ISO 27001 vastauksena EU:n yleisen tietosuoja-asetuksen vaatimuksiin

Petri Vetikko

Opinnäytetyö
Marraskuu 2018
Liiketalous
Oikeudellinen asiantuntijuus

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalous
Oikeudellinen asiantuntijuus

VETIKKO PETRI:
ISO 27001 vastauksena EU:n yleisen tietosuoja-asetuksen vaatimuksiin

Opinnäytetyö 41 sivua
Marraskuu 2018

Tässä opinnäytetyössä keskityttiin löytämään yhteys tietosuoja-asetuksen ja ISO 27001 –standardin tuomien ratkaisumallien välillä. Pääosin lähteinä toimivat tietosuoja-asetus itse vaatimusten osalta, ja standardi sen tuomien ratkaisukeinoja osalta. Johdantona asetukseen ja itse aiheeseen esitellään EU:n digitaalisten sisämarkkinoiden strategia sekä kyberturvallisuusstrategia, jota on tutkittu EU:n omien julkaisujen pohjalta. Kummatkin strategiat koskettavat ja vaikuttavat merkittävään osaan EU:n kansalaisia, yrityksiä ja toimintaa.

Tietosuoja-asetuksesta avataan yrityksille esitetyt vaatimukset siltä osin, kun ne ovat tarpeellisia ISO 27001 –standardin suojakeinojen selittämiseksi. Asetuksen vaatimuksista tärkeimpinä avataan osoitusvelvollisuus, ilmoitusvelvollisuus, riskiperustainen lähestymistapa ja sisäänrakennettu tietosuoja. Vastauksena asetuksen asettamiin haasteisiin esitetään ISO 27001 –standardin tuomia ratkaisumalleja.

ISO 27001 –standardista kuvataan standardin asettamat pakolliset vaatimukset, jotka yrityksen tai organisaation on toteutettava noudattaakseen standardin määräyksiä. Samoin kuvataan standardin sataneljätoista vapaaehtoista vaatimusta, joista yritys tai organisaation voi perustellusti valita mitkä osat se toteuttaa ja erityisesti perusteella pois jätettävät osat.

Tutkimusmenetelmä on kirjallisuustutkimus, standardiin ja sen tietosuojaan liittyviin menetelmiin perehtymisen muodossa, sekä standardin tuomat ratkaisumallit. Ratkaisumalleista tärkeimmiksi nousee riskiperustainen lähestymistapa, joka säännöllisesti toteutettuna pitää yrityksen ajan tasalla siihen kohdistuvista riskeistä myös tietosuojan osalta. Ydinkysymyksenä on, miten yrityselämä voi varautua tietosuoja-asetuksen asettamiin vaatimuksiin.

Opinnäytetyön kirjoittamisen aikana tehtiin myös ISO 27001 sertifiointiprojektia Pirkanmaalla sijaitsevalle yritykselle. Yrityksen toiminnot on tarkoitus virtaviivaistaa standardin mukaiseksi ja lopulta sertifioida koko yritys ISO 27001 –standardiin. Opinnäytetyössä kuvataan standardin toteutuksen prosessi, mutta ei kuitenkaan syvennytä itse standardointiprosessin etenemiseen yrityksessä.

---

tietosuoja-asetus, ISO 27000, ISO 27001, kyberturvallisuus

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Administration
Legal Expertise

PETRI VETIKKO:
ISO 27001 to Meet the Requirements of the EU GDPR

Bachelor's thesis 41 pages
November 2018

This thesis focused on finding common ground between the General Data Protection Regulation GDPR and the ISO 27001 standard family. The information on the requirements was found in the GDPR itself, and the ISO 27001 standard worked as a model to meet the requirements. As an introduction to the subject, the EU digital single market strategy as well as cybersecurity strategy were presented, and both of them were studied on the basis of the EU publications. Both strategies have a significant role for the EU citizens, organizations and operations.

The thesis opens the GDPR requirements to the companies to the relevant extent that is needed to explain the data protection means of the ISO standard. The most important requirements described are the following: the demonstration of compliance, the notification in the case of a data breach, risk-based approach and built-in privacy. To meet the GDPR requirements, the thesis presents models offered by the ISO 27001 standard.

The ISO 27001 standard includes obligatory requirements that every organization shall com-ply with, and voluntary requirements that are voluntary to the organization. The organization must choose the voluntary requirements that it is going to comply with. Both categories are described in this thesis.

The research method in the thesis was a literature study, by the means of studying the standard and its methods for data security, and practical life solutions. The risk-based approach becomes most important, as it, when implemented regularly, keeps the company informed about its risks in the data privacy, too. The core issue is how the business can prepare for the requirements set by the GDPR.

At the same time with the thesis work, the ISO 27001 standardising project was going on in a company in Pirkanmaa. The company’s operations are to be streamlined with the standard, and finally the entire company will be certified. The thesis describes the implementation process of the standard but does not focus on the actual standardising project in the company.

GDPR, ISO 27000, ISO 27001, cyber security

SISÄLLYS

LYHENTEET JA TERMIT

AI	Artificial Intelligence, tekoäly. Tietoa käsittelevistä, oppivista automaatio-ohjelmistoista käytetään usein nimitystä Artificial Intelligence, tekoäly ja se lyhennetään muotoon AI. Varsinainen älykkyys ohjelmistoissa on vielä saavuttamatta.
Anonymisointi	Anonymisoinnilla pyritään siihen, että tiedosta tulee sellaista, ettei sitä voida missään tilanteessa yhdistää tiettyyn henkilöön.
Auditointi	Auditoinnilla (arvioinnilla) selvitetään, miten toiminta täyttää tietyt kriteerit. Tämä arviointi on pistokoeluonteinen otos yrityksen toiminnasta. Auditoinnin voi tehdä myös organisaatio itse (sisäinen auditointi) tai organisaation sidosryhmä, esimerkiksi asiakas tai ns. kolmas osapuoli. Auditoinnin seurauksena yritys voi saavuttaa sertifioinnin tietyn standardin mukaiseksi.
GDPR	General Data Protection Regulation. EU:n yleinen tietosuoja-asetus.
IEC	International Electrotechnical Commission, kansainvälinen sähköalan standardointiorganisaatio
ISO	International Organization for Standardization, kansainvälinen standardisoimisjärjestö.
ISO 27000	ISO/IEC –standardiperhe, joka käsittelee tietoturvallisuuden hallintajärjestelmiä. 27000 viittaa yleiskatsaukseen ja sanastoon.
ISO 27001	Standardiperheen numerosarja 27001 viittaa standardin asettamiin vaatimuksiin.
ISO 27002	Standardiperheen numerosarja 27002 viittaa standardin tietoturvallisuuden hallintaa koskeviin menettelyohjeisiin.
ISO 27003	Standardiperheen numerosarja 27001 viittaa standardin toteuttamisohjeisiin.
ISO 27004	Standardiperheen numerosarja 27004 viittaa standardin tietoturvan mittaamiseen.

ISO 27005	Standardiperheen numerosarja 27005 viittaa standardin ohjeisiin tietoturvariskien hallinnasta.
LIBE-valiokunta	Euroopan parlamentin kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta on Euroopan parlamentin pysyvä valiokunta.
NIST	The National Institute of Standards and Technology on yhdysvaltalainen virasto, jonka tehtävänä on kehittää ja edistää mittaustekniikoita, standardeja ja tekniikkaa. Virasto toimii Yhdysvaltojen kauppaministeriön alaisuudessa.
Pseudonymisointi	Henkilöön yhdistettävästä tiedosta henkilötieto korvataan siten, että se ei enää ole yhdistettävissä kyseiseen henkilöön. Pseudonymisoitu tieto on kuitenkin lisätietojen avulla yhdistettävissä yksittäiseen henkilöön.
Sertifikaatti	Todistus siitä, että toiminta vastaa standardin vaatimuksia.
Sertifiointi	Sertifiointi tarkoittaa yritystoiminnan arvioimiseen perustuvaan todistuksen (sertifikaatin) myöntämistä. Sertifiointi perustuu yrityksessä paikan päällä tehtävään arviointiin (auditointi). Arvioinnin seurauksena yritys voidaan sertifioida eli varmentaa, että toiminta on standardin mukaista.
Tietosuoja	Tietosuoja-termiä käytetään, kun kyseessä on henkilötietojen suojaaminen.
Tietoturva	Tietoturva viittaa tietojen, järjestelmien ja palveluiden toiminnan suojaamiseen.
WLAN	WLAN (ensimmäiset kirjaimet sanoista Wireless Local Area Network) on langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita.

1 JOHDANTO

1.1 Taustaa

Tämän opinnäytetyön tarkoituksena on syventyä EU:n Digitaaliset sisämarkkinat-strategiaan ja selventää tietosuoja-asetuksen merkitytä yrityskentälle. Samaan aikaan tavoitteena on perehtyä ISO 27001 –standardin tuomiin ratkaisumalleihin, kehittää omaa tietotaitoa sekä kyberturvallisuuden, että EU:n lainsäädännön ja eritoten tietosuoja-asetuksen ja ISO 27001 –standardin saralla. Kyberturvallisuus ja EU:n digitaaliset sisämarkkinat-strategia toimivat johdantona aiheeseen, sillä ne toimivat perustana, jonka pohjalta tietosuoja-asetus on tehty.

Tietosuoja-asetuksesta avataan yrityksille esitetyt vaatimukset henkilötietojen suojaamisesta siltä osin, kun ne ovat tarpeellisia ISO 27001 –standardin suojakeinojen selittämiseksi. Lainlaatija ei luota, täydestä syystä, tietosuojan tuottamisessa yrityksien omiin motivaationlähteisiin, tahtoon ja pelkoon, vaan tuo yrityksille uuden motivaation lähteen, pakon. Pakon sanelemana vuoden 2018 alkupuolella monissa yrityksissä onkin käynnistetty tietosuoja-asetukseen liittyviä projekteja ja vielä asetuksen voimaantulon jälkeenkin tietosuoja-asetusprojektit jatkuvat, sillä alue on laaja ja yritysten järjestelmät monimutkaisia.

Lopuksi, vastauksena asetuksen asettamiin haasteisiin esitetään ISO 27001 –standardin tuomia ratkaisumalleja. Standardi tuo mukanaan seitsemän pakollista vaatimusta, jotka yrityksen on toteutettava ja sataneljätoista valinnanvaraista hallintakeinoa, joista yrityksen on jokaiseen perusteltava kyseisen hallintakeinon tarpeellisuus.

1.2 Menetelmät

Tutkimusmenetelmä on kirjallisuustutkimus, standardiin ja sen tietoturvaan liittyviin menetelmiin perehtymisen muodossa, sekä ISO 27001 –standardin tuomat ratkaisumallit. Lainopillinen tutkimus tapahtuu tietosuoja-asetuksen ja ISO 27001 –standardin vertailun muodossa. Ydinkysymyksenä onkin, miten yrityselämä voi varautua tietosuoja-asetuksen, eli GDPR:n asettamiin vaatimuksiin. Standardin osasta 27001 puhuttaessa viitataan

myös usein muihin standardiperheen osiin, siksi tässä selvityksessä vieraillaan koko standardiperheessä, niiltä osin, kun on tarvetta tarkentaa 27001:n eri osia tai yksityiskohtia.

Opinnäytetyön kirjoittamisen aikana tehtiin myös ISO 27001 sertifiointiprojektia Pirkanmaalla sijaitsevalle yritykselle. Yrityksen toiminnot on tarkoitus virtaviivaistaa standardin mukaiseksi ja lopulta sertifioida koko yritys ISO 27001 –standardiin. Opinnäytetyössä kuvataan standardin toteutuksen prosessi, mutta ei kuitenkaan syvennytä itse standardointiprosessin etenemiseen yrityksessä.

2 EU: N DIGITAALISET SISÄMARKKINAT-STRATEGIA

2.1 Strategian kehittyminen

EU maiden sisämarkkina-ajatus on edennyt digitaalisten sisämarkkinoiden kehittämisen asteelle. Strategian kehittämisellä pyritään varmistamaan, että Euroopan digitaalitalouden kasvupotentiaali maksimoidaan (Digitaaliset sisämarkkinat, 4). Varmistetaan siis, että strategia tuo täyden hyödyn taloudelle, teollisuudelle ja yhteiskunnalle. Digitaaliset sisämarkkinat tarkoittavat vapaata verkkokaupankäyntiä kaikkialla EU:n alueella.

Vuosia aikaisemmin alkunsa saanut keskustelu digitaalisista sisämarkkinoista sai tärkeän merkkipaalun, kun tietosuoja-asetus hyväksyttiin 2016. Komissio myös raportoi säännöllisesti strategian edistymisestä (Digitaaliset sisämarkkinat, 20). Tietosuoja-asetuksen jälkeen sisämarkkinastrategia on edennyt muun muassa verkkovierailumaksujen lopettamisen muodossa. Tänä päivänä Euroopan alueella matkustaessa matkapuhelimen dataominaisuuksia voikin käyttää rauhallisin mielin ilman pelkoa ylisuurista tiedonsiirtomaksuista.

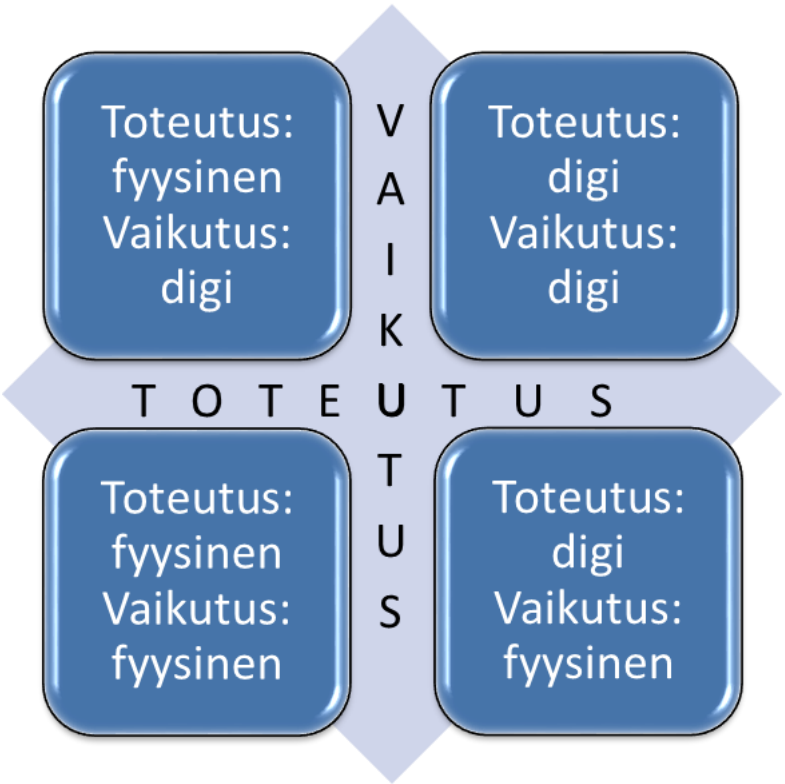
2.2 Strategian merkitys

Digitaalitalouden esteiden purkaminen Euroopasta voisi kasvattaa EU:n BKT:tä jopa 415 miljardilla eurolla (Digitaaliset sisämarkkinat, 3). Lisätulot toiminnan tehostamisen ja sääntelyn yhdenmukaistamisen seurauksena ovat merkittäviä.

Digitaaliteknologioiden avulla voitaisiin automatisoida huomattava osa ihmisten päivittäisistä työtehtävistä, ja joillakin aloilla lähes kaikki tehtävät edellyttävät digitaaliosaamista. Digitalisoinnin ja automatisoinnin rinnalle on noussut myös tekoäly, AI, josta muun muassa Helsingin Yliopisto ja Reaktor yhteistyössä ovat tarjonneet kaikille vapaata verkkokoulutusta. Kurssi opettaa kaikille halukkaille, mitä tekoäly on nykypäivänä ja mitä se voi olla tulevaisuudessa. Tulevaisuuden ihmisen kannalta kaikki tämä tarkoittaa täysin uudenlaisia vaatimuksia osaamiselle ja koulutustarpeille, myös kyberturvallisuuden alueella.

2.3 Kyberturvallisuus

Kyberturvallisuutta voidaan kuvata nelikentän avulla, jossa vaaka-akselilla kyberhyökkäysten toteutustapaa kuvataan skaalalla toteutus digimaailmassa-toteutus fyysisessä maailmassa. Pystyakselilla kuvataan vaikutuksia skaalalla vaikutus digimaailmassa-vaikutus fyysisessä maailmassa. Mallin on esittänyt Jarno Limnéll luennoillaan. Nelikenttä esitettynä kuviossa 1.



KUVIO 1. Kyberturvallisuuden nelikenttä (mukaillen Limnéll, luentoesitys)

Nelikentässä esimerkiksi erilaiset verkkopalvelut sijoittuvat sekä toteutuksiltaan, että vaikutuksiltaan digimaailmaan. Tällöin sekä kyberhyökkäys tapahtuu digitaalisesti ja sen vaikutukset osuvat myös digimaailmaan. (Limnéll, luentoesitys.) Esimerkiksi verkkopalvelun toimintaa voidaan hankaloittaa palvelunestohyökkäyksen avulla. Tällaisessa hyökkäyksessä koko verkkopalvelu kuormittuu niin paljon, että se ei enää ehdi vastaamaan aitoihin verkkopalvelua käyttävien asiakkaiden hakuihin. Tällöin esimerkiksi verkkokaupan kaupankäynti pysähtyy ja aiheuttaa huomattavia tulonmenetyksiä verkkokaupalle ja asiakas jää ilman haluamaansa tuotetta.

Tietojärjestelmän laitteet, kuten reitittimet, joita voidaan vahingoittaa fyysisesti ja seuraukset näkyvät verkon toiminnassa, sijoittuvat kuviossa toteutukseltaan fyysiseen maailmaan ja vaikutukseltaan digimaailmaan (Limnéll, luentoesitys). Reitittimet sijaitsevat usein esimerkiksi kerrostalojen kellarikerroksissa kevyiden ovien ja lukkojen takana ja niihin murtautumalla voidaan helposti hajottaa kyseinen laite tai vain yksinkertaisesti sammuttaa laite. Näin toimien hyökkääjä aiheuttaa kustannuksia operaattorille, joka joutuu korjaamaan laitteen paikan päällä. Palvelua käyttävälle kerrostalon asukkaalle tämä näkyy verkkopalveluiden täydellisenä katoamisena. Tällöin kaikki kyseisen yhteyden takan olevat palvelut, esimerkiksi verkkoon tallennettujen televisio-ohjelmien katselu on mahdotonta.

Yhteiskunnan kriittiset toiminnot, esimerkiksi sähkölaitokset, ovat vaikutukseltaan fyysisessä ja toteutukselta digitaalisessa kentässä (Limnéll, luentoesitys). Maailmalta onkin useita esimerkkejä, jossa sähkölaitoksiin on hyökätty erilaisten haittaohjelmien avulla ja näin haitattu ihmisten jokapäiväistä elämää (CNN, 2016). Laajamittainen sähkökatkos voi aiheuttaa jopa terveyteen kohdistuvaa uhkaa, mikäli sen vaikutuksen osuvat esimerkiksi kirurgisia palveluja ja leikkauksia tarjoavaan yritykseen.

Sekä vaikutuksiltaan, että seurauksiltaan fyysisessä maailmassa on esimerkiksi terroristisku. Tänä päivänä digitaalisia apuvälineitä, esimerkiksi viestinnässä ja näkyvyyden hakemisessa, käytetään usein myös näiden toteutuksessa, mikä osoittaakin sen, että nelikentän eri osa-alueet ovat päällekkäisiä toistensa kanssa.

Lisää ongelmia kyberturvallisuudelle aiheuttaa muun muassa se, että ”Esineiden internet" on jo todellisuutta, ja arvioiden mukaan vuoteen 2020 mennessä siihen on kytkettynä kymmeniä miljardeja digilaitteita EU:ssa” (Kyberturvallisuuden uudistus Euroopassa, 2017). Jo nyt kyberrikolliset käyttävät esineiden internettiä hyökkäyksien toteuttamiseen erilaisia verkkopalveluita vastaan.

2.4 Tietosuoja eli henkilötietojen suojaaminen

Tietosuoja-termiä käytetään, kun kyseessä on henkilötietojen suojaaminen. Henkilötietolain mukaan henkilötiedot jaotellaan arkaluonteisiin henkilötietoihin ja muihin tunnistettuun tai tunnistettavissa olevaan henkilöön liittyvät tiedot. Arkaluonteisia henkilötietoja henkilötietolain (Henkilötietolaki 523/1999) 3 luvun 11§ mukaan ovat

1) rotua tai etnistä alkuperää;
2) henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;
3) rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;
4) henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;
5) henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka
6) henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Ilman arkaluonteistakin tietoa voidaan yksityistä henkilöä kohtaan hyökätä muun muassa avoimesta datasta löytyvän tiedon perusteella. Tutkimuksessaan ”Unique in the shopping mall: On the reidentifiability of credit card metadata”, de Montjoye, Radaelli, Singh, & Pentland vuonna 2015 todistavat että henkilökohtaisen, identifioivan tiedon poistaminen tai sekoittaminen ei ole riittävä suojauskeino yksilön kannalta.

Tutkimuksessa (De Montjoye, 2015) kuvataan, kuinka 1.1 miljoonaa käyttäjän luottokorttitietoa voidaan yhdistää sosiaalisesta mediasta saatavaan tietoon. Tietoja yhdistämällä tutkijat pystyivät 90 prosenttisesti yhdistämään käyttäjän ja kortin, vaikka kyseiset tiedot oli poistettu luottokorttidatasta. Esimerkiksi, yksittäisen henkilön löytämiseen anonymisoidusta luottokorttidatasta riitti seuraavat tiedot: leipomossa käynti ja sen päivämäärä ja ravintolassa käynti ja sen päivämäärä. Kun luottokorttiostoksia etsittiin näillä tiedoilla, osoittautui, että vain yksi henkilö oli asioinut kyseisissä paikoissa samoina päivinä ja näin kyseinen henkilö ja hänen korttinsa oli löytynyt ja samalla kaikki muutkin hänen tekemänsä ostokset.

Samaa asiaa on käsitelty myöhemmissä tutkimuksissa muun muassa The National Institute of Standards and Technology:n (NIST) toimesta vuonna 2015. Tuorein tutkimus ai-

heesta on Melbournen yliopistossa tehty tutkimus joulukuussa 2017 (Culnane, Rubinstein, Teague, 2017). Tutkimuksessa käsitellään Australian avointa terveysdataa, josta henkilötiedot on anonymisoitu. Tutkimuksen mukaan henkilöjä voidaan tunnistaa julkisesti saatavilla olevan tiedon avulla aikaisemmin kuvatulla tavalla.

2.5 Kyberturvallisuus ja tietosuoja osana strategiaa

Kyberturvallisuus on osa EU:n digitalisointi-strategiaa. ”EU-johtajat pitävät kyberturvallisuusuudistusta yhtenä tärkeimmistä tekijöistä digitaalisten sisämarkkinoiden toteuttamiseen tähtäävissä toimissa” (Kyberturvallisuuden uudistus Euroopassa, 2017). Tämä onkin melko luonnollinen lausuma, kun seuraa tämän päivän uutisointia erilaisista tietoturvaongelmista.

Toisaalta taas ”kyberhyökkäysten arvioidaan maksavan maailmantaloudelle 400 mrd. € vuosittain” (Kyberturvallisuuden uudistus Euroopassa, 2017). Ottaen huomioon digitaalisten sisämarkkinoiden tuomat hyödyt ja kyberturvallisuuden puutteiden aiheuttamat kustannukset, ei digitalisaatio ilman tietosuojaa ja kyberturvaa enää vaikutakaan niin kannattavalta. Tämän vuoksi strategian kehittämiseen on panostettu EU tasolla ja eritoten huomio on kiinnitetty kyberturvallisuuteen ja tietosuojaan.

3 EU: N YLEINEN TIETOSUOJA-ASETUS

3.1 Tietosuoja-asetuksen taustat

Euroopan parlamentti ja neuvosto saivat 15.12.2015, neljän vuoden neuvotteluiden jälkeen, valmiiksi lopullisen version tietosuoja-asetuksen sisällöstä ja Euroopan parlamentin LIBE-valiokunta vahvisti uuden asetuksen sisällön äänestyksessään 17.12.2015 (LIBE, 2015). Uusi tietosuoja-asetus hyväksyttiin 24.5.2016 ja tuotiin julki EU:n oikeudellisten asiakirjojen virallisessa julkaisukanavassa, Euroopan unionin virallisessa lehdessä. Asetus astui voimaan kahden vuoden siirtymäajan jälkeen 25.5.2018. (Yleinen tietosuoja-asetus, 99 artikla.) Asetus korvaa Suomen nykyisen henkilötietolain (523/1999) ja Euroopan unionin direktiivin 95/46/EY ja siten se vaikuttaa suoraan kaikkiin yrityksiin, jotka toiminnassaan käsittelevät henkilötietoja.

Vanhat tietosuojalait pohjautuvat EU:n tietosuojadirektiiviin vuodelta 1995 eli aikaan, jolloin Internet ja digitaaliset palvelut olivat vasta lapsenkengissä verrattuna kaksikymmentä vuotta myöhäisempään suosioonsa. Uusi asetus harmonisoi Euroopan Unionin jäsenvaltioissa nykyisin voimassaolevat tietosuojalait ja määrittää yhteiset säännöt henkilötietojen käytölle. (EU Info, 2017.)

3.2 Uusi tietosuoja-asetus

Asetus, kuten se on Euroopan unionin virallisessa lehdessä nimetty: ” EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (Yleinen tietosuoja-asetus, 1)”, koskee kaikkia organisaatioita, jotka EU:n alueella käsittelevät henkilörekistereitä ja niiden tietoja.

EU:n pyrkimys harmonisointiin EU-maiden välillä on samalla pyrkimys luoda eurooppalaiset sisämarkkinat (EU Info, 2017). Yhteisellä lainsäädännöllä yritysten toiminta hel-

pottuu ja niille riittää asiointi yhden maan tietosuojaviranomaisen kanssa. Samalla korostetaan oikeutta omiin tietoihinsa sekä yksityisyyttä perusoikeutena. Tietosuoja-asetus asettaa useita vaatimuksia yrityksille ja organisaatioille ja oikeuksia yksityishenkilöille.

3.3 Osoitusvelvollisuus

Yksi suurimmista tietosuoja-asetuksen vaikutuksista kohdistuu yritysten ja organisaatioiden osoitusvelvollisuuteen. Asetuksen mukaan yritysten ja organisaatioiden on osoitettava, että ne noudattavat rekisterinpitäjälle asetettuja velvollisuuksia lainmukaisuudesta, kohtuullisuudesta ja läpinäkyvyydestä, käyttötarkoitussidonnaisuudesta, tietojen minimoinnista, täsmällisyydestä, säilytyksen rajoittamisesta ja eheydestä ja luottamuksellisuudesta (Yleinen tietosuoja-asetus, 5 artikla).

Kaikki edellä mainittu korostaa yrityksen tarvetta dokumentoida kaikki politiikkansa, prosessinsa ja ohjeistuksensa, sekä säilyttää palaveri- ynnä muut muistiot, jotka osoittavat, miten yrityksessä toimitaan. Samoin tietosuoja-asetuksessa suositellaan sertifiointimekanismeja sekä tietosuojasinettejä ja -merkkejä, joiden ”tarkoituksena on osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat käsittelytoimia” (Yleinen tietosuoja-asetus, 42 Artikla). Sertifiointi tai sertifikaatin mukaisesti toimiminen tuo mukanaan myös mainitut dokumentointivaatimukset.

3.4 Riskiperustainen lähestymistapa

Asetuksen toinen oleellinen lähtökohta on riskiperustainen lähestymistapa, jonka mukaan ”rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet” (Yleinen tietosuoja-asetus, 32 artikla). Tämä tarkoittaa, että suojauskeinoissa otetaan huomioon muun muassa nykyinen tekniikka ja suojauskeinojen toteuttamiskustannukset ja henkilötietojen käsittelyn luonne (Yleinen tietosuoja-asetus, 32 artikla).

Samaa asiaa tarkennetaan tietosuojaa koskevaa vaikutustenarviointia käsittelevässä artiklassa (Yleinen tietosuoja-asetus, 34 artikla) ja 36 artiklassa, ennakkokuuleminen. Ensim-

mäisessä artiklassa korostetaan vaikutusten arviointia ja jälkimmäisessä uudelleenarviointia riskin muuttuessa. Tämän tutkimuksen luvussa Riskien hallinta kuvataan, miten ISO 27001 –standardi vastaa asetuksen vaatimuksiin.

3.5 Sisäänrakennettu tietosuoja

Tietosuoja-asetuksen 25 artiklassa korostetaan tietosuojan rakentamista sisään yrityksen teknisiin ratkaisuihin ja käytäntöihin. Tämä voidaan saavuttaa artiklan mukaan toteuttamalla teknisiä ja organisatorisia toimenpiteitä, kuten pseudonymisointi ja muita suojatoimenpiteitä. Samoin 25 artiklassa korostetaan myös, että oletusarvoisesti käsitellään vain tarpeellisia henkilötietoja. Sisäänrakennettuna tämä tarkoittaa siis suojaavien toimenpiteiden sisällyttämistä yrityksen prosesseihin ja käytäntöihin.

Nämä toimenpiteet voi osoittaa esimerkiksi sertifiointimenettelyjen, kuten ISO 27001 –standardin avulla. Standardissa on vaatimuksia muun muassa salauksen käytölle viestinnässä. Mikäli yrityksessä on tarvetta viestiä esimerkiksi erityisiä henkilötietoja, standardin toteuttaminen antaa esimerkiksi salausvaatimuksen muodossa mahdollisuuden sisäänrakennetun tietosuojavaatimuksen toteuttamiseen. ISO 27001 –standardi on tarkoitus toteuttaa yrityksissä siten, että se sisältyy sopivilta osin kaikkiin yrityksen päivittäisiin toimintoihin.

3.6 Ilmoitusvelvollisuus

33 artiklassa asetetaan vaatimus henkilötietojen tietoturvaloukkauksista ilmoittamiselle 72 tunnin kuluessa valvontavirnaomaiselle. Samoin artiklan mukaan ilmoitusvaatimuksesta poikkeamiselle on annettava perusteltu selitys valvontaviranomaiselle. Vastaava ilmoitus on tehtävä myös rekisteröidylle itselleen. (Yleinen tietosuoja-asetus, 34 artikla.)

Jotta yritys tai organisaatio pystyy vastaamaan kummankin artiklan vaatimuksiin, sen tulee luoda asianomaiset prosessit, käytännöt ja vastuunjaot jo etukäteen. Tässäkin tapauksessa ISO 27001 –standardi tuottaa lisäarvoa toteuttajalleen, sillä etukäteen valmistellut prosessit, käytännöt ja vastuunjaot sisältyvät ISO 27001 –standardin toteutukseen.

3.7 Muut vaatimukset

Tietosuoja-asetuksen vaatimukset, joihin ISO 27001 –standardi pääosin vastaa, kiteytyvät aikaisemmissa luvuissa: osoitusvelvollisuus, riskiperustainen lähestymistapa, sisäänrakennettu tietosuoja ja ilmoitusvelvollisuus. Kyseisissä artikloissa viitataan joko suoraan standardointiin tai muihin vastaaviin toimenpiteisiin. ISO 27001 –standardin ja tietosuoja-asetuksen sopivuuden osoittamiseksi ei olekaan tarkoituksenmukaista käydä läpi muita vaatimuksia, vaan viitata muihin ansiokkaisiin kirjoituksiin kuten Tietosuojavaltuutettu ja tietosuojan informaationlähteet-kappaleessa kuvataan.

3.8 Tietosuojavaltuutettu ja tietosuojan informaatiolähteet

Virallinen neuvova lähde tietosuoja-asioissa on tietosuojavaltuutettu. Tietosuojavaltuutettu on viranomainen, joka antaa neuvoja henkilötietojen käsittelyssä. Tietosuojavaltuutettu onkin julkaissut useita ohjeita tietosuoja-asetukseen valmistautumisesta.

Tietoliikennealalla Finnet-liitto on ansiokkaasti tukenut jäsentensä toimintaa antamalla muun muassa lakineuvontaa asetukseen liittyen. Finnet-liitto myös luo dokumenttipohjia jäsentensä käyttöön erilaisiin tietosuojaan liittyviin sopimus- ynnä muihin asioihin.

Asetukseen liittyvistä lopputöistä muutamia mainitsemisen arvoisia ovat tuoreimmat, 2017 kirjoitetut työt. ”EU:n tietosuoja-asetuksen vaatimusten toteuttaminen pk-yrityksissä” kuvaa, miten pienet ja keskisuuret yritykset voivat varautua tietosuoja-asetuksen vaatimiin muutoksiin (Lönnfors A.). Tietosuoja-asetuksen sisältöön keskitytään ”EU:n TIETOSUOJAUUDISTUS”-lopputyössä. Työssä keskitytään tietosuoja-asetuksen sisältöön ja työssä käydään läpi muun muassa rekisteröidyn oikeudet, rekisterinpitäjän velvollisuudet, siirrot kolmansiin maihin, valvontaviranomaisten toiminta ja muut asetukseen liittyvä artiklat. (Öljymäki J, 14–47.)

4 RATKAISUNA ISO 27001 –STANDARDI

4.1 ISO/IEC organisaatio

ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) muodostavat maailmanlaajuisen standardointiin erikoistuneen järjestelmän, jossa kansalliset jäsenjärjestöt osallistuvat kansainvälisten standardien laadintaan. Järjestössä käsitellään tekniikan eri aloja teknisissä komiteoissa. Organisaatiot yhdistyivät vuonna 1987. (ISO.org, All about ISO.)

ISO ja IEC tekevät yhteistyötä molempia kiinnostavilla aihealueilla. Tietotekniikan alalla järjestöt ovat perustaneet yhteisen teknisen komitean ISO/IEC JTC 1, jonka sääntöjen mukaan kansainväliset standardit laaditaan. Sääntöjen mukaan vähintään 75 % kansallisista jäsenjärjestöistä on hyväksyttävä ehdotus, jotta siitä tulee kansainvälinen standardi. (ISO.org, All about ISO.)

Ensimmäinen virallinen tietoturvastandardi julkaistiin 1999 Britanniassa. ISO/IEC omaksui standardin erinimisenä vuonna 2000 ja 2005 uudistettu standardi nimettiin 27000 –standardiperheeksi. Sittemmin standardia on tarkennettu, parannettu ja uudistettu useaan otteeseen, joitakin osia jopa aivan viime aikoina, viimeksi vuonna 2017. (ISO.org, All about ISO.)

4.2 ISO 27000 –standardiperhe

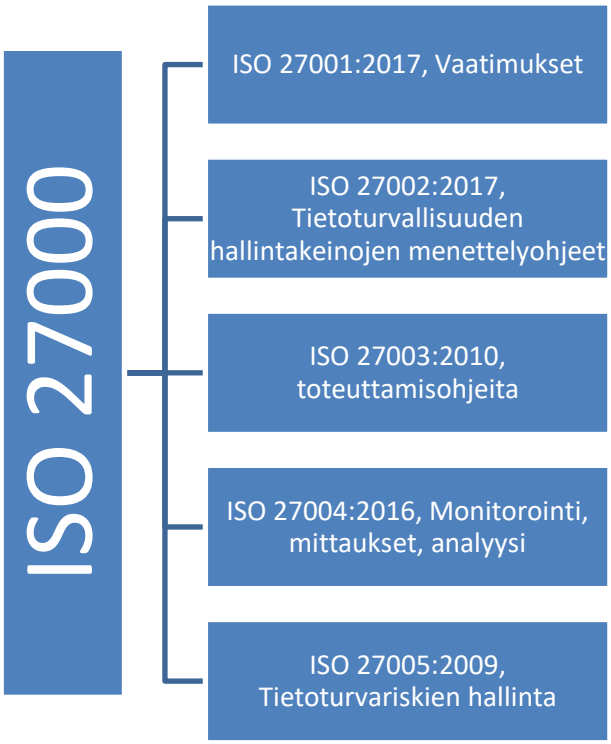
Kansainvälinen tietoturvallisuuden hallintajärjestelmä, koostuu itse ISO 27001 –standardista, sekä useista kyseistä standardia tukevista standardiperheeseen liittyvistä ohjeista. ISO 27000 –standardiperhe käsittelee tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevia vaatimuksia. Vaatimusten tarkoituksena on suojata tiedon luottamuksellisuutta, eheyttä ja saatavuutta riskienhallintaprosessin avulla. (ISO 27001:2017, 5.)

Organisaation strategisena päätöksenä hallintajärjestelmän luomiseen ja toteuttamiseen vaikuttavat tarpeet ja tavoitteet, turvallisuusvaatimukset, käytettävät prosessit sekä organisaation koko ja rakenne. Kaikkien näiden organisaatioon liittyvien tekijöiden odotetaan muuttuvan ajan kuluessa, siksi tietoturvallisuuden hallintajärjestelmän tulisi olla osa organisaation prosesseja ja yleisiä johtamis- ja hallintarakenteita jo suunnitteluvaiheessa. (ISO 27001:2017, 5.)

4.3 Standardiperheen rakenne ja osat

ISO 27000 –standardiperhe määrittelee vaatimukset hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista varten. Osa vaatimuksista on velvoittavia viittauksista, jotka yrityksen on toteutettava, mikäli se aikoo ilmoittaa noudattavansa standardia. (ISO 27001:2017, 5.)

Usein teksteissä ja puhuttaessa mainitaan juuri ISO 27001 –standardi, mutta käytäntö on osoittanut, että alla mainitut standardiperheen osat ovat erittäin tarvittuja standardia toteutettaessa, niiden avatessa ja selittäessä ISO 27001 –standardissa lyhyesti mainitut asiat laajemmin. Kuviossa 2. ISO 27000 –standardiperheen osat.



KUVIO 2. ISO 27000 –standardiperhe (mukaillen ISO 27001–27005 –standardeja)

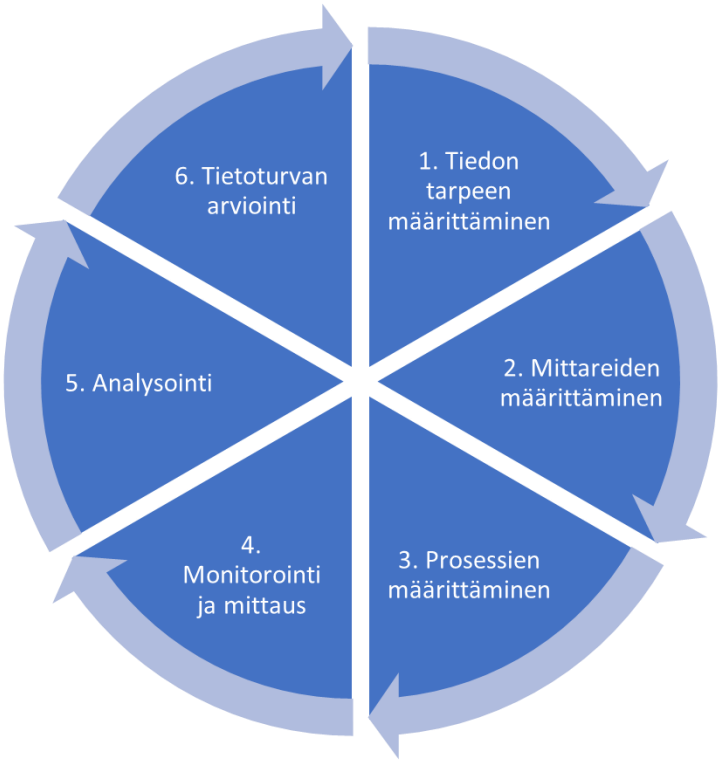
ISO 27001 sisältää standardin vaatimukset, koko ISO/IEC 27000 –perheen yleiskatsauksen ja esittelyn, käytettyjen termien määritelmät ja luokitukset ja yleisiä vaatimuksia. Samalla osa määrittelee yleiset vaatimukset tietoturvallisuuden hallintajärjestelmän luomiselle, toteuttamiselle, käyttämisellä, valvonnalle, katselmoinnille, ylläpidolle ja parantamiselle. (ISO 27001:2017, 5.) Velvoittavien vaatimusten lisäksi standardin liitteessä A määritellään 114 hallintakeinoa, jotka yrityksen on käytävä läpi ja ilmoitettava jokaisen kohdalla noudattaako se kyseistä hallintakeinoa vai ei. Jos yritys ilmoittaa, että kyseinen hallintakeino ei ole käytössä, on hallintakeinon kohdalla perusteltava, miksi näin ei ole. Käytännössä, mikäli toteuttaja haluaa toteuttaa tietoturvan hyvin, ovat lähes kaikki vapaaehtoiset standardit toteutettava.

ISO 27002 –standardi sisältää tietoturvallisuuden hallintaa koskevat menettelyohjeet. Standardi avaa edeltävässä standardissa esitetyt vaatimukset ja antaa vihjeitä ja parhaita käytäntöjä toteutukseen. Standardin mukaan: ”Tietoturvallisuus saavutetaan toteuttamalla soveltuva hallintakeinojen järjestelmä, joka koostuu politiikoista, prosesseista, menettelyistä, organisaatiorakenteista sekä ohjelmisto- ja laitteistotoiminnoista.” (ISO 27002:2017, 5.)

Osassa 27003 kuvataan tietoturvallisuuden hallintajärjestelmän toteuttamissuunnitelman laatiminen. Toteuttamisohjeet kattavat suunnitelmat alkaen projektin käynnistämisessä yrityksessä päätyen tietoturvallisuuden mittaamiseen, kun standardin muut vaatimukset on täytetty. Standardissa esitetään suosituksia ja selityksiä, eikä se sisällä mitään vaatimuksia, vaan tarkoitus on käyttää standardia yhdessä standardin muiden osien kanssa (ISO 27003:2010, 5.)

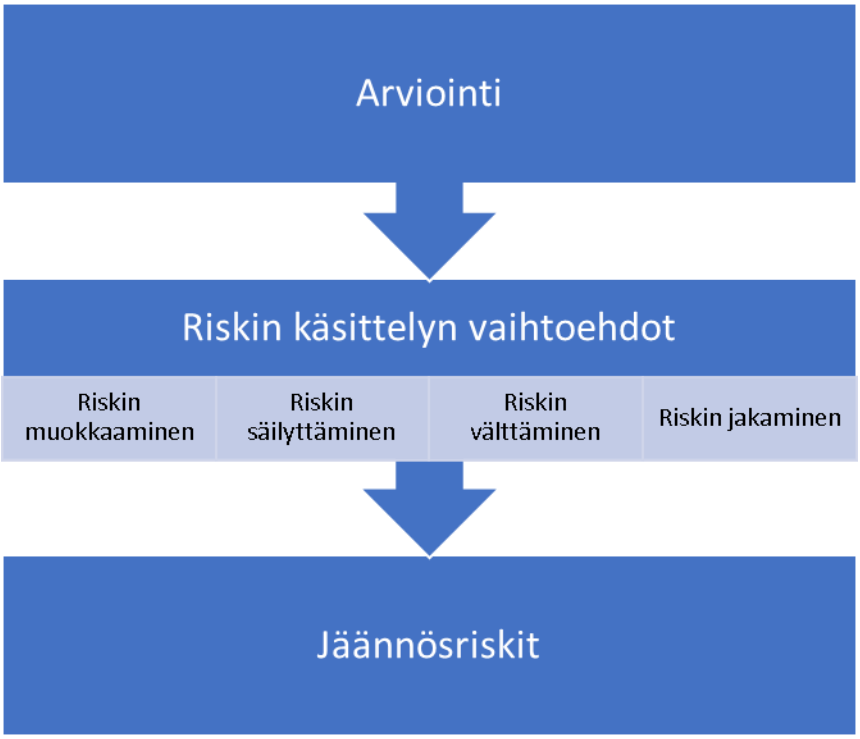
Osassa 27004, mittaaminen kuvataan menetelmät tietoturvallisuuden monitorointiin, mittaamiseen, analysointiin ja evaluointiin. Toimintojen parantaminen on pakollinen ISO 27001 vaatimus ja mittaustulokset tukevat jatkuvaa parantamista hallinnollisissa ja operatiivisissa asioissa tuomalla päätöksentekoon päätöksiä tukevia faktoja. Kuten muitakin standardin osia, tätä tulee soveltaa yrityksen ja organisaation tarpeiden mukaan. (ISO 27004:2016, 5.)

Kuviossa 3. esitetään mittaamisen ja jatkuvan parantamisen prosessi. Prosessin mukaan monitoroinnin ja mittaamisen tulee kytkeytyä takaisin suunnitteluprosessiin, jotta mittaamalla havaitut tapahtumat saadaan joko korjattua, tai niiden ollessa positiivisia, vahvistettua.



KUVIO 3. Monitorointi, analysointi ja arviointiprosessi (mukaillen ISO 27004:2016, Yleistä)

ISO 27005 –standardi kuvaa tietoturvariskien hallintaprosessin. Standardin osa sisältää riskien arvioinnin, käsittelyn, hyväksynnän, riskeistä viestimisen, riskien tarkkailun ja katselmoinnin kuvauksen. Riskien käsittelyn yleisprosessi on esitetty kuviossa 4. Standardin mukaan: ”Kukin organisaatio määrittelee itse riskienhallintaan liittyvät toimintamallinsa, joihin vaikuttavat esimerkiksi tietoturvallisuuden hallintajärjestelmän laajuus, riskienhallinnan toimintaympäristö ja organisaation toimiala.” (ISO 27005:2009, 5.)



KUVIO 4. Riskien käsittelytoiminto (mukaillen ISO 27005:2009, Riskien käsittelyn yleiskuvaus)

Kuviossa 4. esitetään riskien käsittelyprosessi. Prosessin mukaan riskiä voidaan muokata, välttää, jakaa tai jopa säilyttää, sen ollessa riittävän pieni suhteessa muiden vaihtoehtojen aiheuttamiin kustannuksiin.

5 STANDARDIN TOTEUTTAMINEN

5.1 Toteuttamisprojekti

Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeet nojaavat vahvasti suunnittele-toteuta-arvioi-toimi periaatteeseen (ISO 27003:2010, 64). Seuraavissa kappaleissa puhutaan toteuttamisprojektista, mutta kun toimitaan standardin mukaisesti, tulee muistaa, että kyseessä ei ole yksittäinen projekti, vaan toimintatapa, joka organisaation tulee omaksua organisaation päivittäisen toiminnan osaksi.

Päivittäinen toiminta koskettaa jokaista organisaation työntekijää monessa eri muodossa. Esimerkiksi tietosuojaa koskevat ohjeet voivat vaikuttaa henkilötietoja käsitteleviin työntekijöihin muun muassa paperisten tulostusten käsittelyohjeiden muodossa tai sähköisten henkilötietoarkistojen salaamisen muodossa. Salasanavaatimukset taas koskettavat jokaista tietokonetta käyttävää päivittäin, kun laitteisiin on kirjauduttava useita kertoja päivässä.

Toteuttaminen sitä vastoin voidaan tehdä projektimuodossa ja sitä varten usein muodostetaan erillinen projektiorganisaatio, johon nimetään toteuttavat henkilöt ja johtoryhmä ohjaamaan ja valvomaan projektin edistymistä. Toteuttaminen voidaan pilkkoa suunnittele-toteuta-arvioi-toimi periaatteen mukaisesti projektiksi, joka alkaa suunnittelulla.

5.2 Suunnittele

Suunnitteluvaiheessa johdon tulee antaa hyväksyntä projektille, luoda sille edellytykset ja antaa tarvittavat taloudelliset-, materiaali- ja henkilöresurssit projektin käyttöön. Johto määrittelee myös projektin kattavuuden ja rajat. (ISO 27003:2010, 66.) Johto saattaa määritellä kattavuuden koskemaan esimerkiksi pelkästään kotimaan toimintoja tai vain osaa organisaatiosta.

Suunnitteluvaiheessa määritellään myös yrityksen tietoturvavaatimukset ja suojattavat kohteet, sekä tehdään tietoturvariskien analysointi. Edellä mainittujen vaiheiden perus-

teella voidaan laatia toteutussuunnitelma. (ISO 27003:2010, 64.) Kun toteutussuunnitelma on valmis, voidaan suunnitelman perusteella myös arvioida koko projektin kustannukset.

5.3 Toteuta

Projektin toteuttamiseen kuuluu suunnitteluvaiheessa luodun suunnitelman toteuttaminen ja noudattaminen, projekti pyritään toteuttamaan suunnitelmien mukaisesti. Toteuttaminen tarkoittaa prosessien ja ohjeiden kirjoittamista, riskiprosessin suunnittelua ja toteuttamista ja erilaisten hallintakeinojen toteuttamista riskien perusteella (ISO 27001:2017, 18). Kun suunnitelma on toteutettu, suunnitellut toimintamallit muodostuvat päivittäisiksi toiminnoiksi yrityksen toiminnoissa.

Toteuttaminen suunnittele-toteuta-arvioi-toimi-prosessissa tarkoittaa myös päivittäistä operatiivista toimintaa, jossa päivittäin toimitaan standardin mukaisten ohjeiden ja prosessien mukaisesti. Henkilökunnan tulee siis toimia tietoturvallisuuden hallintajärjestelmän ohjeiden mukaisesti ja muun muassa riskienhallinnasta, sisäisitä auditoinneista ja johdon katselmoinneista pitäisi tulla normaalia arkipäivän toimintaa.

5.4 Arvioi

Suorituskyvyn arviointi on oleellinen osa standardin onnistunutta toteutusta. Standardin mukaisesti ” Organisaation on arvioitava tietoturvan tasoa ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta” (ISO 27001:2017, 20).

Organisaation on määritettävä, mitä toimintoja se haluaa seurata ja millä kriteereillä toimintoja mitataan (ISO 27001:2017, 20). Seurannalla ja mittauksilla varmistetaan standardin mukainen toiminta. Seurattavia asioita voivat olla esimerkiksi tietoturvaan liittyvien tapahtumien määrä, yrityksen laitteiden ohjelmistoversioiden ajantasaisuus, havaittujen huijaussähköpostien määrä tai ulosmenevän tietoliikenteen yllättävät määrät.

5.5 Toimi

Toimi-vaihe suunnittele-toteuta-arvioi-toimi periaatteessa viittaa standardin jatkuvan parantamisen vaatimukseen. Vaatimuksen mukaisesti, kun arviointivaiheessa havaitaan poikkeama suunnitelmiin tai mittausten perusteella havaitaan parannettavaa, yrityksen tulee toimia ja korjata tilanne reagoimalla ja tilanteesta riippuen, joko hallita ja korjata poikkeama, tai käsiteltävä sen seuraukset. (ISO 27001:2017, 22.) Vaatimus tarkoittaa, että havaittuihin, suunnitelmista poikkeaviin tapahtumiin tulee reagoida korjaavin toimenpitein.

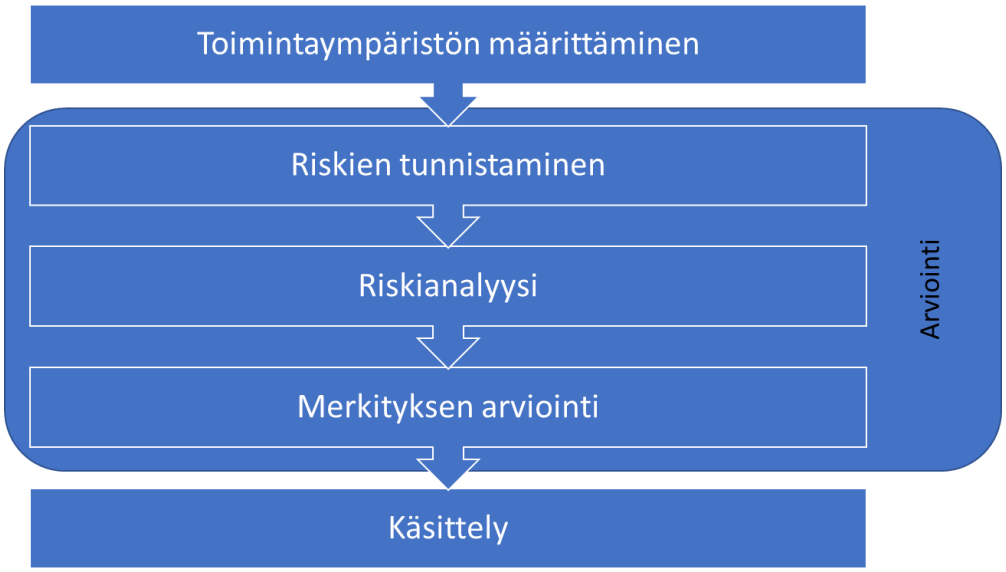
Standardi vaatii, että ”Organisaation on parannettava jatkuvasti tietoturvallisuuden hallintajärjestelmän soveltuvuutta, riittävyyttä ja vaikuttavuutta” (ISO 27001:2017, 20). Tietoturvallisuuden tulee siis olla osa yrityksen jatkuvaa toimintaa ja parantaa jatkuvasti sen vaikuttavuutta. Jatkuvasta parantamisesta tuleekin takaisinkytkentä suunnitteluvaiheeseen, koska havaittuihin poikkeamiin tulee suunnitella toimenpiteet, se tulee toteuttaa ja arvioida ja jälleen toimia, mikäli poikkeamia edelleen havaitaan. Näin standardista muodostuu jatkuva prosessi yksittäisen toteutusprojektin sijaan.

6 VELVOITTAVAT VAATIMUKSET

6.1 Riskien hallinta

Kuten tietosuoja-asetus, myös ISO 27001 –standardi asettaa vaatimuksia erityisesti riskien hallinnalle ja erityisesti riskien ja mahdollisuuksien käsittelyyn (ISO 27001:2017, 8). Kyseisen aiheen tarkempaan käsittelyyn onkin osoitettu kokonaan oma osansa standardiperheessä, ISO 27005.

Kuviossa 5. esitetään riskienhallinnan periaate ISO 27005:n mukaisesti. Koko prosessi alkaa toimintaympäristön määrittämisestä, joka käytännössä tarkoittaa yrityksen omaisuuden, sekä fyysisen omaisuuden; koneiden, laitteiden, tavaroiden, että henkisen omaisuuden; prosessien, toimintojen, organisaatio, listaamista.



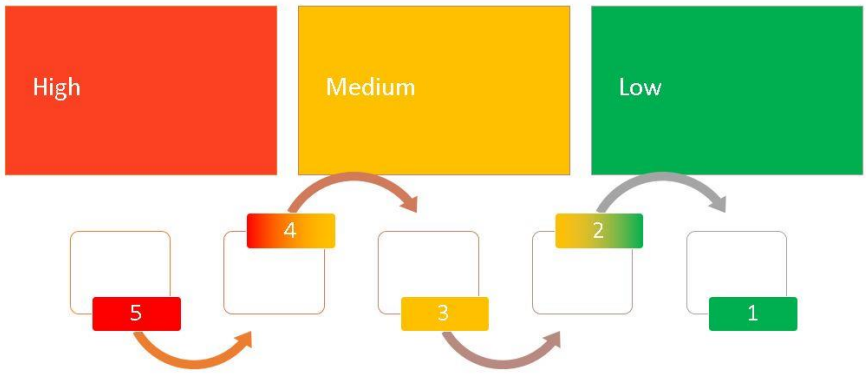
KUVIO 5. Riskienhallinnan periaate (Mukaillen ISO 27005:2009, 20)

Kun omaisuus on selvillä, voidaan tunnistaa siihen kohdistuvia riskejä. Voidaan havaita esimerkiksi etätyö- tai julkisilta paikoilta käytettävien mobiililaitteiden uhat.

Kun riskit on tunnistettu, voidaan analysoida ja arvioida riskit ja käsitellä ne halutulla tavalla ja puuttua riskin aiheuttajaan tai seurauksiin, poistamalla, vähentämällä tai siirtä-

mällä riski tai sen aiheuttaja. Aikaisemmin mainittuun etätyö- tai julkisilta paikoilta käytettävien mobiililaitteiden uhkiin voidaan vastata esimerkiksi laitteiden sisällön salaamisella ja näytönsuojien käyttöönottamisella.

Kuviossa 6. esitetään kaksi vaihtoehtoista riskien kategorisointi-mallia. Riski voidaan arvioida esimerkiksi kolmiportaisella mallilla High-Medium-Low tai viisiportaisella mallilla, asteikolla 5–1.



KUVIO 6. Riskikategoria-esimerkki (mukaillen ISO 27005:2009, 41)

Standardi itsessään ei anna määräystä käytettävästä mallista, vaan antaa yrityksen itse valita käyttämänsä mallin. Puuttumalla riskeihin pyritään pääsemään korkeasta (High tai 5–4) kategoriasta alemmille riskitasoille.

Riskeille pyritään löytämään esimerkiksi todennäköisyyttä kuvaava numeerinen arvo, sekä riskin toteutumisen vaikuttavuutta kuvaava numeerinen arvo. Riskin vakavuus saadaan kertomalla todennäköisyys ja vakavuus keskenään, eli Riski = (todennäköisyys x vakavuus). Vakavuuden selvittyä kaikille havaituille riskeille, ne voidaan asetta tärkeysjärjestykseen ja määritellä hallintakeinot em. vakavuuden perusteella.

6.2 Velvoittavien vaatimusten ja tietosuoja-asetuksen vastaavuus

Standardissa esitetyt vaatimukset ovat yleisluonteisia ja tarkoitus on, että ne soveltuvat kaikille organisaatioille niiden tyypistä, koosta tai luonteesta riippumatta. Velvoittavat vaatimukset ovat nimensä mukaisesti velvoittavia, jos organisaatio ilmoittaa noudattavansa standardin vaatimuksia, ei mitään niistä voida jättää toteutuksen ulkopuolelle.

LUETTELO 1. Velvoittavat vaatimuskategoriat

Organisaation toimintaympäristö
Johtajuus
Suunnittelu
Tukitoiminnot
Toiminta
Suorituskyvyn arviointi
Parantaminen

.

Organisaation toimintaympäristö-vaatimuksen mukaan organisaation on määritettävä asiat, jotka ovat olennaisia organisaation tarkoituksen kannalta ja jotka vaikuttavat sen kykyyn saavuttaa tietoturvallisuuden kannalta halutut tulokset. Tällaisia asioita ovat muun muassa sidosryhmät ja niiden tarpeet, standardin toteutuksen rajaukset ja hallintajärjestelmän luominen. (ISO 27001:2017, 6.)

Johtajuuden vaatimus tarkoittaa, että yrityksen johto osoittaa sitoutumisensa tietoturvallisuuteen varmistamalla, että standardin vaatimukset toteutetaan muun muassa antamalla tarvittavat resurssit projektin käyttöön. Ylimmän johdon on myös laadittava politiikka, joka sisältää sitoutumisen tietoturvallisuuteen. (ISO 27001:2017, 7.)

Tietoturvallisuutta on suunniteltava esimerkiksi toteuttamalla tietoturvariskien arviointiprosessi, jonka perusteella voidaan riskeihin kohdistaa erilaisia toimenpiteitä ja muuttaa siten riskin suuruutta. Prosessiin kuuluu riskien arviointi, käsittely, tavoitteet ja toimenpiteet niiden saavuttamiseksi. (ISO 27001:2017, 8.)

Organisaation on varmistettava tietoturvaprosessin onnistuminen esimerkiksi tarpeellisen koulutuksen, tietoisuuden lisäämisellä ja viestinnän avulla. Tietoturvallisuuteen liittyvä tieto on myös dokumentoitava ja dokumentit päivitettävä. (ISO 27001:2017, 10.)

Toiminta-vaatimus tarkoittaa, että organisaationa on suunniteltava ja toteutettava prosessit, joita tarvitaan tietoturvavaatimusten täyttämiseen. Organisaation on säilytettävä riittävästi dokumentoitua tietoa voidakseen luottaa siihen, että prosessit on toteutettu suunnitelmien mukaisesti, sekä hallittava suunniteltuja muutoksia ja arvioitava tahattomien muutosten seurauksia sekä pyrittävä lieventämään mahdollisia haittavaikutuksia tarpeen mukaan. (ISO 27001:2017, 12.)

Tietoturvan tasoa ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta on arvioitava. Arviointia varten on määritettävä mittarit, sekä koska, miten ja kuka mittauksen tekee ja miten ne analysoidaan. Arviointia on myös suoritettava sisäisten katselmointien ja auditointien avulla. (ISO 27001:2017, 12.)

Parantamisen vaatimus tarkoittaa, että poikkeaman havaittuaan organisaatio ryhtyy toimiin, joiden avulla poikkeama joko korjataan, tai poikkeaman seuraukset käsitellään. Reagoinnin lisäksi on arvioitava millä toimenpiteillä poikkeama ei toistu. (ISO 27001:2017, 14.)

Velvoittavat vaatimukset asettavat perusvaatimukset organisaation tietoturvalliselle toiminnalle ja sen kehittämiselle. Koska tietosuojaa ei voi olla ilman tietoturvaa, nämä vaatimukset edistävät suoraan tietosuoja-asetuksen vaatimuksia organisatorisille toimenpiteille.

6.3 Dokumentointi osana velvoittavia vaatimuksia

Ohjeiden, prosessien ja tapahtumien dokumentointi on oleellinen osa onnistunutta standardointi- ja sertifiointiprosessia. Jotta yritys voi osoittaa toimivansa standardin mukaisesti, sen on dokumentoitava ohjeistuksensa ja suunnitelmansa, sekä pöytäkirja- ja muut merkinnät, jotka osoittavat, mitä on tapahtunut. Yrityksen on siis tuotettava todistusaineistoa auditointitarpeisiin.

Standardi määrittelee, että organisaation on määritettävä ulkoiset ja sisäiset asiat, jotka ovat olennaisia organisaation tarkoituksen kannalta. Dokumenttiin tulee kirjata sidosryhmät ja sidosryhmien asettamat tietoturvallisuutta koskevat vaatimukset sekä rajoitukset ja rajapinnat ja riippuvuudet. (ISO 27001:2017, 6.)

Ylimmän johdon on osoitettava sitoutumisensa tietoturvallisuuden hallintajärjestelmään muun muassa laatimalla yritykselle tietoturvapolitiikka, joka soveltuu organisaatioon ja sisältää yrityksen tietoturvatavoitteet (ISO 27001:2017, 7).

Standardin asettaa vaatimukset tietoturvariskien arvioinnille ja käsittelylle. Vaatimuksen mukaisesti yrityksen on määritettävä ja toteutettava tietoturvariskien arviointi- ja käsittelyprosessit, joiden mukaan yrityksessä tunnistetaan, arvioidaan ja hyväksytään riskit ja niiden käsittely. Tietoturvariksien käsittelystä yrityksen on laadittava soveltuvuuslausunto, joka sisältää valitut hallintakeinot ja perustelut niiden käyttämiselle tai käyttämättä jättämiselle. (ISO 27001:2017, 8–9.)

Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu määritellään ISO 27001 –standardissa. Tietoturvatavoitteissa on määritettävä mitä tehdään, mitä resursseja tarvitaan, vastuut, aikataulu tekemiselle ja arviointikriteerit, jonka perusteella lopputulosta arvioidaan (ISO 27001:2017, 9).

Organisaation on määritettävä pätevyysvaatimukset, varmistettava että henkilöt ovat pätevyysvaatimusten mukaisesti koulutettu tai heillä on vaadittava harjoittelut tai kokemus ja täydennettävä tarvittaessa henkilöiden pätevyyttä eri keinoin. Tästä on säilytettävä asianmukaista dokumentoitua tietoa näyttönä. (ISO 27001:2017, 10.)

Organisaation on suunniteltava ja toteutettava prosessit, joita tarvitaan tietoturvavaatimusten täyttämiseen. Toiminnasta on säilytettävä riittävästi dokumentoitua tietoa, jotta voidaan luottaa siihen, että prosessit on toteutettu suunnitelmien mukaisesti. (ISO 27001:2017, 12.)

Tietoturvariskien arvioinnin ja käsittelyn tulokset on dokumentoitava (ISO 27001:2017, 12). Myös arviointi ja käsittely on toteutettava standardin mukaisesti (ISO 27001:2017, 8–9).

Organisaation on arvioitava tietoturvan tasoa ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta (ISO 27001:2017, 12). Vaatimuksen mukaisesti organisaation on määrättävä, mitä seurataan ja millä seuranta-, mittaus-, analysointi- tai arviointimenetelmillä

seuranta toteutetaan, sekä kuka seurannan tekee, milloin ja miten tulokset arvioidaan. Kaikesta tästä on säilytettävä dokumentoitua tietoa todisteena.

Jatkuvan parantamisen saavuttamiseksi organisaation on tehtävä sisäisiä auditointeja, jotta voidaan määrittää, onko hallintajärjestelmä standardin ja vaatimusten mukainen ja onko sitä toteutettu ja ylläpidetty vaikuttavasti. Auditoinnit on suunniteltava, toteutettava ja dokumentoitavat, jotta auditointiohjelmasta ja tuloksista jää todisteita. (ISO 27001:2017, 13.)

Ylimmän johdon on katselmoitava organisaation tietoturvallisuuden hallintajärjestelmä suunnitelluin aikavälein varmistaakseen, että se on edelleen soveltuva, asianmukainen ja vaikuttava (ISO 27001:2017, 13). Katselmoinnin tarkoitus on varmistaa, että organisaatio toimii standardin osoittamalla tavalla ja että tietoturvatavoitteet täyttyvät ja organisaation parantaa toimintaansa jatkuvasti.

Poikkeamat ja korjaavat toimenpiteet on mahdollisuuksien mukaan havaittava ja niihin on reagoitava tilanteesta riippuen. Organisaation on säilytettävä dokumentoitua tietoa todisteena poikkeamien luonteesta sekä niiden johdosta tehdyistä toimenpiteistä, sekä tehtyjen korjaavien toimenpiteiden tuloksista (ISO 27001:2017, 14).

7 VAPAAEHTOISET VAATIMUKSET

7.1 Vapaaehtoiset hallintatavoitteet ja keinot

ISO 27001 –standardi sisältää myös 114 vapaaehtoista hallintakeinoa. Standardin liitteessä A luetellut hallintatavoitteet ja -keinot on otettu suoraan standardin ISO/IEC 27002:2013 kohdista 5–18. Ne ovat yhteneviä kyseisten kohtien kanssa. (ISO 27001, Liite A.)

Hallintakeinot on jaoteltu neljääntoista eri kategoriaan, niiden sisältämien hallintakeinojen mukaisesti ja eri kategoriat sisältävät yhteensä 114 erillistä vaatimusta/hallintakeinoa tietoturvan parantamiseen. Hallintakeinot ovat sertifiointia hakevalle vapaaehtoisia, mutta jokaisen keinon kohdalla hakijan on ilmoitettava, noudattaako kyseistä keinoa ja mikäli ei noudata, se on perusteltava.

LUETTELO 2. Hallinta-kategoriat

A.5 Tietoturvapolitiikat
A.6 Tietoturvallisuuden organisointi
A.7 Henkilöstöturvallisuus
A.8 Suojattavan omaisuuden hallinta
A.9 Pääsynhallinta
A.10 Salaus
A.11 Fyysinen turvallisuus ja ympäristön turvallisuus
A.12 Käyttöturvallisuus
A.13 Viestintäturvallisuus
A.14 Järjestelmien hankkiminen, kehittäminen ja ylläpito
A.15 Suhteet toimittajiin
A.16 Tietoturvahäiriöiden hallinta
A.17 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia
A.18 Vaatimustenmukaisuus

Hallintakeinojen menetelmistä moni toimii suoraan tietosuojan toteuttajana ja epäsuorasti tietoturvan toteuttamisen kannalta.

7.2 Vapaaehtoisten vaatimusten ja hallintakeinojen ja tietosuoja-asetuksen vastaavuus

Kaikki ISO 27000 –standardiperheen vapaaehtoiset vaatimukset ovat sovellettavissa tietosuoja-asetuksen vaatimuksiin teknisistä ja organisatorisista toimenpiteistä tietosuojan edistämiseen vaatimusten toteuttamiseen. Tämän voi perustella samoin kuin velvoittavien vaatimusten kohdalla: Jokainen vapaaehtoinen hallintakeino edistää tietoturvaa ja sitä kautta myös tietosuojaa.

Empiirisesti asiaa tutkimalla ja eri asiantuntijoita kuulemalla voi päätyä myös erilaisiin päätelmiin. Osa hallintakeinoista on sovellettavissa suoraan tietosuojavaatimuksiin ja osa vaikutta epäsuorasti. Seuraavassa käydään läpi standardin hallintakeinojen kategoriat tietosuoja-asetuksen näkökulmasta.

Hallintakategoriassa A.5 Tietoturvapolitiikat, kategorian molemmat hallintakeinot vastaavat tietosuoja-asetuksen organisaation tietoturvalliselle toiminnalle asettamiin vaatimuksiin. Tietoturvapolitiikoilla määritellään yleisellä tasolla organisaation tavoitteet tietoturvalle ja tietosuojalle (ISO 27001, 25). Tietoturvapolitiikat antavat suuntaviivat yrityksen henkilökunnalle siitä, miten ja millä tasolla yrityksen johto haluaa henkilökunnan suhtautuvat tietoturvavaatimuksiin. Ilman suuntaviivoja ei yrityksessä ole yhteistä toimintatapaa ja suhtautuminen tietoturvaan on jokaisen henkilökohtaisen päätöksen mukaista.

Hallintakategoriassa A.6 Tietoturvallisuuden organisointi sisältää seitsemän hallintakeinoa, joista, kriteerien tiukkuudesta riippuen jopa neljä hallintakeinoa vastaa tietosuoja-asetuksen vaatimuksiin. Hallintakeinot sisältävät muun muassa vaatimuksen, että asiankuuluviin viranomaisiin on ylläpidettävä tarkoituksenmukaisia yhteyksiä. Tämä hallintakeino vastaa tietosuoja-asetuksen ilmoitusvelvollisuus-vaatimukseen. (ISO 27001, 25.) Ilmoitusvelvollisuuden lisäksi vaatimukseen vastaaminen lisää yrityksen kykyä reagoida tietoturvatapahtumaan. Tilanteen ollessa päällä, on hyödyllistä, että tarvittavat yhteystiedot on valmiiksi selvitetty, eikä niitä tarvitse ryhtyä etsimään silloin kuin pitäisi toimia.

A.7 Henkilöstöturvallisuus-hallintakategoria asettaa hallintakeinoja työsopimuksen solmimiseen, päättymiseen ja taustan tarkistukseen. Näistä hallintakeinoista esimerkiksi työntekijöiden nuhteettomuus varmasti edistää myös tietosuojaa, ehkäisten yrityksen työntekijöiden mahdollisia henkilötietojen väärinkäyttötapauksia. (ISO 27001, 26.) Valitettavasti nykyisin (jos koskaan on ollutkaan) nuhteettomuus ei ole itsestäänselvyys ja se näkyy yrityksen toiminnassa muun muassa vaikeutena rekrytoida pätevää henkilöstöä.

A.8 Suojattavan omaisuuden hallintakategoria määrittelee hallintakeinoksi muun muassa tiedon luokittelun lakisääteisten vaatimusten mukaisesti, sekä arvon, kriittisyyden ja luvattoman paljastumisen aiheuttamien vaikutusten perusteella. Tiedon luokittelu vastaa tietosuoja-asetuksen artikla 9:n erityisiä henkilötietoryhmiä koskevaa käsittelyä. Artiklan mukaan tietyt henkilötietoihin liittyvien luokittelujen käsittely on sallittu vain artiklassa mainituista erityisistä syistä. (ISO 27001, 26.) Tiedon luokittelu koskee myös muuta yrityksen tietoa, kuin henkilötietoja. Yritys voi luokitella esimerkiksi sopimustiedot, hinnoitteluperiaatteet ja tuotteen suunnitelmat salaisiksi tiedoiksi, joita se ei halua vuodettavan kilpailijoille.

Hallintakategoriassa A.9 Pääsynhallinta, esitetään hallintakeinoja käyttäjäoikeuksien myöntämiselle, poistamiselle, rajaamiselle ja muille pääsynhallintaan liittyville toimenpiteille (ISO 27001, 28). Pääsynhallinta vastaa lähes jokaisen hallintakeinon kohdalta tietosuoja-asetuksen vaatimuksiin, sillä pääsynhallinnalla rajataan oikeudettomien henkilöiden pääsy muun muassa henkilötietoihin. Pääsynhallintakeinoja ovat muun muassa henkilön käyttäjätunnuksen ja salasanan vaatiminen kirjautumisen yhteydessä. Käyttäjätunnuksen avulla käyttäjä tunnistetaan ja salasanan avulla varmistetaan käyttäjän henkilöllisyys. Tunnistuksen ja varmistuksen jälkeen voidaan käyttäjä päästää järjestelmään ja antaa hänelle kuuluvat käyttöoikeudet käyttöön. Lisää tietoturvaa (ja sitä myöten tietosuojaa) voidaan saada esimerkiksi ottamalla kaksivaiheinen tunnistus käyttöön. Tällöin käyttäjältä vaaditaan vielä käyttäjätunnuksen ja salasanan lisäksi esimerkiksi puhelin, johon vastaanotettua pin koodia vaaditaan vielä käyttäjätunnuksen ja salasana lisäksi kirjautumisen yhteydessä.

Tiedon salaus-hallintakeino määritellään kategoriassa A.10 Salaus (ISO 27001, 31). Salaus voi tulla kyseeseen tietosuoja-asetuksen näkökulmasta, kun henkilötietoja suojataan

salaamalla. Salaus voidaan toteuttaa esimerkiksi tietokannan henkilötietoja sisältävien kenttien salauksella, tiedon salauksella, kun sitä lähetetään sähköpostilla tai muulla tiedonsiirtovälineellä tai salausvaatimuksilla, kun tietoa tallennetaan eri tallennusmedioille.

Fyysisellä suojauksella suojataan toimistoja, tiloja ja laitteita ja tällä hallintakeinolla voidaan suojata henkilötietoja vuotamiselta esimerkiksi fyysisten tulostusten muodossa. A.11 Fyysinen turvallisuus ja ympäristön turvallisuuskategoria määrittelee hallintakeinot kyseisiin uhkiin (ISO 27001, 32). Fyysisen turvallisuuden suojaamiskeinoja ovat muun muassa sähköinen kulunvalvonta ja tilojen videovalvonta.

Tietojärjestelmiä suojataan A.12 Käyttöturvallisuus-hallintakeinojen avulla. Kategoria asettaa vaatimuksia esimerkiksi haittaohjelmilta suojautumiselle ja varmuuskopioinnille (ISO 27001, 34). Näillä keinoilla voidaan suojata henkilötietoja esimerkiksi katoamiselta ja vuotamiselta haittaohjelmien vaikutuksesta. Tietojen kadottua esimerkiksi laiterikon takia voidaan tiedot palauttaa varmuuskopioilta tai haittaohjelman vaikutuksia voidaan estää virustorjuntaohjelmien avulla.

Tietoverkkojen hallintaa ja esimerkiksi sähköisen viestinnän suojaamista käsitellään kategoriassa A.13 Viestintäturvallisuus (ISO 27001, 36). Tietoverkkoja ja sähköistä viestintää suojaamalla voidaan suojata myös tietosuoja-asetuksen mukaisia henkilötietoja. Sähköisen viestinnän salaus voidaan toteuttaa esimerkiksi kaiken tietoliikenteen automaattisella salaamisella.

A.14 Järjestelmien hankkiminen, kehittäminen ja ylläpito vaatii muun muassa, että testiaineisto kehittämisprojekteissa on valittava huolellisesti ja niitä on suojattava ja hallittava (ISO 27001, 38). Aikaisemmin opinnäytetyössä osoitettiin, että henkilötiedot ovat löydettävissä jopa pseudonymisoidusta datasta (tietosuoja eli henkilötietojen suojaaminen). Tämä asettaa testiaineiston valinnalle ja suojaamiselle erityisiä vaatimuksia henkilötietoja sisältävien aineistojen osalta. Aina silloin tällöin julkisuudessakin kirjoitetaan tapauksista, joissa testidataa on päässyt julkiseen käyttöön ja näin esimerkiksi henkilötietoja on vuotanut yrityksen ulkopuolelle.

A.15 Suhteet toimittajiin määrittää tietoturvavaatimukset, jolla kontrolloidaan muun muassa toimittajan pääsyoikeuksista aiheutuvia riskejä (ISO 27001, 40). Toimittajalla saattaa olla pääsy myös henkilötietoja sisältävään dataan, joten hallintakeino on oleellinen myös tietosuoja-asetuksen kannalta. Vaikka toimittaja itsessään ei aikoisi mitään haitallista, voi toimittajan verkossa oleva pahantahtoinen kolmas osapuoli saada pääsyn suojeltavaan dataan toimittajan pääsyoikeuksien myötä.

Tietosuoja-asetus edellyttää, että tietoturvaloukkauksesta ilmoitetaan valvontaviranomaiselle ja rekisteröidylle itselleen. Hallintakeinot kategoriassa A.16 Tietoturvahäiriöiden hallinta määrittelevät yrityksen sisäiset menettelyohjeet kyseisissä tapahtumissa (ISO 27001, 40). Tietosuoja-asetuksen asettama määräaika ilmoitukselle on hyvin lyhyt, kun otetaan huomioon, että tietoturvatapahtuma on aina poikkeustilanne yrityksessä. Tällöin valmiiksi mietityt toimintaohjeet ja yhteystiedot helpottavat kriisitilanteessa työskentelevää henkilökuntaa.

Kategoria A.17 määrittää Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia. Nämä ohjeistuksen varmistavat, että tietoturvallisuuden haluttu taso säilyy myös epäsuotuisissa tilanteissa. Kriisitilanteessa voisi olla mahdollista, että tilanne loisi vielä pahempia tietosuoja- tai tietoturva ongelmia jo olemassa olevan lisäksi.

Vaatimustenmukaisuus kategoriassa A.18 asettaa yritykselle standardin kautta vaatimuksen lakien, viranomaisten ja sopimusten asettamien vaatimusten noudattamiselle (ISO 27001, 42). Lakien ja sopimusten noudattamien on tietysti useimmille meistä itsestään selvää, mutta standardin avulla myös toimintamallit ja organisaatiota koskevat lait, viranomais- ja sopimusten asettamat vaatimukset tulee suunniteltua organisaation toiminnassa etukäteen.

8 JOHTOPÄÄTÖKSET JA POHDINTA

ISO 27000 –standardiperhe ja ISO 27001 –standardi ovat erinomaisia lähtökohtia tietoturvan ja tietosuojan parantamiseen. Standardi esittää vaatimukset, joita noudattamalla voidaan parantaa yrityksen tietoturvaa ja -suojaa huomattavasti. Kuten jo aikaisemmin tässä opinnäytetyössä on mainittu ISO 27001 –standardi vastaa pääosin tietosuoja-asetuksen vaatimuksiin: osoitusvelvollisuus, riskiperustainen lähestymistapa, sisäänrakennettu tietosuoja ja ilmoitusvelvollisuus. Kyseisissä artikloissa on suoraan viitattu standardointiin tai muihin vastaaviin toimenpiteisiin.

Standardin toteuttaminen ja mahdollinen sertifiointi ovat koko yrityksen organisaation-laajuinen projekti. Käytettävät standardin osat on määritettävä ja suunniteltava ja tähän työhön osallistuu tyypillisesti vain pieni joukko tietohallinnon tietoturvaan keskittyneitä työntekijöitä. Tässä vaiheessa työ on pitkälti dokumentointia ja erilaisten hallintakeinojen käyttöönottoa.

Toteutusvaihe koskeekin sitten kaikkia yrityksen työntekijöitä, kaikkien on otettava ohjeistusten mukaiset toimintatavat käyttöönsä, oli kyse sitten toimistossa, asiakkaalla tai etätyöskentelystä. Ohjeistukset saattavat koskea muun muassa turvallista toimintaa julkisissa tiloissa ja miten avoimiin WLAN-verkkoihin tulee suhtautua, tai miten omissa toimitiloissa, ilman henkilökorttia kulkevaan henkilöön tulisi suhtautua.

Valitettavasti standardi ei anna konkreettisia ohjeita vaatimusten ja hallintakeinojen toteuttamiseen. Voisi sanoa, että on mahdollisimman yleisluontoisesti kirjoitettu, mahdollisesti sen vuoksi, että se soveltuisi mahdollisimman erilaisten yritysten käyttöön. Tämä johtaa väistämättä standardiperheen muiden standardien käyttöönottotarpeeseen.

Standardit ISO 27002, 27003, 27004 ja 27005 tuovatkin huomattavasti apua vaatimusten toteuttamiseen, antamalla laajemman kuvauksen yksittäisen vaatimuksen toteuttamiseen. Valitettavasti myöskään laajennukset eivät anna tarpeeksi konkreettisia työkaluja standardin toteuttamiseen, vaan jokaisen yrityksen on toteutettava vaatimukset ja hallintakeinot edelleen omista lähtökohdistaan. Tämä antaakin erinomaisen mahdollisuuden konsulteille myydä osaamistaan standardin toteuttamiseen.

Konsultin mukana usein tuleekin iso joukko erilaisia word- ja excel-dokumenttipohjia, tai muita työkaluja, jotka ovat suureksi avuksi erityisesti sertifiointiprosessin katselmointivaiheeseen, jossa sertifioija tarkistaa ja yrittää löytää puutteita yrityksen dokumentoinnista, prosesseista ja muista toteutuksista standardiin liittyen.

Konsulttien tarjoaman avun lisäksi eri hallintakeinojen toteutuksessa tarvitaan alihankkijoiden ja toimittajien työpanosta. Vain harva yritys hallitsee itse kaikkea toimintaansa liittyvää infrastruktuuria. Yrityksellä saattaa olla toimitiloja useassa eri kaupungissa tai jopa eri maissa ja näitä ylläpitävät eri kiinteistöjen hallintaan erikoistuneet yritykset. Jopa tietoliikenneyhteydet tulevat mahdollisesti usealta eri toimittajalta.

Opinnäytetyöstä saa pikaisen yleiskuvan standardista, sen osista ja niiden käyttötarkoituksista. Työ on hyödynnettävissä esimerkiksi valittaessa hyödynnettäviä osia ISO 27000 –standardiperheestä.

LÄHTEET

CNN. 2016. U.S. investigators find proof of cyberattack on Ukraine power grid. Päivitetty 4.1.2016. Luettu 28.1.2018. CNN Politics.

Culnane, Rubinstein, Teague. 2017. Health data in an open world. Julkaistu 15.12.2017. The University of Melbourne.

De Montjoye, Radaelli, Singh, & Pentland. 2015. Unique in the shopping mall: On the reidentifiability of credit card metadata. Julkaistu 30.1.2015. Science-tiedelehti.

Digitaalisten sisämarkkinoiden strategia Euroopalle, COM (2015) 0192. 2017. Politiikka. Luettu 17.12.2017. Euroopan Parlamentti.

EU info. 2017. Infografiikka –Tietosuoja-asetus. Luettu 15.12.2017. Euroopan Parlamentti.

Euroopan unionin virallinen lehti. L 119, 4.5.2016. Euroopan Parlamentti.

Henkilötietolaki 22.4.1999/523

Internet ja digitaaliteknologia. 2015. Euroopan komissio –Lehdistötiedote. 6.5.2015. Euroopan komissio

ISO.org. 2017. International Organization for Standardization. Luettu 16.9.2017. International Organization for Standardization.

ISO 27001:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. SUOMEN STANDARDISOIMISLIITTO SFS.

ISO 27002:2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. SUOMEN STANDARDISOIMISLIITTO SFS.

ISO 27003:2010. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita. SUOMEN STANDARDISOIMISLIITTO SFS.

ISO 27004:2016. Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation. SUOMEN STANDARDISOIMISLIITTO SFS.

ISO 27005:2009. Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. SUOMEN STANDARDISOIMISLIITTO SFS.

Kyberturvallisuuden uudistus Euroopassa. 2017. http://www.consilium.europa.eu/fi/policies/cyber-security/. Luettu 17.12.2017. Euroopan Parlamentti.

LIBE. 2015. Pöytäkirja, kokous 17.12.2015. Euroopan Parlamentti.

Limnéll, Jarno, 20.1.2017. Luentoesitys.

Lönnfors, Andreas. 2017. EU:n tietosuoja-asetuksen vaatimusten toteuttaminen pk-yrityksissä. 18.4.29017. Metropolia Ammattikorkeakoulu.

Unionin tila 2017. 2017. Euroopan Komissio –Lehdistötiedote. 19.9.2017. Euroopan Komissio.

Yleinen tietosuoja-asetus. 2016. 2016/679, 27.4.2016. Euroopan parlamentti ja neuvosto.

Öljymäki, Jari. 2017. EU:n TIETOSUOJAUUDISTUS. Vaasan Ammattikorkeakoulu.