä kartoitetaan ISO27001-sertifioituneiden yritysten ja organisaatioiden valmiuksia ja asenteita kyseisen standardin uudistuksiin sekä uudelleensertifiointiin.

Kysely toteutetaan ja vastaukset käsitellään anonyymisti, eikä vastaukset ole yhdistettävissä vastaajaan.

Kysely toteutetaan osana Tampereen ammattikorkeakoulun tietotekniikan tutkinto-ohjelman opinnäytetyötä, jonka aiheena on "ISO27001:2022 tuomat muutokset organisaatiossa". Opinnäytetyö julkaistaan myöhemmin Theseus-palvelussa (https://www.theseus.fi/), jossa kyselyn kysymyksiä ja vastauksia käsitellään yleisellä tasolla.

Opinnäytetyön ja kyselyn toteuttaa kokonaisuudessaan opiskelija Iina Antila (iina.antila@tuni.fi).

* Pakollinen

1. Minä vuonna edustamasi organisaatio on sertifioitunut? *

Kirjoita vastaus

2. Mikä on organisaation toimiala? *

- Arkkitehtipalvelut ja tekninen suunnittelu
- Energiapalvelut, energian tuotanto
- Julkinen hallinto ja maanpuolustus; pakollinen sosiaaliturva
- Kiinteistöalan toiminta
- Lakiasiain- ja laskentatoimen toiminta
- Painaminen ja tallennus
- Pääkonttorien toiminta; liikkeenjohdon konsulttitoiminta
- Sähkö-, kaasu-, höyry- ja ilmastointihuolto
- Tietokoneiden sekä henkilökohtaisten ja taloustavaroiden korjaus
- Tietokoneohjelmointi, konsultointi ja niihin liittyvät toiminta
- Tietopalvelutoiminta
- Tietoliikenne
- Toimistopalvelut, tukipalvelut yritystoiminnalle ja liiketoiminnan hallinta
- En osaa vastata / En halua vastata
- Muu

3. Kuinka monta eri tietoturvapäällikköä on työskennellyt organisaatiossa sertifikaatin voimassaolon aikana tietoturvallisuuden hallintajärjestelmän parissa?

(Tietoturvapäällikkö = rooli, jonka tehtävä on suunnitella, kehittää ja johtaa organisaation tietoturvallisuuden hallintaa, mukaan lukien riskienhallinta, auditointi, raportointi ja yhteistyö organisaation osien ja sidosryhmien kanssa.) *

- ○ 1
- ○ 2
- ○ 3 tai enemmän
- ○ En osaa vastata
- ○ En halua vastata
- ○ Muu

4. Onko organisaatiossanne aloitettu valmistautuminen uusien ISO27001:2022 standardin vaatimusten täyttämiseksi? *

- ○ Kyllä
- ○ Ei
- ○ Ei varmaa tietoa
- ○ En halua vastata

5. Miten organisaationne on suunnitellut muutoksen hallinnan ISO27001:2022 standardin uusien vaatimusten osalta? *

Voit valita yhden tai useamman vastausvaihtoehdon.

- ☐ Muutos on suunniteltu
- ☐ Muutos on aikataulutettu
- ☐ Muutosten vastuunjako on tehty
- ☐ Muutoksiin on tutustuttu
- ☐ Muutoksen hallintaan käytetään ulkoista konsulttia, tmv.
- ☐ En halua vastata
- ☐ Ei mikään näistä
- ☐ Muu

6. Onko organisaatiossanne jo lähdetty toteuttamaan ISO27001:2022 standardin myötä uudistuneita vaatimuksia ja kontrolleja? *

- ◯ Kyllä
- ◯ Ei
- ◯ Osittain
- ◯ Ei varmaa tietoa
- ◯ En halua vastata

7. Onko organisaatiossanne varmistettu, että tarvittavat resurssit, kuten taloudelliset, teknologiset ja henkilöstöresurssit ovat käytettävissä ISO27001:2022 standardin muutosten toteuttamiseen? *

- ◯ Kyllä
- ◯ Ei
- ◯ Osittain
- ◯ Ei varmaa tietoa
- ◯ En halua vastata

8. Mitkä ovat organisaationne suurimmat haasteet ISO27001:2022 standardin muutosten implementoinnissa? *

Voit valita yhden tai useamman. Muu-kentään voit kirjoittaa useamman haasteen.

- ☐ Dokumentaatio
- ☐ Riskienhallintaprosessi
- ☐ Sisäiset prosessit
- ☐ Muut prosessit
- ☐ Muutoksiin perehtyminen
- ☐ Aikataulujen hallinta
- ☐ Vaatimusten linkitys organisaation liiketoimintaan
- ☐ Resurssien saatavuus
- ☐ Muutosvastaisuus
- ☐ Johdon tuki
- ☐ En halua vastata
- ☐ Muu

9. Kerro halutessasi tarkemmin haasteista organisaatiossa muutokseen liittyen:

Kirjoita vastaus

10. Kuinka hyvin ISO27001:2022 standardin päivityksen tuomiin muutoksiin organisaatiossanne suhtaudutaan yleisesti?

1 = erittäin negatiivisesti
5 = erittäin positiivisesti

1	2	3	4	5

11. Vapaa sana ja ajatuksia muutoksiin liittyen:

Kirjoita vastaus

Lähetä

Liite 2. Saatekirje 1(1)

Hei,

Olen Iina Antila ja teen opinnäytetyötä Tampereen ammattikorkeakoulun tietotekniikan tutkinto-ohjelman hyväksynnällä aiheesta "ISO27001:2022 standardin muutokset organisaatiossa". Opinnäytetyöni tavoitteena on selvittää standardin päivityksen keskeisiä muutoksia ja vaikutuksia. Osana opinnäytetyötä toteutan kyselyn, jolla selvitän organisaatioiden valmiutta ja asenteita ISO27001:2022 standardin muutoksiin liittyen.

Kutsun teitä osallistumaan opinnäytetyöhöni vastaamalla alla olevaan kyselyyn. Vastauksenne ovat tärkeitä opinnäytetyöni onnistumisen kannalta ja auttavat kehittämään organisaatioiden turvallisuutta entistä paremmaksi. Opinnäytetyö julkaistaan sen valmistuttua Theseus-palvelussa (https://www.theseus.fi/) ja toivon siitä olevan iloa sekä hyötyä myös vastanneille organisaatioille.

Linkki kyselyyn: https://forms.office.com/e/3BudvRcr1Q (lyhennetty linkki)
*Vastaathan kyselyyn **15.5.2023** mennessä.*

Kyselyyn vastaaminen kestää noin 5 minuuttia ja vastauksia käsitellään luottamuksellisesti. Kysymyksiä on yhdeksän ja vapaaehtoisia avoimia kysymyksiä kaksi. Vastaukset käsitellään anonyymisti, eikä vastauksia yhdistetä yksittäisiin henkilöihin tai organisaatioihin. Kysely-lomake on toteutettu Microsoft Forms-työkalulla. Opinnäytetyön valmistuttua raportoin tulokset vain yleisellä tasolla.

Mikäli teillä on kysyttävää opinnäytetyöstäni tai kyselystä, voitte ottaa yhteyttä minuun sähköpostitse. Mikäli et ole oikea henkilö organisaatiossasi vastaamaan kyselyyn, voit välittää viestini sopivalle henkilölle.

Kiitän jo etukäteen osallistumisestanne opinnäytetyöhöni ja avustanne tutkimuksessani.

Terveisin | Best regards,

Iina Antila

TAMK | tietotekniikan tutkinto-ohjelma
ryhmä 20TIETOA
iina.antila@tuni.fi
LinkedIn