Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

KAROLINA YLI-HIETANEN

ISO/IEC 27001 -standardin sertifiointiin valmistautuminen IT-alan yrityksessä

TUOTANTOTALOUDEN TUTKINTO-OHJELMA
2021

Tekijä(t)
Yli-Hietanen, Karolina

Julkaisun laji
Opinnäytetyö, AMK

Päivämäärä
huhtikuu 2021

Sivumäärä
58+27

Julkaisun kieli
suomi

Julkaisun nimi
ISO/IEC -27001 standardin sertifiointiin valmistautuminen IT-alan yrityksessä

Tutkinto-ohjelma
Tuotantotalous- ja tekniikka

Tämä opinnäytetyö tehtiin suomalaiselle IT-alan yritykselle, jonka tarkoituksena on sertifioida ISO/IEC 27001 -standardi. Opinnäytetyön tavoitteena oli laatia dokumentti, jossa verrataan ISO/IEC 27001 -standardin vaatimuksia organisaation nykytilanteeseen ja kartoitetaan tietoturvariskejä.

Tutkimuksessa kuvattiin ensin sertifiointi ja sertifiointiprosessi, seuraavana ISO/IEC 27001 -standardi sekä riskejä, riskien hallintaprosessi ja hallintamenetelmät. Nykytilanteen selvittämiseksi tutkimusmenetelmänä käytettiin puolistrukturoitua haastattelua ja haastateltavina olivat yrityksen tietoturvasta vastaavat henkilöt. Tietoturvariskejä kartoitettiin pääosin lähdekirjallisuuden avulla.

Tuloksena saatiin kattava Excel-taulukko organisaation nykytilasta, puutteista ja suositeltavista toimenpiteistä, jolla organisaatio täyttää ISO/IEC 27001 -standardin vaatimukset. Excel-taulukon avulla organisaatio saa käsityksen puutteista ja siitä, mitä on vielä tehtävä sertifikaatin saamiseksi. Lisäksi työn tuloksena saavutettiin riskiarviointitaulukko, jossa on kuvattuna organisaation tietoturvariskit. Riskiarviointitaulukko havainnollistaa, mihin tekijöihin on kiinnitettävä huomiota tietoturvan parantamiseksi.

Laadittu Excel-taulukko on hyvä työkalu ISO/IEC 27001 -standardin mukaiseen tietoturvallisuuden hallintajärjestelmän kehittämiseen, ja auttaa yritystä sertifikaatin hankinnassa. Riskiarviointitaulukko on hyvä apuväline tietoturvan parantamiseen ja kehittämiseen.

Asiasanat
ISO/IEC 27001, sertifiointi, tietoturva, riskienhallinta, riskianalyysi

Author(s) Yli-Hietanen, Karolina	Type of Publication Bachelor's thesis	Date April 2021
	Number of pages 58+27	Language of publication: Finnish

Title of publication
ISO/IEC 27001 standard's certification preparation in IT company

Degree program
Industrial Management and Technology

This bachelor's thesis was made to finish IT company, whose purpose is to certify ISO/IEC 27001 standard. The aim of this bachelor's thesis was to make documentary in which ISO/IEC 27001 standard's requirements compared from the present organization's situation and survey information security risks.

In this research the first descriptions were to certification and certification process, next was ISO/IEC 27001 standard and risks, risks management process and management methods. To clear the present situation semi-structured interview was used as a method of investigation and the ones who were interviewed was the leading personals of information security. Information security risks were surveyed with help of the sources of reference mainly.

Comprehensive Excel-chart was got as a result from the present state of organization's situation, deprivations, and measures of recommended in which organization will fill ISO/IEC 27001 standard's requirements. With help of Excel-chart's organization gets notion of deprivations and what needs to be done before certification. In addition, a risk assessment chart was got as a result in which the organization's information security risks were described. The risk assessment chart demonstrates to what factors have to get notion to make the information security better.

Live Excel-chart is a good tool to develop ISO/IEC 27001 standard's ISMS and helps organization to get a certification. A risk assessment chart is a good aid to improve and develop the information security.

Key words
ISO/IEC 27001, certification, information security, risk management, risk analysis

SISÄLLYS

1 JOHDANTO

COVID19 -pandemia on korostanut tietoturvaa. Etätyöhön on siirrytty laajasti ja hyvin nopeasti eri puolilla maailmaa, ja etätyöskentelyvälineitä otettiin hallitsemattomasti käyttöön (Traficom 2021, 6). Verkkohyökkäysten määrät ja niiden voimakkuudet ovat kasvussa, ja tehottomasta tietoturvasta johtuvat taloudelliset vahingot ja maineriskit voivat olla organisaatiolle kohtalokkaita (Baker 2017). Suomen merkittävin tietoturvaloukkaustapaus on koskettanut yli kymmeniä tuhansia, kun viime vuonna Psykoterapiakeskus Vastaamon henkilö- ja potilastietoja on levinnyt julkisuuteen ja heitä on uhattu erilaisilla kiristysviesteillä (Traficom 2021, 13).

Tiedot ovat yksi arvokkaimmista omaisuuksista, joita yritys omistaa (Krypsys 2021). Turvallisuushäiriöt vähentävät kuluttajien arvostusta ja horjuttavat toimintavarmuutta (Traficom 2019, 26). Yritykset ovat enemmän riippuvaisia tietojärjestelmistä ja pilvipalveluista kuin koskaan aiemmin. The Influence of Standards on the Nordic Economies -tutkimuksen (2017) mukaan suomalaisyrityksistä 91 % ajattelee, että standardit lisäävät asiakkaiden luottamusta ja 74 % arvioivat, että standardi tehostaa markkinoita ja edistää yrityksiä hallitsemaan kaupan tekniset esteet (Menon Economics 2018, 4). Suomessa ISO/IEC 27001 -standardin sertifioinnit ovat kasvaneet vuodesta 2016 vuoteen 2017 mennessä 33 % ja maailmanlaajuisesti sertifioinnit ovat nousseet 19 % (Traficom 2019, 26).

Kohdeyrityksellä on useita asiakasyrityksiä. He työskentelevät monien sidosryhmien kanssa ja tiedon turvaaminen on heille tärkeää. Kohdeyrityksen tarkoituksena on hankkia tulevaisuudessa ISO/IEC 27001 -standardi. Se on luultavasti myös asiakkaiden vaatimus tulevina vuosina. Kohdeyrityksen on osoitettava, että he noudattavat tietoturvaa koskevia vaatimuksia. Organisaatiolle on olennaista saada selville, millainen tilanne yrityksessä on verratessa standardin vaatimuksiin. Tässä opinnäytetyössä keskitytään sertifiointiprosessiin, ISO/IEC 27001 -standardiin sekä riskien arviointiprosessiin ja hallintamenetelmiin. Aineisto kasataan puolistrukturoidun haastattelun avulla. Haastateltavat ovat yrityksen tietoturvasta vastaavia henkilöitä.

1.1 Tutkimuksen tarkoitus, tavoitteet ja tutkimuskysymykset

Tutkimuksessa on tarkoitus verrata ISO/IEC 27001 -vaatimuksia organisaation käytäntöihin, tapoihin ja laadittuihin dokumentteihin sekä saada selville kohdeyrityksen lähtötilanne, puutteet ja toimenpiteet standardin saamiseksi. Lisäksi tarkoituksena on kartoittaa, mitä riskejä kohdeyrityksellä liittyy tietoturvaan.

Tavoitteena on laatia kohdeyritykselle selkeä dokumentti, jossa kuvataan millä keinoilla se voi saavuttaa ISO/IEC 27001 -standardin mukaisen tietoturvallisuuden hallintajärjestelmän. Dokumentin tavoitteena on helpottaa organisaatiota sertifikaatin hankkimisessa ja kertoa, mitä kaikkea organisaation on vielä tehtävä sertifikaatin hankkimiseksi. Tavoitteena on kuvata myös riskiarviointitaulukko, ja sen tehtävänä on edistää organisaation tietoturvaa.

Kohdeyrityksellä ei ole tietoturvallisuuden hallintajärjestelmää. He eivät ole aikaisemmin tutustuneet ISO/IEC 27001 -standardiin tai muihin tietoturvallisuuden hallintajärjestelmän malleihin. Vuonna 2018 voimaan astunut EU:n yleinen tietosuoja-asetus 2016/679 (GDPR, General Data Protection Regulation) on lisännyt organisaation vastuita ja velvollisuuksia, ja se on kuluttanut useiden organisaation resursseja (Traficom 2019, 28). Organisaatiolla on ollut hyvin vähän aikaa tietoturvallisuuden hallintajärjestelmän kehittämiseen.

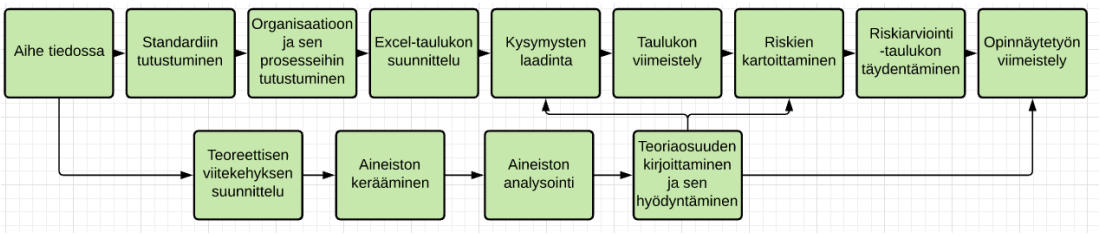
Tutkimuskysymykseksi saadaan:

- Millaisia toimenpiteitä tarvitaan standardin sertifioimiseksi?

Tutkimuksen alakategoriat ovat:

- Millainen nykyinen tilanne on yrityksessä?
- Mitä puutteita on?
- Millaisia toimenpiteitä vaaditaan puutteiden korjaamiseksi?
- Mitä tietoturvaan liittyviä riskejä yrityksellä on?

Prosessikaavio (kuva 1) auttaa havaitsemaan, miten opinnäytetyön teoreettinen viitekehitys ja toiminnallinen osa yhdistyvät. Se edistää opinnäytetyön eri aihealueiden oivaltamista ja kuvastaa, miten ne liittyvät toisiinsa.

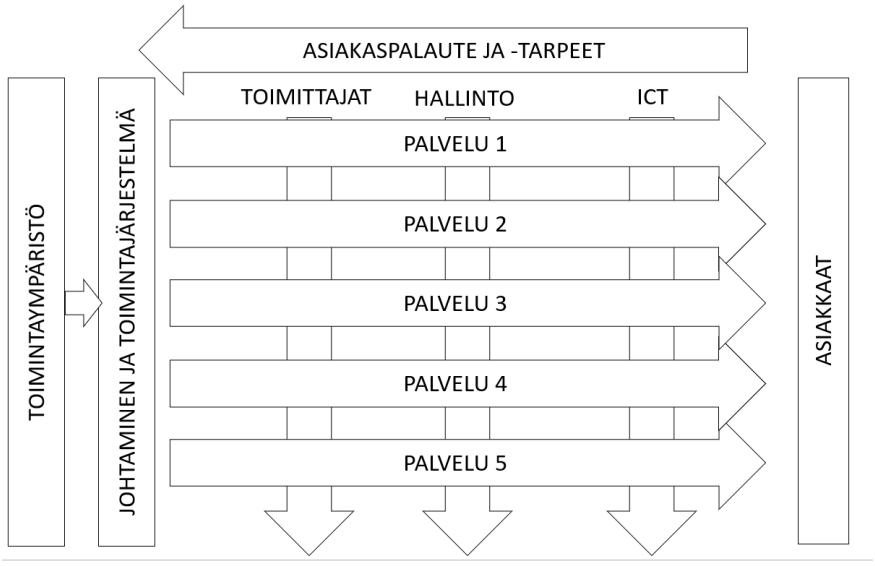


Kuva 1. Opinnäytetyön prosessikaavio

1.2 Toimeksiantaja

Toimeksiantaja on Suomessa toimiva pk-yritys, joka on keskittynyt asiantuntijapalvelujen ja niitä tukevien järjestelmien tuottamiseen. Päätoimialat ovat IT-konsultointi ja IT-palvelut. Yrityksen liikevaihto on useita miljoonia euroja. Yhtiö on toiminut useita vuosia. (Kohdeyritys 2021.)

Kohdeyrityksessä on viisi pääpalvelua (kuva 2) ja ne ovat kuvattuna palvelu 1, palvelu 2 jne. Palveluja ei kuvata tarkemmin, sillä ne pidetään salassa tutkimuksen eettisyyden takia ja toimeksiantajan tunnistamisen välttämiseksi.



Kuva 2. Kohdeyrityksen prosessikartta

1.3 Rajaukset

Tutkimuksessa keskitytään vain ISO/IEC 27001 -standardiin ja sen tietoturvallisuuden hallintajärjestelmään. Tutkimuksessa ei käsitellä muita tietoturvastandardeja tai tietoturvallisuuden hallintajärjestelmän malleja ja niihin liittyviä kriteeristöjä. Taulukossa ei oteta kantaa siitä, kuka on vastuussa kohtien suorittamisesta ja sen toteuttaminen on jätetty pois tästä tutkimuksesta. Tutkimuksesta rajataan pois myös ISO/IEC 27001 -standardin laajennusosa ISO/IEC 27701:2019. Se keskittyy tietosuojan hallintaan ja ottaa huomioon Euroopan tietosuoja-asetuksen (GDPR).

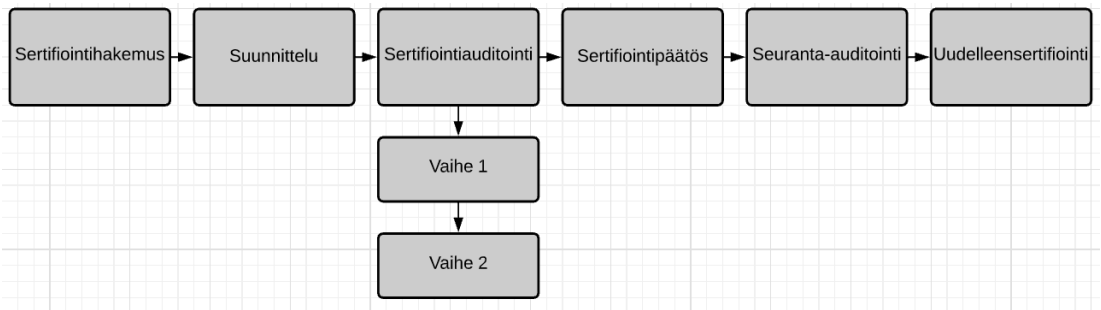
2 SERTIFIOINTI

Sertifiointi tarkoittaa vaatimusten arviointia ja niiden täyttymisen tarkastelua. Vaatimukset ovat kuvattuna standardeissa. Standardi on kirjallinen asiakirja tai julkaisu, joka täsmentää tuotteiden ja niiden valmistamisen tai testaamisen sekä järjestelmien ja palvelujen ominaisuuksia, vaatimuksia tai suosituksia. Sertifioitavia kohteita ovat henkilö, tuote, prosessit tai johtamisjärjestelmä. Sertifiointilaitos myöntää sertifiointitodistuksen arvioinnin perusteella. Sertifiointijakso on yleisesti voimassa kolme vuotta. Sertifiointia voidaan hakea uudelleen jakson päättymisen jälkeen. (ISO/IEC 17021:fi 2015, 53; FINAS www-sivut 2021; Suomen standardisoimisliitto SFS ry 2021.)

Sertifiointeja suorittavat puolueettomat sertifiointilaitokset, jotka ovat anoneet akkreditointia FINAS:sta. Akkreditointi todistaa arvioijan pätevyyden ja riippumattomuuden. FINAS on Suomen akkreditointielin, joka on Turvallisuus- ja kemikaalivirastossa operoiva yksikkö. Suomessa on yli 200 akkreditoitua eri alojen tarkastuslaitosta, sertifiointiorganisaatiota, laboratoriota ja muuta vaatimukset täyttävää arviointilaitosta. (Hänninen 2019, 16–17.)

2.1 Sertifiointiprosessi

ISO/IEC 27001 -standardin ja muiden standardien sertifiointiprosessi alkaa hakemuksella sertifiointia toteuttavalle taholle. Prosessissa on kuusi vaihetta, jossa sertifiointiauditointi toteutetaan kahdessa osassa. (ISO/IEC 17021:fi 2015, 28 & 53.) Vaiheet (kuva 3) ovat kuvattuna seuraavana.



Kuva 3. Sertifiointiprosessi (ISO/IEC 17021:fi 2015, 53)

2.1.1 Sertifiointihakemus

Hakijaorganisaation on toimitettava sertifioivalle taholle olennaiset tiedot, jossa kuvataan hakijaorganisaation toimintaa. Hakemuksessa on määritettävä hakijaorganisaation yleiset tiedot, kuten organisaation nimi, sijaintitiedot, prosessit ja toiminnot sekä kuvattava sertifioinnin tavoiteltu laajuus ja standardi tai muut vaatimukset, jota organisaatio hakee. (ISO/IEC 17021:fi 2015, 22.)

2.1.2 Suunnittelu

Auditointien tavoitteet, soveltamisala ja kriteerit on suunniteltava. Auditointeja varten on kehitettävä prosessi, johon kuuluvat aloitus- ja lopetuskokous. Aloituskokouksen tavoitteena on kertoa, miten auditointitoiminnot suoritetaan ja lopetuskokouksissa on kuvattava auditoinnin johtopäätökset ja sertifiointiin liittyvät suositukset. (ISO/IEC 17021:fi 2015, 25 & 30–32.) Lecklin (2006, 314) täsmentää, että suunnitteluvaiheessa sovitaan myös auditointien aikataulut.

2.1.3 Sertifiointiauditointi, vaihe 1

Ensimmäisessä vaiheessa tarkastellaan asiakkaan johtamisjärjestelmän dokumentoitua tietoa, arvioidaan olosuhteita ja kuinka hyvin organisaatio täyttää ja oivaltaa standardin vaatimukset sekä keskustellaan henkilöstön kanssa, jotta voidaan varmistaa organisaation valmius toiseen vaiheeseen. Ensimmäisessä vaiheessa on hankittava toimintoja, johtamisjärjestelmää ja sen soveltamisalaa koskevat tiedot, kuten toimipaikat, hallintatasot, prosessit ja laitteistot. On arvioitava organisaation valmiutta vaiheeseen kaksi, kuten toteutetaanko sisäisiä auditointeja sekä sovittava toisen vaiheen yksityiskohdista ja varattava riittävästi resursseja siihen. (ISO/IEC 17021:fi 2015, 28–29.)

Ensimmäisessä vaiheessa tehdyt johtopäätökset on välitettävä asiakkaalle ja kerrottava, miten valmiita he ovat toiseen sertifiointiauditointiin. Heille on kuvattava ongelmakohdat ja annettava riittävästi aikaa niiden korjaamiseen ennen toista vaihetta. (ISO/IEC 17021:fi 2015, 29.)

2.1.4 Sertifiointiauditointi, vaihe 2

Toinen sertifiointiauditointi tehdään asiakkaan toimitiloissa ja tavoitteena on arvioida, kuinka asiakkaan johtamisjärjestelmä on toteutettu ja tarkastella sen vaikuttavuutta. Toisessa vaiheessa on auditoitava hallintajärjestelmästandardin vaatimusten noudattaminen sekä mitata, raportoida ja analysoitava toimintaa suhteessa suoritustavoitteisiin. Lisäksi on auditoitava johtamisjärjestelmän kykenevyyttä täyttää vaatimukset sekä miten prosessien toiminnan ohjaaminen, sisäinen auditointi, johdon tarkastelu ja johdon velvollisuus asiakkaan toimintaperiaatteista toteutuvat. Toisessa vaiheessa havaitut ongelmat ja poikkeamat on ratkaistava ennen sertifiointipäätöstä. (ISO/IEC 17021:fi 2015, 29 & 53.) Lecklin (2006, 314) tarkentaa, että tarvittaessa suoritetaan uusintaarviointi tai vahvistetaan kirjallisen aineiston avulla, että vaadittavat toimenpiteet on suoritettu.

2.1.5 Sertifiointipäätös

Sertifiointipäätöksessä hakijaorganisaatiolle myönnetään sertifiointi ja sertifiointiasiakirjat. Jotta sertifiointi voidaan myöntää, tiedoissa on oltava auditointiraportti, lausunnot poikkeamista ja korjaavista toimenpiteistä, tietojen vahvistaminen, tavoitteiden saavuttamisen varmistaminen ja sertifioinnin myöntämiseen liittyvät ehdot tai havainnot. (ISO/IEC 17021:fi 2015, 34–35 &53.) Lecklin (2006, 314) kuvailee, että sertifiointi edellyttää hallintajärjestelmän ylläpitämistä standardin mukaan.

2.1.6 Seuranta-auditointi

Seuranta-auditoinnit ovat organisaatiossa suoritettavia auditointeja, jossa tarkastellaan poikkeamista johtuneita toimenpiteitä, valituksia, johtamisjärjestelmän vaikuttavuutta, jatkuvaa parantamista ja muutoksia. Seuranta-auditointeja on pidettävä vähintään kerran vuodessa ja ensimmäinen seuranta-auditointi on suoritettava 12 kuukauden sisällä sertifiointipäätöksestä. Niiden ei täydy olla kokonaisia järjestelmäauditointeja, sillä sertifioivan tahon on luotettava, että sertifioitu yritys täyttää vaatimukset uudelleen sertifiointiauditointien välissä. Niissä voidaan tarkastella ainoastaan jotain tiettyä toimintoa. (ISO/IEC 17021:fi 2015, 36 &53.) Leckin (2006, 314) kertoo, että sertifikaatti

voidaan perua tietyksi ajaksi tai hylätä kokonaan, jos järjestelmän taso ei täytä vaatimuksia.

2.1.7 Uudelleensertifiointi

Uudelleensertifioinnin tavoitteena on tarkistaa, että johtamisjärjestelmä on vaatimustenmukainen ja se on toteutettava organisaatiossa paikan päällä ennen sertifioinnin vanhentumista. Uudelleensertifiointiauditointi on suunniteltava tarkasti ja siinä on tarkasteltava aiempia seuranta-auditointiraportteja, johtamisjärjestelmän vaikuttavuutta ja johtamisjärjestelmän sitoutumista jatkuvaan kehittämiseen. Poikkeamille on kuvattava aikarajat ennen kuin sertifiointi vanhenee. Jos uudelleensertifiointi on suoritettu onnistuneesti ja poikkeamat ovat korjattu, voidaan myöntää uudelleen sertifiointi. (ISO/IEC 17021:fi 2015, 36–37 &53.)

3 ISO/IEC 27001 -STANDARDI

ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) muodostama organisaatio on laatinut tietoturvallisuutta koskevan ISO/IEC 27001 -standardin. Kansainvälinen ISO/IEC 27001 -standardi kuvailee ehdot, jotka liittyvät tietoturvallisuuden hallintajärjestelmän jatkuvaan kehittämiseen, ylläpitämiseen, toteuttamiseen ja luomiseen. (ISO/IEC 27001:fi 2017, 3–5.)

Standardin käyttöönottaminen ja sen toteuttaminen on strateginen päätös, mitä voidaan hyödyntää erilaisissa organisaatioissa, vaikka ne olisivat luonteeltaan, tyypiltään ja suuruudeltaan toisistaan poikkeavia. Organisaation toimiessa eri sidosryhmien kanssa, standardi turvaa tiedon saatavuuden, eheyden ja luottamuksellisuuden. (ISO/IEC 27001:fi 2017, 5.) Hakala, Vainio ja Vuorinen (2006, 4) kertovat, että:

- Saatavuudella eli käytettävyydellä tarkoitetaan, että tieto on saatavissa ja sellaisessa muodossa, että tietoa voidaan hyödyntää jatkuvasti.
- Eheys tarkoittaa, ettei tietoa vähene tai lisäänny ja tieto säilyy alkuperäisenä koko sen eliniän ajan.
- Luottamuksellisuus tarkoittaa, että tieto on käytettävissä vain niillä tahoilla ja henkilöillä, jotka sitä tarvitsevat.

3.1 Standardin hyödyt

Suurin etu ISO 27001 -standardissa on se, että se auttaa organisaatiota hallitsemaan tietoturvaa ja vähentämään tietomurtoriskejä. ISO 27001 -sertifikaatti on vaikuttava keino osoittaa, että organisaatio noudattaa kansainvälisiä asetuksia ja lakeja, kuten GDPR ja NIS-direktiivi. ISO 27001 -standardi suojaa organisaation elektronisata dataa, ja myös tietokoneiden, mobiililaitteiden ja muiden elektronisten laitteiden dataa sekä organisaation asiakastietoja ja muita luottamuksellisia tietoja. (IT Governance 2021, 2.)

ISO/IEC 27001 -standardin sertifioinnista on muitakin etuja, kuten

- Uusien asiakkaiden saaminen ja nykyasiakkaiden säilyminen
- Edistää laajentumista globaaleille markkinoille

- Todistaa, että organisaatio ottaa vakavasti kyberturvallisuuden
- Helpottaa arkaluonteisen tiedon suojaamista
- Organisaatio saa tarkemman käsityksen toiminnastaan
- Organisaation toiminta helpottuu, kun prosessit ja vastuut ovat kuvattuna
- Kommunikointi helpottuu toisten yritysten kanssa, kun käytössä on yhteiset termit ja selkeät käytännöt
- Vahvistaa tietoturvaosaamista ja kehittää tietoturvallisuuden ymmärtämistä, erityisesti sen tärkeydestä
- Osoittaa luotettavuutta ja sitoutuneisuutta tietoturvaan
- Täyttää lukuisat sopimukselliset, kaupalliset ja lain velvollisuudet
- Antaa kilpailuetua ja edistää organisaation mainetta
- Edistää riskienhallintaa ja vältetyt riskit vähentävät kustannuksia. (Baker 2017; Klaus 2017; Krypsys 2021; Pro Pilvipalvelut 2021.)

3.2 Tietoturvallisuuden hallintajärjestelmä (ISMS)

Tietoturvallisuuden hallintajärjestelmä (Information Security Management System) tarkoittaa toisiinsa vaikuttavia tai liittyviä osia, jotka pienentävät organisaatiossa tietoturvariskiä ja suojaavat digitaalisesti, fyysistesti ja aineettomasti talletettavaa tietoa. Tietoturvallisuuden hallintajärjestelmä on systemaattinen lähestymistapa organisaation tietoturvallisuuden laatimiseen, noudattamiseen, ylläpitoon, valvontaan ja kehittämiseen. Se sisältää ohjeita, menettelytapoja, toimintaperiaatteita, organisaatiorakenteita ja toimintoja sekä henkilöstön vastuualueita. Järjestelmän avulla organisaatio saa tilaisuuden täyttää tietoturvaa koskevat vaatimukset, kehittää hallintaympäristöä, täydennettyä puutteet ja ennen kaikkea varmuuden siitä, että tieto on suojattu riittävästi uhkilta. (ISO/IEC 27000:fi 2020, 10–23.)

Tietoturvallisuuden hallintajärjestelmä noudattaa viitekehystä, joka rakentuu usein seuraavista asiakirjoista ja dokumenteista:

- Soveltamisala, kuten tietyt liiketoimintayksiköt, toimipisteet tai osastot.
- Tietoturvapolitiikka ja -strategia, johon kuuluvat tietoturvallisuuden prosessit, tarvittavat resurssit, vastuut, organisointi ja suunnittelu.
- Tietoturvakäytännöt ja -periaatteet sekä kehittämissuunnitelma.

- Tietoturvallisuuden ohjeistus ja tarvittava lisäohjeistus.
- Henkilöstön pätevyyden ylläpitäminen.
- Tietoturvariskien arviointiin, hallintaan ja menettelemiseen liittyvät tavat sekä tarvittavat mittarit tietoturvariskien seuraamiseen, ohjaamiseen ja analysoimiseen. Johdolle on raportoitava tietoturvasta ja kertoa tuloksista.
- Poikkeamat ja korjaavat toimenpiteet, jota varten tarvitaan jatkuvuus- ja toimintasuunnitelmat.
- Sisäiset tarkastukset ja auditointisuunnitelmat. (Valtionvarainministeriö 2017, 40.)

3.3 Standardin vaatimukset

Standardissa kuvatut tietoturvallisuuden hallintajärjestelmän vaatimukset ovat

- organisaation toimintaympäristö
- johtajuus
- suunnittelu
- tukitoiminnot
- toiminta
- suorituskyvyn arviointi
- parantaminen (ISO/IEC 27001:fi 2017, 2).

Kaikki ISO/IEC 27001 -standardissa esitetyt vaatimukset ovat pakollisia ja niitä on noudatettava (ISO/IEC 27001:fi 2017, 5). Vaatimukset eivät ole kuvattuna tärkeys- tai toteuttamisjärjestyksessä, vaan järjestys noudattaa standardin rakennetta. Niitä kuvataan tarkemmin seuraavana.

3.3.1 Organisaation toimintaympäristö

Organisaation on kuvattava sisäiset ja ulkoiset toimintaympäristöt, jotka liittyvät organisaation kykenevyyteen päästä tietoturvallisuuden hallintajärjestelmän toivottuihin tuloksiin ja jotka ovat tärkeitä organisaation merkityksen osalta (ISO/IEC 27001:fi 2017, 6). Ulkoisia asioita ovat esimerkiksi teknologiset, taloudelliset, kilpailulliset ja yhteiskunnalliset aihealueet. Niitä organisaatio ei voi itse ohjata. Organisaatio pystyy

ohjaamaan sisäisiä asioita ja niitä ovat esimerkiksi tiedonkulku, organisaatiorakenne ja prosessit. Analysoinnin tarkoituksena on tarkastella tietoturvallisuuden hallintajärjestelmän muuttumista sisäisten ja ulkoisten tekijöiden mukaisesti, kartoittaa riskejä ja mahdollisuuksia sekä ymmärtää omaa toimintaympäristöä. (ISO/IEC 27003:fi 2017, 7–8.)

Organisaation pitää määrittää sidosryhmät ja niiden tietoturvavaatimukset, jotka ovat tärkeitä tietoturvallisuuden hallintajärjestelmän kannalta (ISO/IEC 27001:fi 2017, 6). Sidosryhmällä tarkoitetaan organisaatiota tai henkilöä, jolla on merkitystä päätöksen tekemiseen tai joka on sen kohteena. Sisäisillä ja ulkoisilla sidosryhmillä voi olla tietoturvaan koskevia vaatimuksia, tarpeita ja odotuksia. Sisäisiä sidosryhmiä ovat esimerkiksi päätöksentekijät ja tietohallinnon tukitoiminto. Ulkoisia sidosryhmiä ovat muun muassa toimittajat ja sääntelyviranomaiset. Sidosryhmiä on tarkasteltava säännöllisesti, sillä ne muuttuvat ajan kuluessa. Organisaatio on talletettava vain ne tiedot, joita se pitää hallintajärjestelmän vaikuttavuuden kannalta oleellisena. (ISO/IEC 27003:fi 2017, 9–10.)

Organisaation on luotava tietoturvallisuuden hallintajärjestelmä ja määritettävä sen soveltamisala sekä järjestelmää koskevat soveltamiset ja rajaukset. Soveltamisalan määrittämiseen vaikuttavat sisäiset ja ulkoiset tekijät, liiketoiminnot ja niiden tukitoiminnot sekä sidosryhmät. Tietoturvallisuuden hallintajärjestelmää on päivitettävä ja kehitettävä standardin vaatimusten mukaan. (ISO/IEC 27001:fi 2017, 6; ISO/IEC 27003:fi 2017, 10–12.)

3.3.2 Johtajuus

Ylimmällä johdolla tarkoitetaan ryhmää tai henkilöä, joka opastaa korkeimmalla tasolla tietoturvallisuuden hallintajärjestelmää ja joka on kokonaan vastuussa järjestelmästä. He voivat antaa tarvittaessa valtuuksia muille. Ylin johto viestittää sitoutumisestaan ja johtajuudestaan tietotuvallisuuden hallintajärjestelmään käyttäen useita keinoja:

- He tarkistavat, että tietoturvatavoitteet ja -vaatimukset laaditaan ja, että ne noudattavat organisaation strategiaa.

- He huolehtivat, että hallintajärjestelmä on osa organisaation prosesseja ja se sopii toimintaympäristöön sekä järjestelmälle on saatavissa välttämättömät resurssit, kuten toimitilat, henkilökunta, taloudelliset varat ja tekninen infrastruktuuri.
- He varmistavat, että järjestelmä aikaansaa toivottavat tulokset tukien prosesseja ja tarkkailevat järjestelmän mittaus- ja auditointiraportteja.
- He välittävät tietoa järjestelmän vaatimuksien noudattamisesta ja hallinnan edellytyksestä sekä ohjaa muita kehittämään järjestelmää edistäen sen paranemista ja antamalla tukea muille motivoidakseen heitä. (ISO/IEC 27001:fi 2017, 7; ISO/IEC 27003:fi 2017, 12–13.)

Ylin johto määrittää ja hyväksyy tietoturvan roolit, valtuudet ja vastuut sekä viestii niistä organisaatiolle (ISO/IEC 27001:fi 2017, 7). Tällä saadaan varmistus siihen, että organisaatiossa toimitaan standardin vaatimusten mukaisesti, sekä ylimmän johdon pitäisi tarkistaa toistuvasti toteutuvatko ne oikein (ISO/IEC 27003:fi 2017, 15).

Tietoturvapolitiikan laatii ylin johto ja se on dokumentoitava. Se on organisaation käytössä ja ulkoisilla sidosryhmillä, jos he tarvitsevat sitä. Tietoturvapolitiikka ohjaa tietoturvaan liittyviä asioita sekä kertoo tietoturvallisuuden tarpeesta ja hallintajärjestelmän strategisesta merkityksestä. Tieturvapolitiikka koostuu tietoturvatavoitteista ja sen on sovittava organisaation liikeideaan sekä siinä vakuutetaan järjestelmän toistuva kehittäminen ja vaatimusten suorittaminen. Se vahvistaa, että ylin johto sitoutuu tietoturvatavoitteisiin ja hallintajärjestelmän jatkuvaan kehittämiseen sekä tukemiseen. (ISO/IEC 27001:fi 2017, 7; ISO/IEC 27003:fi 2017, 14.)

3.3.3 Suunnittelu

Organisaation pitää tunnistaa riskit ja mahdollisuudet sekä rakentaa tietoturvariskien arviointiprosessi, jossa havaitaan, tarkastellaan ja tutkitaan tietoturvariskejä suunnitellessaan tietoturvallisuuden hallintajärjestelmää. Organisaation on suunniteltava tietoturvariskien käsittelyprosessi, jossa havaitaan hallintakeinot ja tarkastellaan niitä ISO/IEC 27001 - standardin keinoihin sekä luodaan soveltuvuuslausunto ja käsittelysuunnitelma tietoturvariskejä varten. Toimintoihin on laadittava tietoturvatavoitteet ja

niiden on sisällettävä useita vaatimuksia, kuten mitattavuus, yhdenvertaisuus tietoturvapolitiikan kanssa ja ylläpidettävyys. (ISO/IEC 27001:fi 2017, 8–9.)

3.3.4 Tukitoiminnot

Tietoturvallisuuden hallintajärjestelmää suunniteltaessa on varattava riittävästi resursseja järjestelmän rakentamiseen, hallitsemiseen, tarkastelemiseen ja jatkuvaan kehittämiseen sekä huolehdittava henkilöstön pätevyydestä. Organisaation pitää kuvata, millainen pätevyys henkilöstöllä kuuluu olla ja varmistaa, että he ovat riittävän päteviä sekä säilyttää tietoa osaamisesta. Välttämätön pätevyys voidaan hankkia käyttäen useita keinoja, kuten hyödyntäen mentorointia, palkkaamalla taidokas henkilö tai kouluttamalla henkilöstöä. (ISO/IEC 27001:fi 2017, 10.)

Henkilöstön on tiedettävä tietoturvapolitiikasta ja siitä, miten he pystyvät vaikuttamaan järjestelmän laatuun ja tiedostaa hyödyt tietoturvallisuuden kehittämisestä sekä vaikutukset, jos tietoturvallisuuden hallintajärjestelmän vaatimuksia ei noudateta. Organisaation on sovittava, millaista ulkoista ja sisäistä viestintää he tarvitsevat, kuten kenen kanssa, mistä ja milloin viestitään. (ISO/IEC 27001:fi 2017, 10.)

Kun organisaatio kirjoittaa tai päivittää uutta tietoa hallintajärjestelmään, tallennetun tiedon on noudatettava oikeaa talletusmuotoa, merkintää ja kuvausta. Henkilöstö tarkistaa ja vahvistaa tiedon oikeellisuuden ja kattavuuden. (ISO/IEC 27001:fi 2017, 11.)

3.3.5 Toiminta

Jotta organisaation toimii tuloksekkaasti, sen pitää määrittää toisiinsa kuuluvia prosesseja ja toimintoja. Toiminnot, jotka käyttävät resursseja, vaativat ohjausta ja hallintaa. Niiden avulla saadaan tuotosta, kun toimintojen panokset ovat liitettynä yhteen toimintojen sarjana. Prosessin tuotos voi vastata jonkin prosessin panosta. Prosessimainen toimintajärjestelmä tarkoittaa, että organisaatio soveltaa prosessijärjestelmää, tunnistaa prosesseja ja niiden vuorovaikutusta sekä johtaa niitä. Organisaation pitää

tallentaa riittävästi dokumentteja, jotta voidaan osoittaa prosessien toteuttaminen tavoitteiden mukaisesti. (ISO/IEC 27001:fi 2017, 12; ISO/IEC 27000:fi 2020, 18.)

Organisaation toimintaan kuuluvat prosessien ja toimintojen määrittelemisen ja ohjaamisen lisäksi tietoturvariskien arvioiminen ja käsitteleminen. Tietoturvariskejä pitää arvioida tietyn väliajoin ja laatia tietoturvariskien käsittelysuunnitelma sekä niiden tuloksista täytyy säilyttää tietoa. (ISO/IEC 27001:fi 2017, 12.)

3.3.6 Suorituskyvyn arviointi

Organisaation pitää määrittää mittarit sekä analysointi- ja seurantamenetelmät, jotka edesauttavat tulosten mittaamisessa sekä tietoturvallisuuden hallintajärjestelmän ja tietoturvatason vaikuttavuuden arvioinnissa. Organisaation pitää tarkentaa, milloin mittaaminen ja seuraaminen tehdään sekä ketkä sen tekevät. Heidän täytyy täsmentää, milloin saadut tulokset analysoidaan ja tarkistetaan sekä ketkä ne suorittavat. (ISO/IEC 27001:fi 2017, 12.)

Organisaatio on tehtävä sisäisiä auditointeja tietyn väliajoin ja niiden avulla saadaan tietoa siitä, onko hallintajärjestelmä standardin ja organisaation hallintajärjestelmää liittyvien vaatimuksien mukainen. Organisaation pitää laatia ja tehdä auditointiohjelma, jossa on kuvattuna raportoiminen, auditointien aikaväli ja käytettävät menetelmät sekä henkilöiden vastuut. Heidän on täsmennettävä auditointikriteerit ja nimettävä auditoijat sekä raportoida tuloksista eteenpäin. Auditoinneista ja niiden tuloksista pitää säilöä dokumentteja. (ISO/IEC 27001:fi 2017, 13.) Auditoinneissa tarkastellaan muun muassa standardin vaatimuksien toteutumista ja tietoturvavaatimusten ja -tavoitteiden edistymistä (ISO/IEC 27003:fi 2017, 41–42).

Ylin johto tarkastelee tietoturvallisuuden hallintajärjestelmää määräajoin tarkistaakseen sen vaikuttuvuuden, kelvollisuuden ja soveltuvuuden. Se tehdään organisaatiossa prosessina päivittäin, viikoittain tai kuukausittain keskustellen, kokoustaen tai tutkien raportteja. Johto kiinnittää tarkastuksessaan huomiota sidosryhmien ja tietoturvaan liittyvään palautteeseen sekä toimenpiteisiin, joita on aikaisemmin tarkastuksissa käynnistetty. He tarkastelevat sisäisten ja ulkoisten tekijöiden uudistuksia sekä

arviointien tuloksia ja jatkuvaa parantamista koskien tietoturvallisuuden hallintajärjestelmää ja hallintakeinojen tehokkuutta. Tarkastuksen tuloksiin kirjataan muutostarpeet tietoturvallisuuden hallintajärjestelmästä ja jatkuvaa parantamista koskevat päätökset. Tarkastuksista pitää tehdä dokumentteja, jotta voidaan osoittaa ISO 27001 - standardin osa-alueiden huomioonottaminen. (ISO/IEC 27001:fi 2017, 13; ISO/IEC 27003:fi 2017, 42–44.)

3.3.7 Parantaminen

Organisaation pitää kehittää jatkuvasti tietotuvallisuuden hallintajärjestelmän vaikuttavuutta, soveltuvuutta ja tarkoituksenmukaisuutta sekä arvioida sisäisiä ja ulkoisia tekijöitä ja sidosryhmien vaatimuksia (ISO/IEC 27003:fi 2017, 47).

Kun havaitaan poikkeama, organisaation on reagoitava välittömästi siihen ja arvioitava tilanne, korjata ja suorittaa tarvittavat toimenpiteet. Organisaation on aloitettava toimenpiteet poikkeaman korjaamiseksi sekä selvittää poikkeaman syyt ja korjata ne, jotta vastaava ei toistuisi. Organisaation on talletettava tietoa poikkeamista sekä korjaavista toimenpiteistä ja niiden tuloksista, jotta se voi todistaa käyttäytyneensä tilanteissa oikein. (ISO/IEC 27001:fi 2017, 14; ISO/IEC 27003:fi 2017, 44–46.)

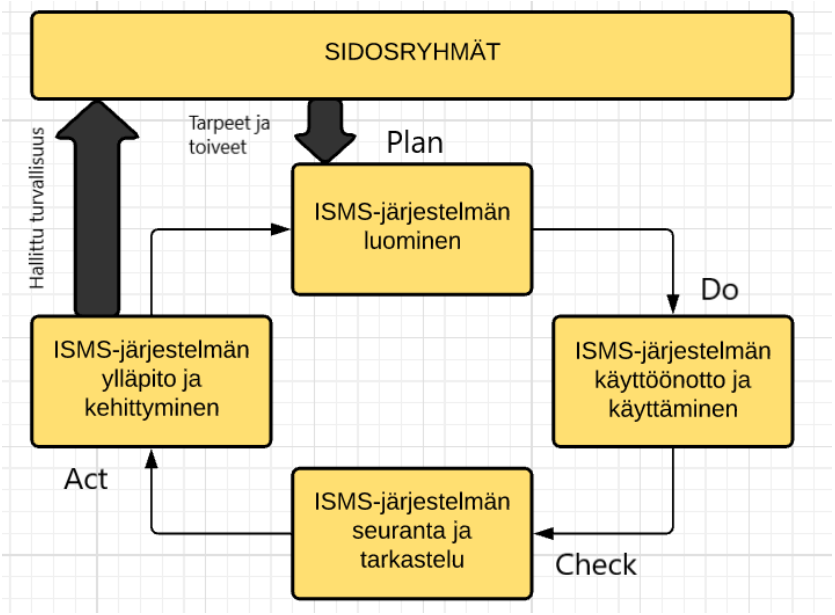
3.4 PDCA-malli

Standardissa hyödynnetään PDCA-mallia, joka tukee tietoturvallisuuden hallintajärjestelmän jatkuvaa uudistamista ja edistää organisaation reagointia vastata toimintaympäristön ja toiminnan muutoksista johtuneisiin turvallisuustarpeisiin (Hakala, Vainio & Vuorinen 2006, 106). PDCA-malli erotellaan neljään vaiheeseen:

- (Plan) Suunnittele: Laaditaan tietoturvapolitiikka, -tavoitteet ja -prosessit sekä toimintatavat, jotka ovat suhteessa tietoturvallisuuden hallintajärjestelmän politiikkaan ja tavoitteisiin sekä ovat välttämättömiä riskienhallintaa varten.
- (Do) Toteuta: Suoritetaan ja hyödynnetään tietoturvapolitiikkaa, prosesseja, toimintatapoja sekä valvontaa.

- (Check) Arvioi: Seurataan ja tarkkaillaan tietoturvallisuuden hallintajärjestelmää ja sen prosesseja. Verrataan saatuja mittaustuloksia tieturvapolitiikkaan, asetettuihin tavoitteisiin ja tottumuksiin sekä viestitään niistä johdolle.
- (Act) Toimi: Ylläpidetään ja kehitetään tietoturvallisuuden hallintajärjestelmää jatkuvasti aloittaen kehittävät ja tehostavat toimenpiteet, jotka on johdettu sisäisten auditointien, tulosten tai jonkin aiemman tiedon perusteella. (Andreasson & Koivisto 2013, 42–43.)

PDCA-malliin (kuva 4) on kuvattuna tietoturvallisuuden hallintajärjestelmän jatkuva ja prosessinomainen kehittäminen. Kun kierros on loppunut, aloitetaan aina uusi kierros.



Kuva 4. PDCA-mallin prosessi (Hakala, Vainio & Vuorinen 2006, 49)

4 TIETOTURVALLISUUDEN HALLINTAVOITTEET JA -KEINOT

Organisaation on huomioitava hallintavoitteiden ja -keinojen viiteluettelo, joka on kuvattuna ISO/IEC 27001 -standardin liitteessä A. Viiteluettelo liittyy standardin kohtaan 6.1.3, tietoturvariskien käsittelyyn. Organisaation on verrattava liitteen hallintakeinoja omiin hallintakeinoihin. Liite sisältää 14 turvallisuuden hallintaan liittyvää pääkohtaa, jotka koostuvat 35 pääturvallisuusluokasta ja 114 hallintakeinoista. Kohdat eivät ole kuvattuna tärkeysjärjestyksessä. (ISO/IEC 27001:fi 2017, 9 & 15; ISO/IEC 27002:fi 2017, 8.)

4.1 Tietoturvapolitiikat

Johdon pitää ohjata ja edistää tietoturvallisuuden toteuttamista lakien, asetusten ja vaatimusten mukaan. Tietoturvallisuudelle on laadittava joukko politiikkoja, jotka ovat johdon hyväksymiä ja niistä on viestittävä henkilökunnalle ja olennaisille ulkoisille osapuolille. Tietoturvapolitiikat pitää tarkastaa tietyn aikavälein tai kun muutoksia on ilmennyt. Säännöllisellä tarkastamisella vahvistetaan, että tietoturvapolitiikat ovat yhä vakuuttavia, päteviä ja sopivia. (ISO/IEC 27001:fi 2017, 15.)

4.2 Tietoturvallisuuden organisointi

Tietoturvallisuuden organisointi jakaantuu sisäiseen organisaatioon sekä mobiililaitteisiin ja etätyöhön.

4.2.1 Sisäinen organisaatio

Tarkoituksena on laatia hallintarakenne, jolla tietoturvallisuuden toteuttaminen ja hyödyntäminen aloitetaan. Kaikki tietoturvaroolit – ja vastuut on havaittava ja ryhmiteltävä. Ristiriitaiset tehtävät ja vastuualueet on eroteltava, jotta suojattavan omaisuuden asiaton muuntelu ja väärinkäyttö vähenisi. On pidettävä yhteyttä osaamisyhteisöihin, ammatillisiin järjestöihin ja viranomaisiin sekä määritellä menettelyohjeet, josta selviäisi kenen ja milloin viranomaisia on tavoitettava sekä miten tietoturvahäiriöistä on

kirjattava. Projektinhallinnassa on käytettävä tietoturvallisuutta huolimatta projektityypistä ja sen luonteesta. Tietoturvallisuus on liitettävä osaksi organisaation projektinhallintamenetelmää, joka edellyttää, että tietoturvatavoitteet ovat osa projektitavoitteita ja tietoturvariskien arviointi toteutetaan aikaisessa vaiheessa, jotta saadaan tunnistettua välttämättömät hallintakeinot sekä tietoturvallisuuden on kuuluttava projektinmenettelyn kaikkiin vaiheisiin. (ISO/IEC 27001:fi 2017, 15; ISO/IEC 27002:fi 2017, 12–13.)

4.2.2 Mobiililaitteet ja etätyö

Organisaation pitää ottaa käyttöön mobiililaitteisiin liittyvä politiikka ja sitä edistävät turvallisuuskäytännöt, jotka ohjaavat mobiililaitteiden käytöstä johtuvia riskejä. Henkilökunnalle on järjestettävä koulutusta sekä kertoa mobiililaitteiden todennäköisistä riskeistä ja hallintakeinoista. Organisaation on huolehdittava, että mobiililaitteiden käyttäminen on turvallista. Liiketoimintatiedot eivät saa vaarantua, kun laitteita käytetään suojaamattomissa ympäristöissä. (ISO/IEC 27001:fi 2017, 15–16; ISO/IEC 27002:fi 2017, 14.)

Mobiililaitteita käsittelevässä politiikassa pitää huomioida riskit ja kuvailla, sallitaanko henkilökohtaisten mobiililaitteiden käyttö organisaation verkossa. Politiikassa tarkasteltavat asiat ovat:

- Mobiililaitteiden rekisteröiminen
- Fyysinen suojaaminen
- Ohjelmistojen asentamisen ja tietojenkäsittelypalvelujen rajoitukset
- Haittaohjelmistoilta suojautuminen
- Ohjelmistoversioiden ja päivitysten asentaminen
- Salaustekniikat
- Pääsynhallinta
- Varmuuskopioiminen
- Verkkosovellusten ja -palveluiden käyttäminen
- Etäsammuttaminen, -lukitseminen tai -poistaminen (ISO/IEC 27002:fi 2017, 14.)

Organisaation tulisi ottaa käyttöön etätyöpolitiikka ja sitä vahvistavat turvallisuuskäytännöt, jotka tukevat etätyöpaikassa hyödynnettyä, muokattua tai säilytettävää tietoa. Etätyöpolitiikka täsmentää etätyötä koskevia rajoituksia ja ehtoja. Politiikassa tulisi kiinnittää huomiota seuraavin kohtiin, kun ne ovat soveltuvia ja lain mukaisia:

- Etätyöpaikan fyysinen työympäristö ja turvallisuus.
- Tietoliikenteen turvallisuusvaatimukset ottaen huomioon tiedon arkaluontoisuuden, kun tietoa siirretään tietojärjestelmän yli tai käytetään etänä organisaation sisäisissä järjestelmissä.
- Oikeus virtuaalipöydälle, joka estää tiedon käsittelemisen ja tallentamisen henkilökohtaisiin laitteisiin.
- Muiden henkilöiden aiheuttama uhka, kun he käyttävät tietoa ja resursseja luvattomasti jakaessaan saman tilan.
- Kotiverkkojen ja langattomien verkkopalvelujen konfiguraatiota koskevat rajoitukset ja vaatimukset.
- Menettelyt ja politiikat, jotka ehkäisevät henkilökohtaisella laitteella luotuja aineettomaan omaisuuteen liittyviä kiistoja.
- Henkilökohtaisiin laitteisiin pääsy.
- Ohjelmistolisenssisopimukset, joiden mukaan organisaatiot voivat olla vastuussa asiakasohjelmistolisensseistä, jotka ovat ulkopuolisten osapuolten tai työntekijöiden henkilökohtaisissa työasemissa.
- Palomuuriin ja haittaohjelmilta suojautumiseen liittyvät vaatimukset.
(ISO/IEC 27001:fi 2017, 16; ISO/IEC 27002:fi 2017, 15.)

4.3 Henkilöstöturvallisuus

Henkilöstöturvallisuuden tavoitteena on tarkistaa, että organisaation työntekijät ja vuokratyöntekijät käsittävät velvollisuutensa ja ovat soveliaita heille mietittyihin tehtäviin. Työsopimuksessa on kerrottava organisaation ja työntekijän tai vuokratyöntekijän vastuut tietoturvallisuudesta. Työntekijöiden tausta on tarkastettava määräysten, eettisten normien ja lakien mukaisesti sekä ne on suhteutettava liiketoiminnallisiin vaatimuksiin, tarkasteltavan tiedon luokitukseen ja arvioituihin riskeihin. Taustatarkastuksissa kiinnitetään huomioita tietosuojaan, työyhteisöön liittyvään lainsäädäntöön ja henkilötietojen suojaamiseen. Tarkastuksiin on mahdollisesti sisällytettävä

kattava henkilösuositusten saatavuus, hakijan ansioluettelon oikeellisuuden ja vastaavuuden tarkistaminen, koulutuksen tai ammatillisen pätevyyden todentaminen, henkilöllisyyden tarkistaminen, kuten passi tai muu vastaava asiakirja ja perusteellinen tarkastus, kuten rikosrekisteri tai luottotiedot. (ISO/IEC 27001:fi 2017, 16; ISO/IEC 27002:fi 2017, 16.)

Johdon on velvoitettava, että henkilöstö toimii tietoturvallisesti noudattaen menettelyjä ja politiikkoja. Henkilöstön on saatava riittävästi tietoturvakoulutusta ja -opastusta sekä heidän tietojaan on päivitettävä säännöllisesti työsuhteen aikana. Organisaatiolla tulisi olla kurinpitoprosessi, joka kuvailee toimintaohjeet, kun työntekijä on rikkonut tietoturvaa. Organisaation on asetettava tietoturvavelvollisuudet ja -vastuut sekä viestittävä ja tarkistettava niiden noudattaminen, kun työsuhde päättyy tai vastuu muuttuu suojatakseen organisaatiota. (ISO/IEC 27001:fi 2017, 16.)

4.4 Suojattavan omaisuuden hallinta

Organisaation on yksilöitävä tietoon ja tietojenkäsittelypalveluihin koskeva suojattava omaisuus, joka on luetteloitava ja ylläpidettävä jatkuvasti. Suojattavalla omaisuudella pitää olla omistaja, joka on vastuussa sen hallinnasta ja ajantasaisuudesta. Suojattavan omaisuuden sallittava käyttö ja siihen liittyvät säännöt on dokumentoitava, yksilöitävä ja toteuttava, jotta suojattavaa tietoa käyttävät henkilöt olisivat tietoisia tietoturvavaatimuksista. Kun työtehtävän, työsuhde tai sopimus päättyy, työntekijän ja organisaation ulkopuolisen käyttäjän on palautettava hallussaan oleva organisaation omaisuus. Organisaation on huolehdittava, että tiedolla on riittävä suojaustaso. Suojaustaso riippuu siitä, miten merkittävä tieto on. Tieto täytyy luokitella kriittisyyden, laakisääteisten vaatimusten ja tiedon arvon mukaan. Suojattavan omaisuuden käsittelemiselle ja tiedon merkitsemiselle on laadittava tietyt käytännöt. Siirrettäessä tai hävittäessä tietovälineitä, on estettävä tietojen poistaminen, muuttuminen, turmeleminen tai väärinkäyttäminen. (ISO/IEC 27001:fi 2017, 17–18; ISO/IEC 27002:fi 2017, 21–22.)

4.5 Pääsynhallinta

Pääsynhallinnan liiketoiminnallisena vaatimuksena on pääsynhallintapolitiikka sekä pääsyoikeudet ainoastaan niihin verkkoihin ja verkkopalveluihin, jotka ovat myönnetty käyttäjille. Käyttäjien tunnistautumistietoja ja ylläpito-oikeuksia on hallittava ja rajoitettava. Pääsyoikeudet on muutettava tai poistettava, kun työsuhde, työtehtävä tai sopimus muuttuu tai päättyy noudattaen rekisteröinti-, poistamis- ja jakoprosessia sekä niitä on uudelleenarvioitava tietyn väliajoin. Pääsyoikeuden myöntäminen tai niiden poistaminen on kaksivaiheinen prosessi:

1. Myönnetään ja aktivoidaan käyttäjätunnus tai suljetaan.
2. Myönnetään tai kumotaan pääsyoikeus käyttäjätunnukseen. (ISO/IEC 27001:fi 2017, 18; ISO/IEC 27002:fi 2017, 29.)

Käyttäjien on noudatettava organisaation tapoja, kun he tunnistautuvat järjestelmiin. Järjestelmien ja sovellusten pääsynhallinnassa on rajoitettava tietoihin ja ohjelmien lähdekoodeihin pääsemistä pääsynhallintapolitiikan mukaisesti sekä käytettävä turvallista kirjautumismenettelyä, vahvoja salasanoja ja yksilöllisiä käyttäjätunnuksia, jotta voidaan estää luvatonta pääsyä järjestelmiin ja sovelluksiin. (ISO/IEC 27001:fi 2017, 19; ISO/IEC 27002:fi 2017, 33–35.)

4.6 Salaus

Salauksen periaatteista ja salausavainten hallinasta on tehtävä ja toteuttava politiikka, jota on noudatettava suojatessa tietoa salauksen avulla. Politiikan tulisi kiinnittää huomiota salauksen hallintakeinojen hyödyntämisestä organisaatiossa, tarvittavaan suojaustasoon, mobiililaitteiden tai siirrettävien tietovälineiden salauksen käytöstä ja salausavainten suojaamisesta, käytöstä ja käyttöiästä sekä kuinka toimia, kun salausavaimet vaarantuvat, häviävät tai luodessa uusi avain eri salausjärjestelmään ja eri sovellukseen. Politiikkaa tulisi noudattaa koko ajan. (ISO/IEC 27001:fi 2017, 19; ISO/IEC 27002:fi 2017, 36–38.)

4.7 Fyysinen turvallisuus ja ympäristön turvallisuus

On rajattava fyysinen turva-alue, jota on noudatettava tietojenkäsittelypalveluissa ja käsiteltäessä arkaluontoista tai kriittistä tietoa. Turva-alueisiin on luotava kulunvalvonta ja määritellä menettelyohjeet, kuinka työskennellä turva-alueilla. On suunniteltava toimistojen, laitteistojen ja tilojen suojaus sekä fyysiset suojakeinot uhkia vastaan, kuten onnettomuuksien tai luonnonkatastrofien varalta. Toimitus- ja kuormausalueet tulisi olla valvottuja tiloja ja ne olisi eristettävä tietojenkäsittelypalveluista. Tavoitteena olisi estää tietojen vahingoittuminen, toiminnan häiriintyminen ja luvaton pääsy organisaation tietoihin. (ISO/IEC 27001:fi 2017, 19–20.)

Laitteistoja olisi suojattava häiriöiltä, huollettava säännöllisesti ja sijoitettava organisaatiossa siten, että estettäisiin tiedon katoaminen, vahingoittuminen, vaarantuminen tai varastaminen. Sähkö- ja tietoliikennekaapelointi sekä toimitilan ulkopuolinen suojattava omaisuus tulisi turvata vahingoittumiselta, häirinnältä ja salakuuntelulta. Laitteet olisi tarkastettava ennen kuin ne poistetaan käytöstä tai kierrätetään, ettei laitteeseen olisi jäänyt suojattavia ohjelmistoja tai tietoja. Käyttäjien on tarkistettava, että ilman valvontaa olevat laitteet ovat riittävän suojattuja. Tallennusvälineissä, tietojenkäsittelypalveluissa ja papereissa tulisi noudattaa puhtaan näytön ja pöydän periaatetta. Sen tarkoituksena olisi, että arkaluontoinen tai kriittinen tieto säilytetään lukitussa paikassa, tietokoneista on kirjauduttava ulos niiden jäädessä ilman valvontaa ja kopiointilaitteiden luvaton käyttö on estettävä sekä tulostimista on poistettava heti arkaluontoiset tai salaiset tiedot. (ISO/IEC 27001:fi 2017, 20–21; ISO/IEC 27002:fi 2017, 46.)

4.8 Käyttöturvallisuus

Käyttöturvallisuudessa laaditaan dokumentoidut toimintaohjeet tietokoneiden käynnistys- ja sammutusmenettelystä, laitteiden huollosta, tiedonvarmistuksesta, tietovälineiden käsittelystä sekä tietokonehuoneen turvallisuudesta ja hallinnasta. Toimintaohjeet pitää olla saatavissa niitä tarvitseville käyttäjille. Tietoturvallisuuteen liittyviä muutoksia on hallittava ja kiinnitettävä huomiota esimerkiksi muutosten tunnistamiseen ja kirjaamiseen, tietoturvavaatimusten toteutumiseen ja muutosten hyväksymisprosessiin. Kapasiteettivaatimukset pitää yksilöidä huomioiden järjestelmän

kriittisyyden liiketoiminnan osalta. Riittävä kapasiteetti saadaan, kun rajoitetaan kaistanleveyttä, poistetaan vanhentuneita tiedostoja, sovelluksia tai tietokantoja sekä optimoidaan eräajoprosesseja ja sovelluslogiikkaa. (ISO/IEC 27001:fi 2017, 21–22; ISO/IEC 27002:fi 2017, 46–48.)

Tuotantoympäristön muuttumisen ja luvattoman käytön riski vähenee, kun kehitys-, testaus ja tuotantoympäristöt eritellään toisistaan. Haittaohjelmilta suojautuessa käytetään apuna erilaisia palautus-, havaitsemis- ja estomekanismeja sekä käyttäjille tiedotetaan jatkuvasti haittaohjelmista. Organisaation järjestelmät, ohjelmistot ja tiedostot on varmuuskopioitava tietyn väliajoin ja niille on laadittava varmuuskopiointipolitiikka, joka tarkentaisi varmuuskopiointivaatimukset. Toiminnoista, poikkeamista, virheistä ja tietoturvatapahtumista on kirjattava, säilytettävä ja tarkasteltava säännöllisesti sekä suojattava väärentämiseltä ja luvattomalta pääsyltä. On talletettava tietoa järjestelmän pääkäyttäjistä ja operaattorien toiminnoista, jotta vastuu voidaan säilyttää ylläpito-oikeuden haltijoilla. Samalla turvallisuusalueella tai organisaatiossa olevat tietojärjestelmäkellot pitää synkronoida. (ISO/IEC 27001:fi 2017, 21–22; ISO/IEC 27002:fi 2017, 51–53.)

Tuotannossa oleviin järjestelmiin on laadittava menettelyohjeet, kun niihin asennetaan ohjelmistoja ja jotta niitä voidaan valvoa. Ohjelmien asentamista on rajoitettava yhteisillä säännöillä. Järjestelmien teknisiä haavoittuvaisuuksia on seurattava, jotta altistuminen voidaan arvioida ja luoda niille hyväksyttävät toimenpiteet. Tietojärjestelmien auditointimekanismit on suunniteltava siten, että ne vaikuttavat muihin käytössä oleviin järjestelmiin hyvin vähän. (ISO/IEC 27001:fi 2017, 22.)

4.9 Viestintäturvallisuus

Viestintäturvallisuuden tarkoituksena on suojata verkossa liikkuvaa tietoa ja sitä tukevia tietojenkäsittelypalveluita. Verkkoja on valvottava ja hallittava, jotta tieto järjestelmien ja sovelluksien tieto olisi suojattua. Verkkopalvelujen palvelutasot, turvamekanismit ja hallintavaatimukset tulisi yksilöidä ja yhdistää aina verkkopalvelusopimuksiin. Tietojenkäsittelypalvelut, tietojenkäsittelyryhmät ja käyttäjät on eriteltävä selkeästi jakaen ne erillisiksi verkkoalueiksi luottamustason, organisaatioyksiköiden

tai jonkin muun yhdistelmän mukaan. Tiedon siirtäminen turvataan tiedonsiirtopolitiikan ja -menettelyjen sekä tiedonsiirtoa koskevien sopimuksien avulla. Sähköisessä viestinnässä olisi tarkasteltava esimerkiksi, että viestit on suojattu luvattomalta pääsyltä, viestillä on oikea osoite, lakiasioita sekä palvelun luotettavuutta ja saatavuutta. Vaitiolo- ja salassapitosopimukset pitää yksilöidä, tarkastella toistuvasti ja dokumentoida. (ISO/IEC 27001:fi 2017, 22–23; ISO/IEC 27002:fi 2017, 58–61.)

4.10 Järjestelmien hankkiminen, kehittäminen ja ylläpito

Tietojärjestelmien turvallisuusvaatimuksien tehtävänä on turvata, että tietoturvallisuus on merkittävä osa tietojärjestelmiä ja ne on sisällytettävä tietojärjestelmiä koskeviin vaatimuksiin. Sovelluspalveluita ja niiden tapahtumia on suojattava, jotta estetään niiden muuttuminen, kopiointi, puutteellinen lähetys tai väärään paikkaan joutuminen. (ISO/IEC 27001:fi 2017, 23.)

Kehitys- ja tukiprosessien turvallisuuden tarkoituksena on, että tietoturvallisuutta laaditaan osana tietojärjestelmien kehittämistä. Ohjelmien ja järjestelmien kehittämistä varten on laadittava säännöt sekä muutoksia on hallittava organisaation määrittämillä muutosten hallintamenettelyillä. Ohjelmistopaketteihin on suoritettava vain pakolliset muutokset. Organisaation on toteutettava turvallisen järjestelmäsuunnittelun periaatteet ja turvallinen kehitysympäristö sekä tarkasteltava ulkoistettua kehittämistä. Aina muutosten jälkeen, on suoritettava tekninen tarkastelu ja testaus. Testiaineistot on suojattava tiedon suojaamiseksi. Järjestelmälle on suoritettava turvallisuustestaus sekä suunnitella hyväksymistestausohjelmat ja kriteerit. (ISO/IEC 27001:fi 2017, 23–24.)

4.11 Suhteet toimittajiin

Organisaation toimittajien käyttämä tieto pitää olla valvottua ja suojattua sekä jokaisen toimittajan kanssa on sovittava tietoturvavaatimuksista tietoturvapolitiikassa. Tietoturvallisuuden hallintakeinot tulisi yksilöidä ja toimittajien pääsyä organisaation tietoihin on täsmennettävä koskemaan organisaation menettelyjä ja prosesseja. Tietoturvavaatimusten on vähennettävä suojattavaan omaisuuteen liittyviä riskejä ja kerrottava tieto- ja viestintäpalvelun sekä tuotteen toimitusketjujen vaatimuksista reagoida

tietoturvariskeihin. Toimittajien palveluiden hallinnan ja säännöllisen tarkastuksen tehtävänä on edistää toimittajasopimuksissa määriteltyä tietoturvatasoa ja palveluiden toimitustasoa. Toimittajasopimukset on toteutettava ja dokumentoitava ehkäistäkseen väärinkäsityksiä. (ISO/IEC 27001:fi 2017, 24–25; ISO/IEC 27002:fi 2017, 71–72.)

4.12 Tietoturvahäiriöiden hallinta

Tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinnasta on laadittava toimintamalli, joka on vaikuttava, johdonmukainen sekä siinä viestitään ja raportoidaan tietoturvatapahtumista ja -heikkouksista. Organisaation on eriteltävä hallintavastuut ja menettelyt, jotta osataan reagoida pikaisesti, tehokkaasti ja menettelyohjeiden mukaisesti tietoturvahäiriöihin. Henkilöstön on tiedettävä vastuustaan ja tietoturvatapahtumien yhteydenottopisteen sijainnista, johon tietoturvatapahtumat raportoidaan. (ISO/IEC 27001:fi 2017, 25; ISO/IEC 27002:fi 2017, 76–78.)

Tietoturvatapahtumat pitää arvioida sekä niiden analysoinnista on opittava, jotta voidaan vähentää tulevia häiriöitä ja pienentää niiden vaikutuksia. Todisteiden kokoamista, yksilöimistä, hankkimista, keräämistä ja säilyttämistä varten on suunniteltava menettelyt, kun todisteita tarkastellaan. Menettelyssä olisi kiinnitettävä huomiota hallussapitoketjuun, henkilöstön ja todisteiden turvallisuuteen, henkilöstön pätevyyteen, selontekoihin, ja dokumentaatioon sekä asiaan koskevien henkilöiden vastuisiin ja rooleihin. (ISO/IEC 27001:fi 2017, 25–26; ISO/IEC 27002:fi 2017, 76–79.)

4.13 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia

Liiketoiminnan jatkuvuuden hallintajärjestelmiin on yhdistettävä tietoturvallisuuden jatkuvuus, jolle on asetettava vaatimukset tietoturvallisuuden jatkuvuudesta epäsuotuisissa tilanteissa sekä noudatettava jatkuvasti prosesseja ja käytäntöjä tietoturvallisuuden jatkuvuuden parantamiseksi. Tietoturvallisuutta ja sen hallintakäytäntöjä on tarkasteltava säännöllisesti, jotta jatkuvuus säilyisi. Tietojenkäsittelypalvelut on rakennettava vikasietoisiksi, jotta saatavuusvaatimukset täyttyisivät. Jos saatavuutta ei voida luvata, organisaation olisi investoitava päällekkäinen komponentti ja testattava sen toimintakyky. Olisi mahdollisuus siirtyä toiseen järjestelmään moitteettomasti,

kun vika ilmenee toiseen komponenttiin. (ISO/IEC 27001:fi 2017, 26; ISO/IEC 27002:fi 2017, 81.)

4.14 Vaatimustenmukaisuus

Organisaatiossa on noudatettava tietoturvallisuuden lakeja ja asetuksia sekä viranomaisten ja sopimusten vaatimuksia. Organisaatiossa on laadittava ja suoritettava menettelyt tekijän- ja immateriaalioikeuksiin suojattujen ohjelmistojen käytöstä. Immateriaalioikeudet määrittävät asiakirjojen ja ohjelmistojen tekijänoikeudet, tavaramerkit, suunnitteluoikeudet, lähdekoodilisenssit ja patentit. Tallenteet pitää suojata väärentämiseltä, katoamiselta, tuhoutumiselta sekä luvattomalta käytöltä ja levittämiseltä liiketoiminnan vaatimusten mukaisesti. Henkilötieto- ja tietosuoja on tarkistettava lakien ja viranomaisten vaatimusten mukaisesti sekä salaustekniikan hallintaa koskevia sääntöjä on noudatettava. (ISO/IEC 27001:fi 2017, 26–27; ISO/IEC 27002:fi 2017, 83.)

Esimiesten on tehtävä säännöllisesti tietoturvallisuuden tarkastukset tai kun on tapahtunut muutoksia, jotta voidaan vahvistaa tietoturvallisuuden hallintajärjestelmän vaatimustenmukaisuus ja tehokkuus. Tietoturvallisuuden tarkastuksissa kiinnitetään huomiota hallintatavoitteisiin ja -keinoihin, prosesseihin, menettelyihin ja politiikkaan. Jos havaitaan poikkeama, esimiesten pitäisi tunnistaa poikkeaman syyt, arvioida tarvittava toimenpide ja suorittaa se sekä tarkastettava suoritettu toimenpide, jotta sen vaikuttavuus, heikkoudet ja puutteet voidaan todeta. (ISO/IEC 27001:fi 2017, 27; ISO/IEC 27002:fi 2017, 85–86.)

5 RISKIT

Riski tarkoittaa vaaraa tai uhkaa, johon liittyvät tekijät ovat tapahtuman epävarmuus, odotukset, laajuus sekä vakavuus ja ne vaikuttavat siihen, millaisena riski koetaan. Riski määritellään todennäköisyyden ja riskin vakaavuuden mukaan. (Juvonen ym. 2014, 8–9.)

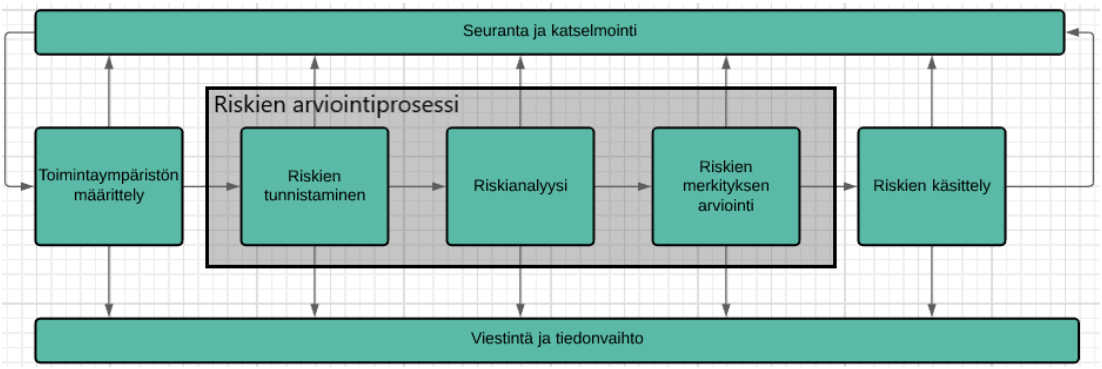
Riskit jaetaan usein neljään riskilajiin:

- Strategiset riskit ovat liiketoimintaympäristöön ja kehittymiseen liittyviä riskejä.
- Operatiiviset riskit liittyvät yrityksen päivittäisiin toimintoihin, kuten johtamiseen, tuottavuuteen tai tietoturvaan.
- Taloudelliset riskit viittaavat yrityksen rahaprosessiin ja maksuvalmiuteen.
- Vahinkoriskeillä tarkoitetaan työterveys- ja turvallisuusriskejä sekä ympäristöriskejä. (Ilmonen, Kallio, Koskinen & Rajamäki 2016, 76–81.)

5.1 Riskienhallintaprosessi

Riskienhallintaprosessi tarkoittaa systemaattista tapaa, jossa riskejä tunnistetaan, arvioidaan ja raportoidaan. Sen on oltava organisaatiossa osa päätöksentekoa ja johtamista sekä kuuluttava prosesseihin, toimintoihin ja rakenteeseen. Riskienhallintaprosessin tavoitteena on havaita yrityksen liiketoimintaa, prosesseja, tavoitteita ja kilpailuetuja uhkaavia riskejä. (Ilmonen ym. 2016, 95–96; ISO/IEC 31000:fi 2018, 14.)

Riskienhallintaprosessi on kuvattuna kuvassa 5 ja se perustuu ISO 31000 -standardin riskienhallinta- ja arviointiprosessien kuvaamiseen. Riskien arvioinnin osa-alueet ovat riskien tunnistaminen, riskianalyysi ja riskien merkityksen arviointi (Ilmonen ym. 2016, 19). Riskienhallintaprosessin vaiheet (kuva 5) ovat kuvattuna tarkemmin seuraavana.



Kuva 5. Riskienhallintaprosessi (Kangas 2017, 2)

5.1.1 Toimintaympäristön määrittäminen

Organisaation on määriteltävä kattavuus, toimintaympäristö ja riskien kriteeristö, jotta riskienhallintaprosessista tulisi organisaatiolle sopiva. Riskin kriteeristössä kuvataan esimerkiksi, mitkä riskit ovat siedettäviä ja mitä riskitasoa tavoitellaan. (Juvonen ym. 2014, 17–18; ISO/IEC 31000:fi 2018, 15.)

5.1.2 Riskien tunnistaminen

Riskien tunnistamisen tavoitteena on etsiä, havaita ja kuvata kaikki riskit, jotka edistävät organisaatiota tavoitteiden saavuttamisessa tai ovat niiden esteenä. On kiinnitettävä huomiota myös sellaisiin riskeihin, joiden lähteet eivät ole organisaation hallinnassa. (ISO/IEC 31000:fi 2018, 16–17.)

Kangas (2017, 8) kertoo, että riskin tunnistamisvaiheessa (kuva 6) ensimmäisenä on kirjattava riskin nimi tai kuvailla riski lyhyesti, jonka jälkeen riski sijoitetaan riskiluokkaan. Riskiluokitus voi noudattaa riskien yleistä luokittelua (kohdat 1–4) tai organisaatiolla voi olla käytössä oma riskiluokituksensa.

1. Strategiset riskit
2. Operatiiviset riskit
3. Taloudelliset riskit
4. Vahinkoriskit

Viimeisenä on määriteltävä yksilöivä tunniste, jossa noudatetaan organisaation käytäntöjä.

	Riskien tunnistaminen		
Riskin tunniste	Riskiluokka	Riski (riskin nimi)	Riskin kuvaus (mistä riski johtuu, mitä voi tapahtua)
	Arvo 1-4		
	Arvo 1-4		
	Arvo 1-4		
	Arvo 1-4		
	Arvo 1-4		

Kuva 6. Riskien tunnistaminen (Kangas 2017, 8)

5.1.3 Riskianalyysi

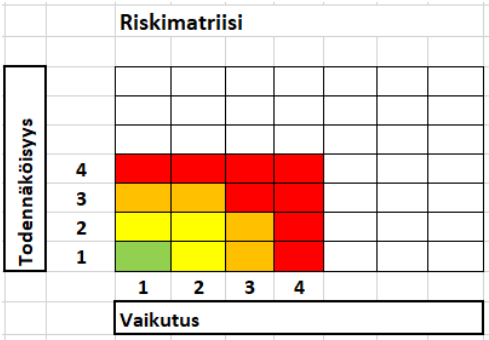
Riskianalyysissa (kuva 9) on arvioitava havaittujen riskien todennäköisyyttä ja vaikuttavuutta, jotta riskeihin osataan varautua enemmän (Juvonen ym. 2014, 20). Kangas (2017, 9) toteaa, että organisaatio hyödyntää analyysissa valitsemaansa asteikkoa tai voidaan käyttää yleisiä todennäköisyyden ja vaikutuksen arvoja. Yleiset todennäköisyyden ja vaikutuksen arvot ovat kuvattuna seuraavana (kuva 7).

Todennäköisyyden arvot	
4	Lähes varma
3	Todennäköinen
2	Mahdollinen
1	Epätodennäköinen

Vaikutuksen arvot	
4	Kriittinen
3	Merkittävä
2	Kohtalainen
1	Vähäinen / ei vaikuta

Kuva 7. Todennäköisyyden ja vaikutuksen arvot (Kangas 2017, 6)

Kangas (2017, 6) jatkaa, että organisaatiossa on kehotettu käyttämään vain yhtä matriisia (kuva 8). Väriasteikko vaihtelee organisaatioittain.



Kuva 8. Riskimatriisi (Kangas 2017, 6)

Riskianalyysi	
Todennäköisyys	Vaikutus
Ei arvioitu	Ei arvioitu
Ei arvioitu	Ei arvioitu
Ei arvioitu	Ei arvioitu
Ei arvioitu	Ei arvioitu
Ei arvioitu	Ei arvioitu

Kuva 9. Riskianalyysi (Kangas 2017, 9)

5.1.4 Riskien merkityksen arviointi

Riskien merkityksen arvioinnissa (kuva 10) verrataan riskianalyysin tuloksia riskikriteereihin, jotta saadaan selville, tarvitaanko lisää jatkotoimenpiteitä (ISO/IEC 31000:fi 2018, 18). Kangas (2017, 10) täsmentää, että riskin suuruus tarkoittaa todennäköisyyden ja vaikutuksen tuloa. Kun riskin suuruus on ratkaistu, on arvioitava, millaisia toimenpidetarpeita tarvitaan. Riskin suuruutta voidaan kuvailla seuraavasti

- Ei riskiä
- Huomioitava riski
- Merkittävä riski
- Sietämätön riski

Toimenpidetarpeita ovat esimerkiksi

- Kriittinen riski
- Merkittävä tai nopeita reaktioita vaativa riski
- Huomioitava tai seurattava riski
- Otettava riski
- Ei riskiä

Riskin merkityksen arviointi	
Riskin suuruus (T x V)	Toimenpidetarpeet (vakavuus/sietokyky)
Ei arvioitu	Ei arvioitu
Ei arvioitu	Ei arvioitu
Ei arvioitu	Ei arvioitu
Ei arvioitu	Ei arvioitu
Ei arvioitu	Ei arvioitu

Kuva 10. Riskien merkityksen arviointi (Kangas 2017, 10)

5.1.5 Riskien käsittely

Riskien käsittelyn (kuva 11) tavoitteena on valita riskienhallintamenetelmä tai toimenpide, joka voi olla riskin välttäminen, jakaminen, pienentäminen, siirtäminen tai omalla vastuulla pitäminen (Juvonen ym. 2014, 23). Kangas (2017, 12) kertoo, että toimenpiteiden lisäksi on nimettävä vastuuhenkilöt ja tavoiteaikataulu.

	Riskin käsittely		
Toimenpide-ehdotukset riskin käsittelylle	Toimenpiteiden vapaamuotoinen kuvaus	Vastuuhenkilö	Tavoiteaikataulu (mihin mennessä toimenpiteitä)
Ei arvioitu			
Ei arvioitu			
Ei arvioitu			
Ei arvioitu			
Ei arvioitu			

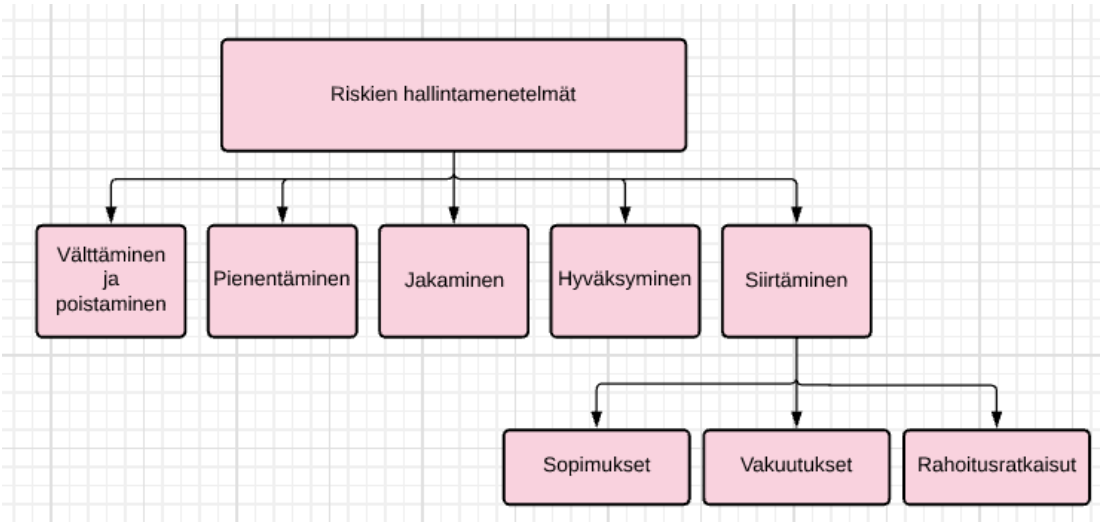
Kuva 11. Riskien käsittely (Kangas 2017, 12)

5.1.6 Seuranta ja katselmointi sekä viestintä

Seuranta ja katselmointi pitää olla osa riskienhallintaprosessia ja siihen on liityttävä säännölliset tarkastukset ja jatkuva tulosten tutkiminen. Vastuut on määritettävä ja rajattava selkeästi. Riskienhallintaprosessi ja sen tulokset on talletettava ja raportoitava. Prosessin vaiheissa on varmistettava riittävä sidosryhmien välinen viestintä, jonka tavoitteena on lisätä tietoa ja käsitystä riskeistä. Tiedonvaihdossa keskitytään hankkimaan päätöksentekoa tukevia palautteita ja tietoja. (Kangas 2017, 13; ISO/IEC 31000:fi 2018, 14–19.)

5.2 Riskien hallintamenetelmät

Organisaation omat riskienhallintatoimenpiteet ovat riskin välttäminen ja poistaminen, pienentäminen ja hyväksyminen (Ilmonen ym. 2016, 130). Myös riskin jakaminen on merkittävä hallintamenetelmä (Juvonen 2014, 26). Riskejä on hallittava ensisijaisesti organisaation omilla menetelmillä ja tarvittaessa riskejä voidaan siirtää vakuutuksilla, sopimuksilla ja rahoitusratkaisuilla kolmannelle osapuolelle. Riskihallintatoimenpiteitä on kohdistettava erityisesti kriittisiin riskeihin ja sen valintaan vaikuttavat esimerkiksi riskiarvioinnin tulokset, käytettävät taloudelliset- ja henkilöresurssit ja kilpailutilanne. (Ilmonen ym. 2016, 130–131.) Riskienhallintamenetelmiä havainnollistaa kuva 12.



Kuva 12. Riskienhallintamenetelmät mukaillen Ilmosta ym. (Ilmonen ym. 2016, 130)

5.2.1 Riskin välttäminen ja poistaminen

Juvonen ym. (2014, 24) mukaan riskin välttäminen tarkoittaa, että organisaatio pidättäytyy riskialttiista toiminnasta, omaisuudesta tai henkilöstä. Keinoja ovat esimerkiksi työsuojelutoimenpiteet, rakenteellinen ennaltaehkäisy ja henkilökunnan koulutukset. Riskin välttäminen voi lisätä menoja tai vähentää tuloja. Riskin välttämisen etäisin muoto on riskin poistaminen.

Riski on harvoin kokonaan poistettavissa, ja poistettava riski voi saada aikaan toisen riskin. Riskitekijät on poistettava erityisen tarkasti merkittävistä henkilöriskeistä sekä

ympäristö- ja turvallisuusriskeistä. Niiden tavoitteena on nollatoleranssi. Kun harkitaan riskin poistamista, on verrattava siitä saatavaa hyötyä sen aiheuttamiin kustannuksiin. (Ilmonen ym. 2016, 133.)

5.2.2 Riskin pienentäminen

Riskin pienentämisen tavoitteena on riskin seurausten tai todennäköisyyden pienentäminen (Juvonen ym. 2014, 24; Ilmonen ym. 2016, 133). Ilmosen ym. (2016, 133) mukaan riskit kehittyvät yrityksen omasta toiminnasta tai sen muutoksista. Riskejä voidaan pienentää useilla keinoilla, kuten lisäämällä resursseja, koulutusta ja teknisiä suojelutoimenpiteitä.

5.2.3 Riskin jakaminen

Riskin jakamisessa on kyse siitä, että itsenäisten riskikohteiden lukumäärää lisätään esimerkiksi jakamalla toimintaa eri osiin tai paikkakuntiin. Jakamisen tavoitteena on ehkäistä yksipuolisuudesta johtuvia riskejä ja se voi parhaimmillaan estää toiminnan pysähtymisen tai tuhoutumisen. Riskin jakaminen usein lisää kustannuksia. (Suominen 2003, 103–104; Juvonen ym. 2014, 26)

5.2.4 Riskin hyväksyminen

Paras ratkaisu mitättömissä ja epätodennäköisissä riskeissä voi olla, että ne hyväksytään osana liiketoimintaa. Riskeistä sovitaan ainoastaan se, kuka on vastuussa niiden seuraamisesta ja raportoimisesta. Riskien arvioinnissa on syytä huomioida niiden kokonaisvaikutukset, kehittyminen ja riippuvuussuhteet. (Ilmonen ym. 2016, 132.)

Juvonen ym. (2014, 28) kuvailevat, että riskien pitäminen omalla vastuulla on tietoista ja usein tiedostamatonta. Esimerkiksi toistuvat ja mitättömät kiusanteot tai rikkoutumiset ovat monesti edullisinta ylläpitää organisaation vastuulla.

5.2.5 Riskin siirtäminen

Ilmonen ym. (2016, 133) kertovat, että siirtämisen keinoja toisen osapuolen kannettavaksi ovat rahoitusratkaisut, vakuudet ja sopimukset. Rahoitussopimuksissa on kyse siitä, että riskinhallintavälineinä käytetään erilaisia rahastoivia ratkaisuja ja niiden johdannaisia. (Ilmonen ym. 2016, 133.) Ilmonen ym. (2016, 135–137) jatkavat, että vakuuttaminen tarkoittaa taloudellisen riskin siirtämistä vakuutussopimuksella sopimusteitse vakuutettujen riskien toteutumisen varalta. Muu riskien siirtäminen tarkoittaa, että toiselle osapuolelle siirretään sopimusteitse kannettavaksi tai omistettavaksi riskialtis toiminta tai kohde esimerkiksi alihankintasopimuksella. Yleisin siirrettävä toiminto on jokin liiketoiminnan tukitoiminto, kuten ICT-palvelut. Riskiä voidaan siirtää myös vuokraamalla esimerkiksi organisaation toimitilat. Osa riskistä siirtyy vuokranantajan kannettavaksi.

Kun pohditaan jonkin toiminnon siirtämistä, vaihtoehtoja on harkittava ja analysoitava. Sopimuksiin on tutustuttava huolella, jotta väärinkäsityksiä ei kehittyisi. (Ilmonen ym. 2016, 139–140).

6 TUTKIMUKSEN TOTEUTTAMINEN JA TULOKSET

Tässä luvussa kuvataan toiminnallista osaa. Ensimmäisenä kuvataan tutkimuksen aikataulua, seuraavana tutkimusmenetelmää. Sen jälkeen kerrotaan ISO/IEC 27001 -taulukon laadinnasta sekä tulokset standardin vaatimuksista ja tietoturvallisuuden hallintatavoitteista ja -keinoista. Viimeisenä kuvataan riskiarviointitaulukkoa, sen laatimista ja tuloksia.

6.1 Tutkimuksen aikataulu

Tutkimusta aloitettiin suunnitella jo ennen joulua. Opinnäytetyön tavoitteeksi asetettiin, että se tulisi olla kokonaisuudessaan valmis ennen toukokuuta. Jotta toiminnallinen osa ehdittäisiin kirjoittaa valmiiksi ennen toukokuuta, haastattelujen aikakohdaksi on valittava maaliskuu. Ensimmäinen haastattelu pidettiin jo maaliskuun alussa 3.3.2021 liittyen standardin kysymyslistaan. Kysymyslistan läpikäyntiä jatkettiin 12.3.2021. Seuraavat palaverit pidettiin 25.3.2021 ja 31.3.2021 riskiarviointitaulukosta.

6.2 Tutkimusmenetelmä

Opinnäytetyö on kvalitatiivinen eli laadullista tutkimus. Kvalitatiivisessa tutkimuksessa tarkastellaan usein yksittäistä ilmiötä sekä tutustutaan aihealueen teoriaan ja aiempiin tutkimuksiin. Laadulliseen tutkimukseen on valittava pääkäsitteet sekä oivallettava niiden suhde lähikäsitteisiin ja itse tutkimukseen. Olennaista tutkimuksessa on osallistuvien henkilöiden mielipiteet ja näkökulmat. Tavoitteena on saada miellyttävä tulkinta tutkittavasta ilmiöstä. (Puusa & Juuti 2020, 75–82.)

Puolistrukturoitu haastattelu on soveltuvin aineistonkeruumenetelmä tähän tutkimukseen. Yrityksen nykyistä tilannetta selvitetään haastattelulla, johon valitaan vain ne henkilöt, jotka tietävät asioista paljon ja ovat kokeneita. Puolistrukturoidussa haastattelussa kysymykset ovat tarkkaan mietittyjä ja tarvittaessa esitetään täydentäviä kysymyksiä teemojen pohjalta. Kysymykset voidaan esittää erilaisessa järjestyksessä haastateltaville ja osa kysymyksistä voidaan tarvittaessa jättää pois. Haastattelussa ei ole

valmiita vastausvaihtoehtoja. (Saaranen-Kauppinen & Puusniekka 2006; Valli & Aarnos 2018, 24–25; Puusa & Juuti 2020, 84 & 111–112.) Haastattelut toteutettiin ryhmähaastatteluna ajan säästämiseksi ja moniäänisyyden takia. Puusa ja Juuti (2020, 115) kertovat, että ryhmähaastattelujen tavoitteena on saada haastateltavilta yhteinen mielipide (Puusa & Juuti 2020, 115). Haastattelut suoritettiin etänä Teams -sovelluksen välityksellä koronapandemian takia ja ne nauhoitettiin sovelluksen avulla. Aineisto hävitetään asianmukaisella tavalla. Haastateltavina olivat kohdeyrityksen liiketoimintajohtaja ja kaksi eri palvelun tuotepäällikköä.

Kvalitatiivisen tutkimuksen muotoja ovat haastattelun lisäksi havainnointi, aineistot, organisaation dokumentit ja kuvat. Tässä opinnäytetyössä keskitytään pääsääntöisesti haastatteluun, henkilökunnan mielipiteisiin ja osittain havainnointiin siten, että ne edistävät tarvittavien toimenpiteiden löytämistä yritykselle ja hyödynnetään organisaation dokumentteja edellisistä standardimenettelyistä ja -käytännöistä. (Järvenpää 2006, 13.)

6.3 ISO/IEC 27001 -taulukon laatiminen

ISO/IEC 27001 -standardissa on kaksi osaa, jotka ovat tietoturvallisuuden hallintajärjestelmän vaatimukset ja tietoturvallisuuden hallintatavoitteet ja -keinot (ISO/IEC 27001:fi 2017, 5; ISO/IEC 27002:fi 2017, 8). Ne sisältävät useita kohtia ja alakategorioita. Kaikista selkeintä oli tehdä Excel-taulukko. Ensimmäisenä Excel-taulukkoon kuvattiin standardin kohdat ja seuraavana vaadittavat dokumentit. Sen jälkeen taulukkoon lisättiin kysymyssarake. Kuvassa 13 on esimerkki taulukon rakenteesta, jolta se näyttää tässä vaiheessa.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset
A.5 Tietoturvapolitiikat	A.5.1 Johdon ohjaus tietoturvallisuutta koskevissa asioissa		Tarjota johdon ohjausta ja tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti.			
		A.5.1.1 Tietoturvapolitiikat		Tietoturvallisuudelle on määriteltävä joukko johdon hyväksymiä poliitikkoja, jotka julkaistaan henkilökunnan ja asiaankuuluvien organisaation ulkopuolisten osapuolten käyttöön ja joista tiedotetaan henkilökunnalle ja muille osapuolille.		Oletteko määritelleet johdon hyväksymät poliitikot tietoturvallisuudelle? Mitä nämä dokumentit ovat? Miten tietoturvapolitiikasta tiedotetaan muille? Onko se tarvittavien henkilöiden saatavissa? (Ks. Kohta 7.3 Tietoisuus)
		A.5.1.2 Tietoturvapolitiikkojen katselmointi		Tietoturvapolitiikat on katselmoitava suunnitelluin aikavälein tai kun merkittäviä muutoksia tapahtuu, jotta varmistetaan, että ne ovat edelleen soveltuvia, asianmukaisia ja vaikuttavia.		Tarkistetaanko tietoturvapolitiikat säännöllisesti? Miten tarkastukset toteutetaan? Kuinka usein? Ketkä sen suorittavat?

Kuva 13. Esimerkki taulukon laatimisesta keskeneräisenä

Excel-taulukkoon liitettiin seuraavana kolme saraketta, jotka ovat lähtötilanne, puutteet ja suositeltavat toimenpiteet tutkimuksen alakategorioiden selvittämiseksi. Kuvassa 14 on esimerkki taulukon rakenteesta, jolta se viimein näyttää.

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.5 Tietoturvapolitiikat	A.5.1 Johdon ohjaus tietoturvallisuutta koskevissa asioissa		Tarjota johdon ohjausta ja tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti.						
		A.5.1.1 Tietoturvapolitiikat		Tietoturvallisuudelle on määriteltävä joukko johdon hyväksymiä poliitikkoja, jotka julkaistaan henkilökunnan ja asiaankuuluvien organisaation ulkopuolisten osapuolten käyttöön ja joista tiedotetaan henkilökunnalle ja muille osapuolille.		Oletteko määritelleet johdon hyväksymät poliitikot tietoturvallisuudelle? Mitä nämä dokumentit ovat? Miten tietoturvapolitiikasta tiedotetaan muille? Onko se tarvittavien henkilöiden saatavissa? (Ks. Kohta 7.3 Tietoisuus)			
		A.5.1.2 Tietoturvapolitiikkojen katselmointi		Tietoturvapolitiikat on katselmoitava suunnitelluin aikavälein tai kun merkittäviä muutoksia tapahtuu, jotta varmistetaan, että ne ovat edelleen soveltuvia, asianmukaisia ja vaikuttavia.		Tarkistetaanko tietoturvapolitiikat säännöllisesti? Miten tarkastukset toteutetaan? Kuinka usein? Ketkä sen suorittavat?			

Kuva 14. Esimerkki taulukon laatimisesta valmiina

Laaditussa Excel-taulukossa ensimmäisellä välilehdellä on kuvattuna standardin vaatimukset ja toisessa välilehdessä on tietoturvallisuuden hallintatavoitteet ja -keinot, jotka ovat osa standardin vaatimusta, kohtaa 6.1.3. Jotta taulukoita olisi helpompi lukea, niiden rakenne on tehty samantyyliseksi. Ne ovat numeroitu ja ryhmitelty alakategorioihin samalla tavalla kuin standardissa. Standardin vaatimusten ensimmäinen

vaatimuskohta 4 ja viimeisin kohta on 10. Hallintatavoitteiden ja -keinojen ensimmäinen vaatimuskohta on A.5 ja viimeisin kohta on A.18. Kohdat on otettu suoraan standardista, ja niitä on osittain muokattu ja lyhennetty. Vaadittavat dokumentit -sarakkeessa on käytetty apuna Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 revision) -listaa (Advisera 2021). Suositeltavat dokumentit ovat laitettu sulkeisiin. Taulukon kaikista kohdista pois lukien hallintatavoitteet on laadittu kysymykset, jotka auttavat kohdeyrityksen lähtötilanteen selvittämisessä. Hallintatavoitteista ei ole kysymyksiä, sillä ne saavutetaan hallintakeinojen avulla.

Valmis Excel-taulukko lähetettiin haastateltaville noin viikkoa ennen haastattelua, jotta he ehtivät tutustua siihen. Kysymykset käytiin läpi haastatteluissa. Lähtötilannetta on verrattu standardin tavoitteisiin ja siitä on johdettu puutteet ja suositeltavat toimenpiteet. Excel-taulukko on kuvattuna tarkemmin liitteessä 1, jossa laajat kohdat on jaettu kahteen tai useampaan kuvaan. Taulukosta on peitetty lähtötilanne, puutteet ja suositeltavat toimenpiteet arkaluonteisen tiedon vuoksi.

6.4 ISO/IEC 27001 -taulukon tulokset

Organisaation toimintaympäristössä, kohdassa 4 (liite 1) kohdeyrityksen on päätettävä tietoturvallisuuden hallintajärjestelmän soveltamisala sekä tarkennettava organisaation toimintaympäristöä ja sidosryhmien tarpeita. Johtajuudessa, kohdassa 5 (liite 1) on päivitettävä tietoturvapolitiikka ja -vastuut sekä määritettävä ryhmä tai henkilö vastaamaan tietoturvallisuuden hallintajärjestelmästä. Suunnittelu, kohta 6 (liite 1) ei vastaa yrityksessä standardin vaatimuksia. Yrityksen on tarkennettava erityisesti tietoturvariskien käsittelyprosessia ja laadittava puuttuvia dokumentteja, kuten riskikriteerit ja soveltuvuuslausunto. Tukitoiminnot, kohta 7 (liite 1) eivät täytä standardin vaatimuksia ja yrityksen on tehtävä toimenpiteitä lähes kaikkiin alakohtiin 7.1–7.5. Kohdat 8 ja 9, toiminta ja suorituskyvyn arviointi (liite 1) eivät ole kunnossa. Yrityksen on esimerkiksi suoritettava säännöllisesti tietoturvariskien arvioinnit ja sisäiset auditoinnit sekä määritettävä, miten tietoturvallisuuden hallintajärjestelmää seurataan ja mitataan. Kohta 10, parantaminen (liite 1) ei vastaa yrityksessä täysin standardin vaatimuksia, sillä yrityksen on tarkennettava poikkeamien hallintaan ja korjaaviin

toimenpiteisiin liittyvää prosessia sekä parannettava jatkuvasti tietoturvallisuuden hallintajärjestelmää, kun se on laadittu.

Tietoturvapolitiikat, kohtaan A.5 (liite 1) on päivitettävä tietoturvapolitiikka ja tietosuojapolitiikka. Tietoturvallisuuden organisointi, kohdassa A.6 (liite 1) on päivitettävä organisaation roolit ja laadittava etätyötä ja mobiililaitteita koskevat politiikat. Yritys ei täytä kaikkia vaatimuksia henkilöstöturvallisuudesta ja suojattavan omaisuuden hallinnasta, kohtia A.7 ja A.8 (liite 1). Kohdassa A.9 ja A.10, pääsynhallinnassa ja salauksessa (liite 1) yrityksen on täsmennettävä ja dokumentoitava puuttuvia ohjeita, politiikkoja ja käytäntöjä. Yritys on huolehtinut hyvin fyysisestä turvallisuudesta ja ympäristön turvallisuudesta, kohdasta A.11 (liite). Yrityksen on päivitettävä muutamaa politiikkaa ja harkittava, ottavatko he käyttöön myös muita standardin ohjeistuksia, kuten fyysisissä turva-alueissa. Kohta A.12 ja A.13, käyttöturvallisuuden hallintakeinot ja viestintäturvallisuus toteutuvat pääosin yrityksessä. Yrityksen on täsmennettävä tiedonsiirto- ja varmuuskopiointipolitiikkaa. Järjestelmien hankkiminen, kehittäminen ja ylläpito sekä suhteet toimittajiin, kohdissa A.14 ja A.15 (liite 1) yrityksen on tehtävä pieniä muutoksia, kuten tarkennettava muutoksenhallintamenettelyä ja harkittava standardissa kuvattujen ehtojen sisällyttämistä toimittajasopimuksiin. Kohtaa A.16, tietoturvahäiriöiden hallintaa (liite 1) koskevat menettelyt ovat kuvattuna yrityksessä ainoastaan ylätasolla, ja yrityksen on laadittava tarkemmin siihen liittyviä prosesseja ja menettelyohjeita. Yritys ei täytä kokonaan kohdan A.17, liiketoiminnan jatkuvuuden hallintaan (liite 1) liittyviä kohtia. Kohdassa A.18, vaatimustenmukaisuudessa (liite 1) yritys huolehtii tietoturvallisuuden riippumattomasta katselmoinnista, mutta yrityksen olisi tarkastettava säännöllisesti tietojärjestelmien tekniset vaatimukset ja otettava käyttöön salaustekniikan hallintamekanismit.

Tuloksena saatiin, että kohdeyrityksellä on laadittuna muutama standardin vaatimukset täyttävä politiikka. Yrityksellä on enemmän kehitettävää standardin hallintajärjestelmää koskevissa vaatimuksissa, kohdissa 4–10 kuin hallintatavoitteissa ja -keinoissa, kohdissa A.5–A.18. Heillä oli useasta kohdasta käsitys, millä tavalla asia pitää tehdä. He eivät ole vain dokumentoineet niitä standardin edellyttämällä tavalla. Organisaation on tarkennettava ja päivitettävä osaa laadituista ohjeistuksia, jotta henkilöstö tietäisi yksityiskohtaisemmin, miten tilanteessa kuuluisi toimia. Heidän on mietittävä

tarkkaan tietoturvallisuuden hallintajärjestelmän soveltamisalasta ja päätettävä, mihin he rakentavat hallintajärjestelmän.

6.5 Riskiarviointitaulukon laatiminen

Riskien kartoittamisessa ja tunnistamisessa on hyödynnetty lähdekirjallisuutta, ISO/IEC 27001 -standardia, haastatteluja ja aiempaa kohdeyrityksen laatimaa riskiarviointitaulukkoa. Riskiarviointitaulukossa on käytetty kohdeyrityksen laatimaa pohjaa.

Havaitut riskit ovat kuvattuna hyvin yleisellä tasolla ja niitä tunnistettiin yhteensä 45. Jokaiselle riskille kirjattiin syyt ja tekijät riskin taustalla, toimenpide-ehdotukset ja riskiluokat (arvot 1–7), jotka ovat

1. strateginen riski
2. operatiivinen riski
3. taloudellinen riski
4. vahinkoriski
5. vastuuriski
6. imagoriski
7. ympäristöriski.

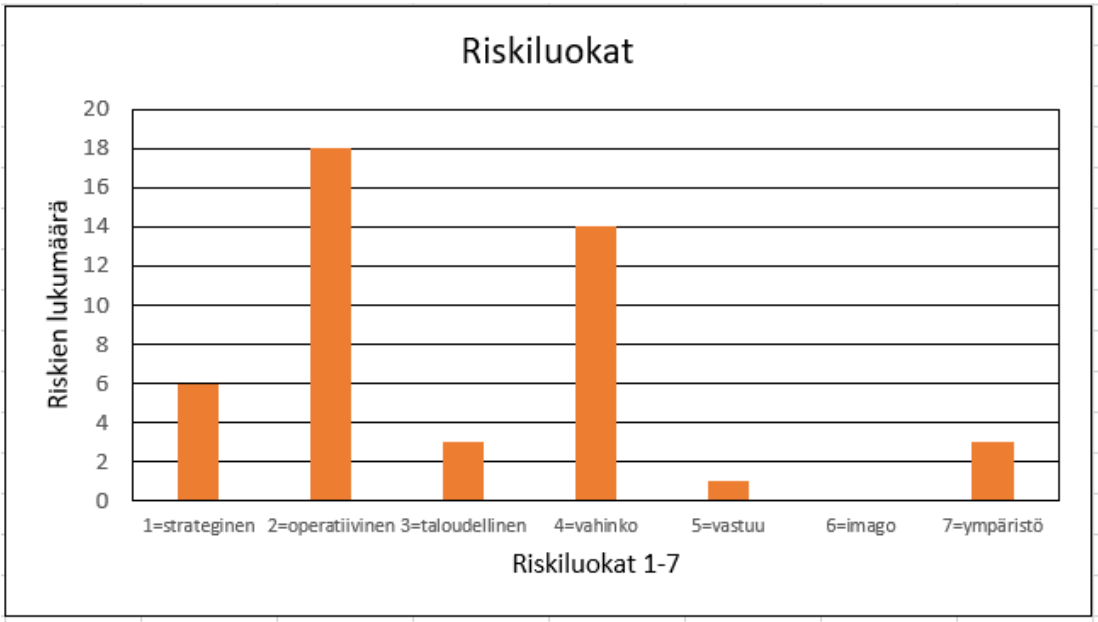
Seuraavana riskejä analysoitiin ja arvioitiin niiden todennäköisyys ja vaikuttavuus (arvot 1–4). Asteikkona käytettiin yleisiä todennäköisyyden ja vaikuttavuuden arvoja. Viimeisenä pohdittiin, onko riskillä välitöntä mahdollisuutta, kun toimenpide-ehdotus toteutetaan.

6.6 Riskiarviointitaulukon tulokset

Osa tutkimuksen tuloksista on salassa pidettäviä, ja siitä johtuen riskiarviointitaulukkoa ei ole liitetty kokonaan työhön. Tuloksia havainnollistetaan erilaisilla kuvaajilla ja osaa kuvataan sanallisesti tarkemmin.

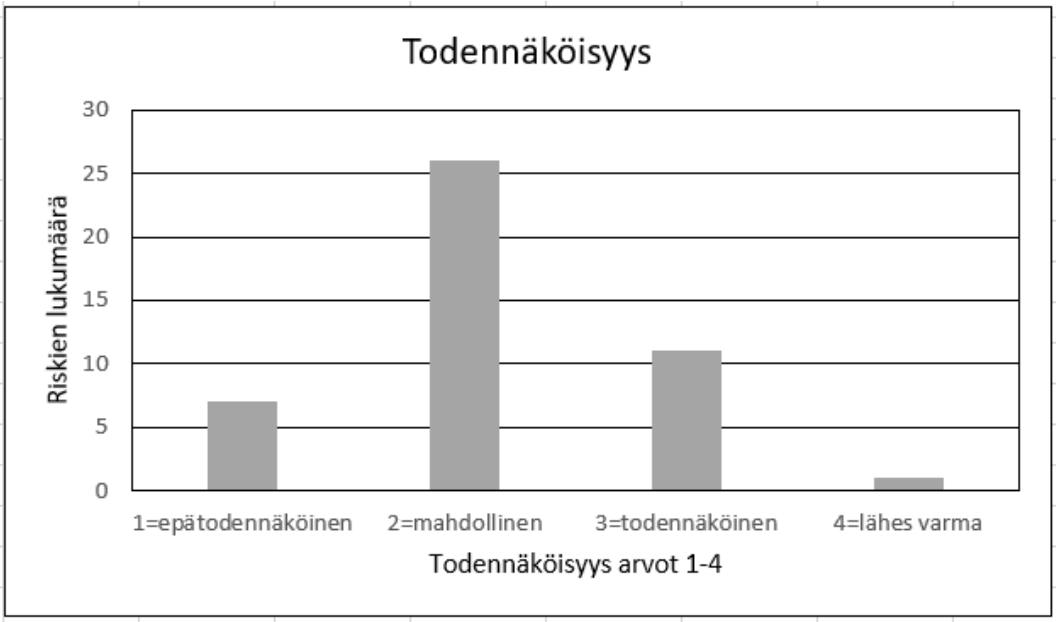
Kuva 15 havainnollistaa, kuinka tunnistetut riskit ovat jakautuneet eri riskiluokkiin.

Lähes puolet tunnistetuista riskeistä ovat operatiivisia riskejä ja toiseksi eniten on vahinkoriskejä. Imagoriskejä ei havaittu ollenkaan ja vastuuriskejä ainoastaan yksi.

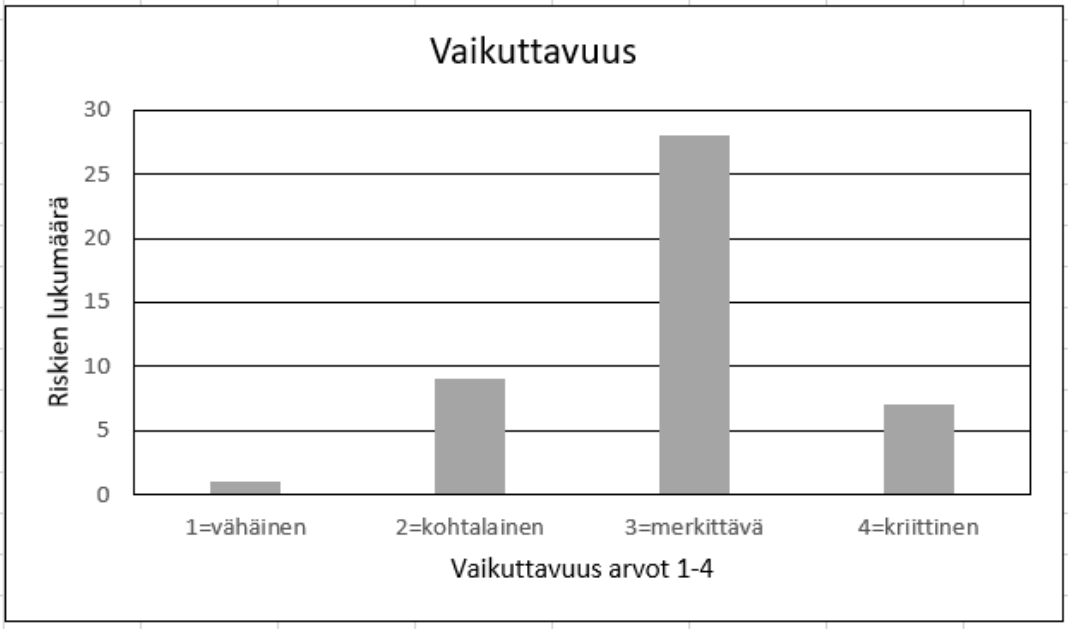


Kuva 15. Taulukko riskiluokkien jakautumisesta

Kuvat 16 ja 17 kertovat, miten tunnistettujen riskien todennäköisyydet ja vaikuttavuudet ovat jakautuneet. Todennäköisyystaulukossa suurin osa riskeistä on mahdollisia ja vähiten on lähes varmoja riskejä. Vaikuttavuustaulukossa yli puolet ovat merkittäviä riskejä ja noin viidesosa on kohtalaisia.



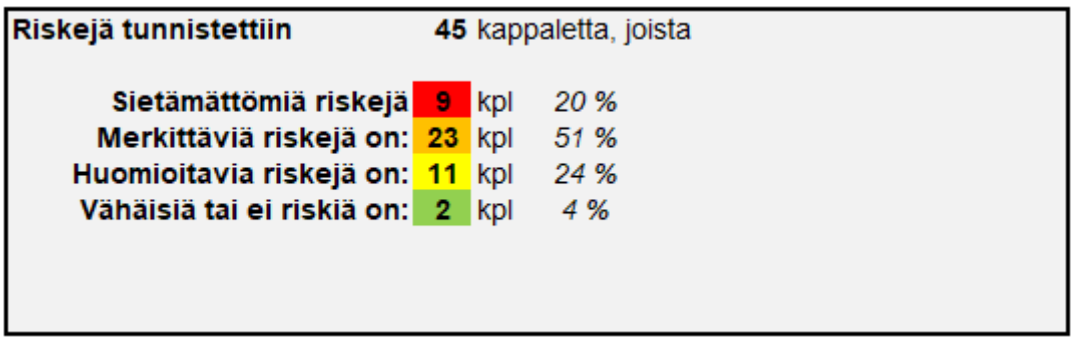
Kuva 16. Taulukko todennäköisyyden jakautumisesta



Kuva 17. Taulukko vaikuttavuuden jakautumisesta

Kuva 18 selventää, miten riskien merkitys jakaantuu. Sietämättömiä riskejä on yhteensä yhdeksän ja yli puolet ovat merkittäviä riskejä, joita on 23. Vähiten, yhteensä kaksi riskeistä on vähäisiä tai ei ole riskiä. Välitön mahdollisuus on yhteensä kolmellatoista riskillä, kun toimenpide-ehdotus suoritetaan.

Sietämättömät riskit ja niiden toimenpide-ehdotukset riskin pienentämiseksi tai poistamiseksi ovat kerrottuna kuvassa 19. Muita riskejä ei kuvata työssä, jotta säilytetään tutkimuksen eettisyys ja vältetään liiallinen kohdeyrityksen riskien paljastaminen.



Kuva 18. Riskien merkityksen arviointi

SIETÄMÄTÖN RISKI	TOIMENPIDE-EHDOTUS
Huono organisointi ja hallinta	Hallintakeinojen, toiminnan linjauksien ja resursoinnin kehittäminen, säännölliset koulutukset
Tietojärjestelmien kehittyminen	Osaamisesta huolehtiminen, oltava tietoinen uudesta teknologiasta
Dokumenttien, menettelyjen ja toiminta-ohjeiden puuttuminen ja niiden epäsäännöllinen päivittäminen ja tarkistaminen	Laadittava puuttuvat politiikat, suunniteltava käytäntö niiden säännölliseen tarkistamiseen ja päivittämiseen
Dokumenttien huono saatavuus, eheys tai luottamuksellisuus	Tietojen oleminen vain yhdessä paikassa, dokumenttien järjestelmällinen tallentaminen, pääsyoikeuksien rajoittaminen
Etätyö	Laadittava politiikka ja säännöt, järjestettävä koulutusta
Mobiililaitteet ja omat laitteet	Laadittava politiikat, järjestettävä koulutusta
Pilvipalveluiden käyttö	Dokumentaatio, opastus, tietoisuuden lisääminen sen vaaroista
Tietojen kalastelu ja manipulointi	Jatkuva koulutus
Puuttuva tai hyväksymätön jatkuvuus- ja toipumissuunnitelma	Laadittava jatkuvuus- ja toipumissuunnitelmat, tietoisuuden kehittäminen, suunniteltava tehokkaat viestintämallit ja -keinot, hyödynnettävä kolmannen osapuolen asiantuntijalausuntoja

Kuva 19. Sietämättömät riskit

7 POHDINTA

Tutkimuksessa päätavoitteena oli saada selville toimenpiteet standardin saamiseksi, ja alakategoriat olivat yrityksen nykytilanteen kartoittaminen, puutteiden tunnistaminen, toimenpiteiden selvittäminen puutteiden korjaamiseksi sekä tietoturvariskien havaitseminen. Standardin vaatimukset ja tietoturvallisuuden hallintatavoitteet ja -keinot alkoivat vähitellen muodostua Excel-taulukoksi, johon lisättiin sarakkeet lähtötilanteelle, puutteille ja suositeltaville toimenpiteille. Toisena dokumenttina laadittiin riskiarviointitaulukko havaituista riskeistä, jotka analysoitiin ja arviointiin riskiarviointiprosessin mukaan.

Opinnäytetyön tutkija on tyytyväinen laadittuihin dokumentteihin, ja ne vastaavat hyvin tutkimuskysymykseen ja alaongelmiin. Dokumentit ovat hyvä työväline ISO/IEC 27001 -sertifikaatin hankkimisessa. Excel-taulukossa on kuvattuna suositeltavat toimenpiteet -sarakkeessa, millä keinoilla voi täyttää standardin kohdan sekä mitä politiikkojen ja ohjeiden on sisällettävä, jotta se vastaa standardia. Siinä ei kuvailla sanatarkasti, millä tyylillä se on suoritettava. Se ei ole standardin tarkoitus, sillä jokainen organisaatio suorittaa kohdat omalla tyylillään. Ei ole olemassa kahta samanlaista tietoturvallisuuden hallintajärjestelmää.

Tutkija oli innoissaan aiheesta ja siitä, että työ saatiin tehdä tilaajalle. Työtä oli mielekästä tehdä, kun oppi uutta sertifioinnista sekä pääsi tutustumaan tarkasti standardiin ja ennestään tuntemattomaan organisaatioon, tutkija kuvailee. Tutkija yllättyi siitä, miten paljon aikaa kului standardiin tutustumiseen ja oli kuvitellut standardin huomattavasti yksinkertaisemmaksi. Se vaati hurjasti aikaa, että sai avattua kaikki kohdat standardista ja kuvan siitä, mitä niillä tarkoitetaan. Haasteena oli löytää tieteellisiä lähteitä. Esimerkiksi moni sertifiointilaitos tarjoaa materiaaleja riskienhallinnasta, sertifiointiprosessista sekä standardista. Kaikista aikaa vievin ja kiinnostavin vaihe oli kirjoittaa Excel-taulukkoa. Yhteistyö sujui kohdeyrityksen kanssa erittäin hyvin. Haastateltavat tekivät hyvin nopeasti tilaa kalentereihin, ja toimeksiantajan edustaja auttoi tutkimuksen hankalissa kohdissa. Tutkija sai koko prosessista vahvan ISO/IEC 27001 -standardin osaamisen ja Excel-taulukon, jota on mahdollista käyttää apuna poistamalla

kohdeyrityksen tiedot, jos tutkija on tulevaisuudessa mukana toisen organisaation ISO/IEC 27001 -standardin sertifioinnissa.

Opinnäytetyö oli laadullinen eli kvalitatiivinen tutkimus ja aineistonkeruumenetelmänä käytettiin puolistrukturoitua haastattelua, ja haastattelut suoritettiin ryhmähaastatteluna. Tämä keino oli soveltuvin menetelmä, sillä haastattelut saatiin suoritettua kerralla kuntoon, eikä tarvinnut tehdä uusintakierrosta tarkistaakseen jotain kohtaa toiselta henkilöltä. Ryhmähaastatteluissa saatiin aikaiseksi enemmän keskustelua ja mielipiteiden jakamista. Tutkija pystyi esittämään haastattelujen aikana täydentäviä kysymyksiä ja avata epäselviä kohtia.

Tutkija kokee, että opinnäytetyö on onnistunut. Tutkimuksessa vastattiin tutkimuskysymykseen ja asetetussa aikataulussa pysyttiin. Nyt kohdeyrityksellä on selkeä listaus siitä, mitä organisaatiossa on kehitettävä ja tehtävä sertifikaatin saamiseksi. Samalla yritys saa yleiskuvan siitä, mitä kaikkea standardi vaatii.

7.1 Tutkimuksen luotettavuus ja eettisyys

Tutkimusta voidaan pitää luotettavana, koska tutkimustulokset kuvastavat tutkittavaa ilmiötä. Tutkimus aloitettiin huolellisella suunnittelulla ja aihe oli tiedossa alusta saakka. Teoreettisen viitekehyksen rakentaminen ja siihen tutustuminen helpottuivat, kun aihe rajattiin tarkasti. Taulukkoon listattiin tutkimuskysymysten määrittämisen jälkeen sarakkeet lähtötilanteelle, puutteille ja suositeltaville toimenpiteille, jotta tutkimuskysymykseen ja alaongelmiin saataisiin selvyys. Haastattelun kohderyhmä ja koko oli tiedossa alusta alkaen, ja heillä on asiantunteva näkemys organisaation tietoturvasta.

Laadullisessa tutkimuksessa luotettavuudesta kertoo tutkija ja tutkijan tekemät valinnat, ratkaisut ja teot. Luotettavuutta on arvioitava jatkuvasti tutkimuksen aikana, kuten teoreettisessa viitekehyksessä, analyysitavassa, tulkinnassa ja johtopäätöksissä sekä kiinnitettävä huomiota puolueettomuusnäkökantaan. Analyysissä voidaan tarkastella tutkijan iän, sukupuolen, uskomusten, arvojen tai poliittisten asenteiden merkitystä tutkimuksessa suoritettuun tulkintaan. Tutkijan omakohtainen tieto organisaatiosta ja sen

toiminnasta voi aiheuttaa ennakkokäsityksiä. (Vilkka 2015, 196–197; Tuomi & Sarajärvi 2018, 160; Puusa & Juuti 2020, 181.)

Haastatteluun osallistuivat kohdeyrityksen liiketoimintajohtaja ja kahden eri palvelun tuotepäälliköt. Saadut vastaukset ovat useamman henkilön mielipiteitä ja niistä voi tehdä luotettavia johtopäätöksiä. Jos haastettuluun eivät olisi osallistuneet kaikki tietoturvasta vastaavat henkilöt, tutkimusta ei voitaisi pitää yhtä luotettavana. Tutkija ei tuntenut organisaatiota tai haastateltavia ennen tutkimusprojektin aloittamista ja tutkimuksessa on hyödynnetty luotettavia ja erityyppisiä lähteitä, kuten videoita, artikkeleita ja standardeja. Haastattelut nauhoitettiin, jotta keskustelusta tulisi sujuvampaa ja tutkijalla ei kuluisi aikaa asioiden kirjaamiseen. Nauhoituksella turvattiin se, että haastatteluun oli mahdollista palata uudelleen.

Haastattelun hyötynä on se, että haastattelun aikana voi kysyä täydentäviä kysymyksiä ja, jos ei ole käsittänyt jotakin kohtaa. Kasvotusten suoritettavassa haastattelussa olisi ollut mahdollisuus seurata ympäristöä sekä tutkia haastateltavien eleitä ja ilmeitä. Ryhmähaastattelussa tuloksia voi vääristää se, että haastateltavat eivät aina uskalla kertoa omaa mielipidettä asiasta ja helposti tyytyvät kollegan näkökantaan. Haastateltavat kyseenalaistivat ryhmähaastattelusta huolimatta kollegoiden mielipiteitä useaan otteeseen. Asioista saatiin aina yhteinen käsitys.

Oikean tuloksen tai tieteellisen teorian erottaminen ei-tieteellisestä ja väärästä tuloksesta on vaikeaa. Tieteen formaaliset kriteerit voivat toteutua helposti, kun taas sisältö voi olla yksittäisen tarkkuushavainnon tai henkilön nojassa. (Enqvist 2017, 24–34.) Luotettavuutta kuvastaa myös se, että teoriaan ei ole vaikuttanut satunnaiset tai epäolennaiset tekijät. Tutkijan onkin osoitettava taito tarkastella tutkittavaa ilmiötä yleisellä tasolla ja osattava yhdistää useita havaintoja, eli yleistää tulkinta. Tutkimuksen voidaan sanoa olevan pätevä, kun tutkimustulokset ovat yhteneviä tutkimustavoitteiden ja -kohteen kanssa (Vilkka 2015, 195–196.)

Tutkimuksen eettisyyden kannalta haastateltavien anonymiteetti säilytetään ja yrityksestä ei kerrota tarkkoja tunnistetietoja. Tutkija on kirjoittanut salassapitosopimuksen. Jaetut materiaalit pidetään salassa ja tallenteet ovat tutkijan hallussa. Materiaalit ja

tallenteet hävitetään asianmukaisesti. Salassa pidetyt asiat ovat olleet vain tutkijan käytössä lukitun tietokoneen takana.

7.2 Jatkokehitys

Tässä tutkimuksessa laaditut dokumentit toimivat hyvänä tukena ja pohjana ISO 27001 -sertifikaatin hankkimiselle. Jotta sertifikaatti saadaan, on vielä uurastettava. Toimeksiantaja voi harkita halutessaan eri yrityksiä, jotka auttavat sertifikaatin hankinnassa ja standardin vaatimusten soveltamisessa. Se voi tulla kalliiksi ja maksaa kohdeyritykselle useita tuhansia. Hyötynä on se, että se vähentää väärinkäsityksiä ja ei aiheuta haasteita standardin soveltamisessa.

ISO 27001 Global Report on kuvannut aika-arviointeja, jossa keskimääräinen aika sertifikaatin saamiseksi on 6–12 kuukautta (IT Governance 2018, 10). Kohdeyrityksellä vierähtää todennäköisesti kaksi vuotta, jos tietoturvallisuuden hallintajärjestelmää kehitetään omien töiden ohessa. Katselmoinnit, auditoinnit ja muutosten korjaamiset takaavat, että on aherrettava tietoturvallisuuden hallintajärjestelmän ylläpidon ja ISO/IEC 27001 -sertifikaatin uusimisen eteen.

Kohdeyritys voi käyttää taulukkoa apuna edistymisen seuraamisena ja lisätä tarvittaessa sarakkeita, joissa kuvaillaan esimerkiksi lisähuomiot, tarvitaanko hallintakeinoa organisaatiossa ja onko hallintakeino tai -tavoite toteutettu.

LÄHTEET

Advisera. 2021. Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 revision). Viitattu 13.4.2021. https://advisera.com/27001academy/knowledge-base/list-of-mandatory-documents-required-by-iso-27001-2013-revision/

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Baker, A. 2017. Why ISO 27001is 'the' standard for information security. 26.7.2017. Viitattu 13.4.2021. https://www.itgovernance.eu/blog/en/why-iso-27001-is-the-standard-for-information-security

FINAS www-sivut. 2021. Sertifiointiorganisaatiot. Viitattu 22.2.2021. https://www.finas.fi/Sivut/default.aspx

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo

Hänninen, A. 2019. Varman päälle. Presiis-lehti 1, 16–19. Viitattu 22.2.2021. https://sfs.fi/

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2016. Johda riskejä: Käytännön opas yrityksen riskienhallintaan. Toinen laitos. Helsinki: Finva.

ISO/IEC 17021:fi. Vaatimustenmukaisuudenarviointi. Vaatimukset johtamisjärjestelmiä auditoiville ja sertifioiville elimille. Osa 1: Vaatimukset. 2015. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS. Viitattu 2.2.2021. http://www.sfs.fi

ISO/IEC 27000:fi. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. 2020. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS. Viitattu 13.1.2021. http://www.sfs.fi

ISO/IEC 27001:fi. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. 2017. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS. Viitattu 13.1.2021. http://www.sfs.fi

ISO/IEC 27002:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS. Viitattu 22.1.2021. http://www.sfs.fi

ISO/IEC 27003:fi. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Ohjeistusta. 2017. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS. Viitattu 13.1.2021. http://www.sfs.fi

ISO/IEC 31000:fi. Riskienhallinta. Ohjeet. 2018. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS. Viitattu 1.2.2021. http://www.sfs.fi

IT Governance. 2018. ISO 27001 Global Report. Viitattu 13.4.2021. https://www.itgovernance.asia/iso27001-global-report-2018

IT Governance. 2021. ISO 27001: The facts. Viitattu 14.4.2021. https://www.itgovernance.co.uk/iso27001-facts

Järvenpää, E. 2006. Laadullinen tutkimus. SoberIT jatko-opintoseminaarin materiaali, Teknillinen korkeakoulu. Viitattu 11.1.2021. http://www.cs.tut.fi/~ihtesem/k2007/materiaali/luento4.pdf

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala, T. 2014. Yrityksen riskienhallinta. Helsinki: Finanssi- ja vakuutuskustannus Oy FINVA.

Kangas, A. 2017. VM 22/2017 Ohje riskienhallintaan Riskiarviointityökalu – käyttö- ja täyttöohje. Viitattu 1.2.2021. https://vm.fi/documents/10623/1898625/Riskiarviointi+ohje/fe847307-0fc9-4389-bc0c-f003a98c150f

Klaus, N. 2017. Why certify and what is ISO 27001?. 30.5.2017. Viitattu 13.4.2021. https://www.nixu.com/blog/why-certify-and-what-iso-27001

Kohdeyrityksen nettisivut. 2021. Viitattu 12.1.2021.

Krypsys. 2021. What is ISO 27001 and why is it so important for organizations?. Viitattu 13.4.2021. https://www.krypsys.com/iso27001/iso-27001-important-organisations/

Lecklin, O. 2006. Laatu yrityksen menestystekijänä. 5. uud. p. Helsinki: Talentum.

Menon Economics. 2018. The Influence of Standards on the Nordic Economics. Menon-Publication. Yhteistyössä Nordic Innovation & Oxford Research. Oslo Menon Economics. Viitattu 13.4.2021. https://sfs.fi/standardeista/standardien-hyodyt/tutkittua/

Pro Pilvipalvelut. 2019. Standardit. Viitattu 24.1.2021. https://www.youtube.com/watch?v=YXtu64qReWo&feature=emb_logo

Pro Pilvipalvelut. 2021. Tietoturvan hallinta ja johtaminen ehkäisevät turvallisuusuhkia. Viitattu 13.4.2021. https://www.tietoturva.pro/iso-iec-27001

Puusa, A., & Juuti, P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Gaudeamus.

Raevaara, T., Enqvist, K., Häkkinen, J., Kotro, A., Lauerma, H., Lindeman, M., Linja-Aho, V., Järvinen, K., Nevala, H., Nystén, A., Myllykangas, M. & Puustinen, R. 2017. Voiko se olla totta?: Skeptisiä näkökulmia nykymenoon. Helsinki: Tähtitieteellinen yhdistys Ursa ry.

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Verkkojulkaisu. Tampere: Yhteiskuntatieteellinen tietoarkisto Viitattu 11.1.2021. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L1_2_2.html

Suomen standardisoimisliitto SFS ry. 2021. Mitä standardi tarkoittaa?. Viitattu 3.3.2021. https://sfs.fi/

Suominen, A. 2003. Riskienhallinta. 3. uud. p. Helsinki: WSOY

Traficom. 2019. Luottamuksen lähteillä. Näkökulmia tietoturvanstandardointiin ja sertifiointiin. Traficomin julkaisuja 31/2019. Helsinki: Traficom. Viitattu 13.4.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

Traficom. 2021. Tietoturvan vuosi 2020. Kyberturvallisuuden turvallisuuskeskus. Traficomin julkaisuja 13/2021. Helsinki: Traficom. Viitattu 13.4.2021. https://www.traficom.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Kustannusosakeyhtiö Tammi.

Valli, R. & Aarnos, E. 2018. Ikkunoita tutkimusmetodeihin: 1, Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. 5., uudistettu painos. Jyväskylä: PS-kustannus.

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Helsinki: Valtionvarainministeriö. Vahti 3/2007. Viitattu 8.2.2021. https://vm.fi/julkaisut/vahti

Vilkka, H. 2015. Tutki ja kehitä. 4. uud. p. Jyväskylä: PS-kustannus.

Haastattelut:

Päällikkö. Kohdeyritys. Teams -haastattelut 14.12.2020 ja 27.1.2021. Haastattelijana Karolina Yli-Hietanen. Aiheena opinnäytetyön alustaminen ja seuranta. Tallenteet ovat tekijän hallussa.

Päällikkö. Kohdeyritys. Teams -haastattelut 17.2.2021 ja 10.2.2021. Haastattelijana Karolina Yli-Hietanen. Aiheena toiminnallisen osuuden toteuttaminen. Tallenteet ovat tekijän hallussa.

Liiketoimintajohtaja, tuotepäällikkö 1 & tuotepäällikkö 2. Kohdeyritys. Teams -haastattelut 3.3.2021 ja 12.3.2021. Haastattelijana Karolina Yli-Hietanen. Aiheena ISO/IEC 27001 -standardin kysymyslistan läpikäyminen. Tallenteet ovat tekijän hallussa.

Liiketoimintajohtaja, tuotepäällikkö 1 & tuotepäällikkö 2. Kohdeyritys. Teams -haastattelut 25.3.2021 ja 31.3.2021. Haastattelijana Karolina Yli-Hietanen. Aiheena riskiarviointitaulukon läpikäynti ja täydentäminen. Tallenteet ovat tekijän hallussa.

LIITE 1

ISO/IEC 27001 -taulukko

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
4. Organisaation toimintaympäristö	4.1 Organisaation ja sen toimintaympäristön ymmärtäminen		Organisaation on määritettävä ulkoiset ja sisäiset asiat, jotka ovat olennaisia organisaation tarkoituksen kannalta ja jotka vaikuttavat sen kykyyn saavuttaa tietoturvallisuuden hallintajärjestelmältä halutut tulokset.	Soveltamisala	Oletteko määritelleet ulkoiset ja sisäiset toimintaympäristöt, jotka vaikuttavat organisaation suorituskykyyn tai ovat olennaisia organisaation tarkoituksen kannalta? Missä määrittely on? Mitkä nämä ulkoiset ja sisäiset toimintaympäristöt ovat?			
	4.2 Sidosryhmien tarpeiden ja odotusten ymmärtäminen		Määrittävä tietoturvan kannalta olennaiset sidosryhmät ja niiden asettamat tietoturvavaatimukset.		Oletteko määrittäneet sidosryhmät ja niiden asettamat tietoturvavaatimukset? Missä määrittely on? Mitkä nämä ulkoiset ja sisäiset sidosryhmät ovat?			
	4.3 Tietoturvallisuuden hallintajärjestelmän soveltamisalan määrittäminen		Päätettävä tietoturvallisuuden hallintajärjestelmän rajaukset ja soveltamisala. Otettava huomioon kohdat 4.1, 4.2 sekä muut toimintojen rajapinnat ja riippuvuudet.		Oletteko päättäneet hallintajärjestelmän rajaukset ja soveltamisalan? Huomioidaanko siinä kohdat 4.1, 4.2 ja muut rajapinnat? Millainen tämä rajaus on?			
	4.4 Tietoturvallisuuden hallintajärjestelmä		Luotava, toteutettava, ylläpidettävä ja parannettava tietoturvallisuuden hallintajärjestelmä standardin mukaisesti.		Onko teillä käytössä jonkinlainen tietoturvallisuuden hallintajärjestelmä?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
5. Johtajuus	5.1 Johtajuus ja sitoutuminen		Ylimmän johdon on osoitettava johtajuus ja sitoutuminen tietoturvallisuuden hallintajärjestelmään: - varmistamalla tietoturvapolitiikan laatiminen, tietoturvatavoitteiden asettaminen ja niiden yhdenmukaisuus organisaation strategian kanssa - varmistamalla hallinjärjestelmän vaatimusten yhdistäminen prosesseihin - varmistamalla hallintajärjestelmää varten riittävät resurssit (taloudelliset resurssit, henkilöstö, toimitilat ja tekninen infrastruktuuri) - viestimällä hallintajärjestelmän vaatimusten noudattamisen tärkeydestä ja hallinnan tarpeesta - varmistamalla, että hallintajärjestelmä saavuttaa halutut tulokset tukemalla prosessien toteuttamista ja katselmoimalla raportteja hallintajärjestelmän tilasta ja vaikuttavuudesta - ohjaamalla ja tukemalla organisaatiossa niitä henkilöitä, jotka edistävät tietoturvallisuutta - arvioimalla resurssitarpeet ja asettamalla tavoitteet jatkuvalle parantamiselle, edistämällä hallintajärjestelmän jatkuvaa parantamista - tukemalla muuta johtoa heidän vastuualueillaan.		Oletteko määritelleet jonkin ryhmän tai henkilön, joka on vastuussa tietoturvallisuuden hallintajärjestelmästä ja ohjaa sitä? Sitoutuvatko he tietoturvallisuuden hallintajärjestelmään? Miten sitoutuminen osoitetaan?			
	5.2 Tietoturvapolitiikka		Ylimmän johdon on laadittava tietoturvapolitiikka, joka - soveltuu organisaation toiminta-ajatukseen - sisältää tietoturvatavoitteet (yhtenäinen kohdan 6.2 kanssa) - sisältää sitoutumisen vaatimusten täyttämiseen ja hallintajärjestelmän jatkuvaan parantamiseen. Politiikan pitää olla dokumentoitu, koko organisaation tiedossa ja tarvittaessa sidosryhmien saatavilla.	Tietoturvapolitiikka ja tarkoitus	Oletteko laatineet tietoturvapolitiikan? Täyttääkö se vaatimukset? Mistä se löytyy? Onko politiikka dokumentoitu ja kaikkien saatavilla?			
	5.3 Organisaation roolit, vastuut ja valtuudet		Ylimmän johdon on varmistettava, että tietoturvan kannalta tärkeiden roolien vastuut ja valtuudet ovat määriteltynä ja että niistä viestitään. Henkilöiden on varmistettava, että hallintajärjestelmä on standardin vaatimusten mukainen ja heidän on raportoitava ylimmälle johdolle hallintajärjestelmän suorituskyvystä.		Ovatko tietoturvan kannalta tärkeiden roolien vastuut ja valtuudet määriteltynä? Mitkä ne ovat? Ovatko ne muiden tiedossa? Miten he raportoivat järjestelmän suorituskyvystä?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
6. Suunnittelu	6.1 Riskien ja mahdollisuuksien käsittely							
		6.1.1 Yleistä	Otettava huomioon kohtien 4.1 ja 4.2 asiat ja vaatimukset sekä määritettävä riskit ja mahdollisuudet, joiden käsittelemisen jälkeen voidaan - varmistaa, että hallintajärjestelmä voi saavuttaa halutut tulokset - estää tai vähentää ei-toivottuja vaikutuksia - saada aikaan jatkuvaa parantamista - suunniteltava riskeihin ja mahdollisuuksiin kohdistuvia toimenpiteitä, kuinka ne yhdistetään prosesseihin ja toteutetaan sekä kuinka niiden vaikuttavuus arvioidaan.		Onko riskeihin ja mahdollisuuksiin suunniteltu toimenpiteitä niiden yhdistämiseksi prosesseihin sekä niiden toteuttamiseksi ja arvioimiseksi? Millaisia?			
		6.1.2 Tietoturvariskien arviointi	Määriteltävä ja toteutettava tietoturvariskien arviointiprosessi, jossa - laaditaan ja ylläpidetään riskikriteerejä (hyväksymiskriteerit ja arvioinnin suorittamiskriteerit) - varmistetaan, että toistuvat riskiarvioinnit tuottavat yhdenmukaisia, päteviä ja verrattavissa olevia tuloksia - tunnistetaan tietoturvariskejä toteuttaen arviointiprosessi, jolla havaitaan hallintajärjestelmän soveltamisalaan kuuluvan tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit sekä tunnistetaan riskien omistajat - analysoidaan tietoturvariskit arvioimalla tunnistettujen riskien mahdolliset seuraukset ja realistinen todennäköisyys sekä määrittämällä riskin taso - vertaamalla riskianalyysin tuloksia alussa laadittuihin riskikriteereihin ja priorisoimalla analysoidut riskit. Arviointiprosessista on säilytettävä dokumentoitua tietoa.	Riskien arviointi ja menetelmät	Onko teillä käytössä tietyt riskikriteerit? Mitkä ne ovat? Miten osoitatte, että riskiarvioinneista saadaan yhdenmukaisia, päteviä ja verrattavissa olevia tuloksia? Määritteletkö riskien omistajat? Säilytetäänkö arviointiprosessista dokumentteja? Missä?			

	Katso erillinen taulukko toiselta välilehdeltä (ovat suoraan ISO/IEC 27002:2017 ja ovat pakollisia tässä kohdassa, jotta ISO/IEC 27001 vaatimukset täyttyvät)	6.1.3 Tietoturvariskien käsittely	Määriteltävä ja toteutettava tietoturvariskien käsittelyprosessi, jossa - valitaan soveltuvat riskien käsittelyvaihtoehdot riskien arvioinnin tulosten perusteella - määritetään käsittelyvaihtoehtojen toteuttamiseen tarvittavat hallintakeinot, jotka organisaatio voi suunnitella itse tai yksilöidä muista lähteistä. Niitä ovat esimerkiksi riskin välttäminen päättämällä olla aloittamatta tai jatkamatta riskin aiheuttavaa toimintaa tai poistamalla riskin lähteen, jaetaan riski muiden osapuolten kanssa vakuuttamisen, alihankkimisen tai riskin rahoittamisen avulla tai otetaan toinen riski tai kasvatetaan riskiä, jotta voidaan pyrkiä hyödyntämään liiketoimintamahdollisuus. - verrataan määritettyjä hallintakeinoja erilliseen taulukkoon ja todennetaan, ettei yhtään tarvittavaa keinoa ole jätetty pois (taulukko ei ole täydellinen, muita keinoja voidaan myös tarvita) - laaditaan soveltuvuuslausunto, joka sisältää vaaditut hallintakeinot (katso kaksi edellistä kohtaa) ja erillisessä taulukossa olevat perustelut hallintakeinojen käyttämiselle tai käyttämättä jättämiselle - laaditaan tietoturvariskien käsittelysuunnitelma, johon on dokumentoitava riskin käsittelemiseksi valittu vaihtoehto tai ehdot, tarvittavat hallintakeinot ja hallintakeinon toteuttamisen vaihe. Muut hyödylliset tiedot ovat riskin omistaja(t) ja odotettu jäännösriski, kun toimenpiteet on toteutettu. - hankitaan riskien omistajilta hyväksyntä käsittelysuunnitelmalle ja jäljelle jääville riskeille Käsittelyprosessista on säilytettävä dokumentoitua tietoa.	Soveltuvuuslausunto (Statement of Applicability), standardin tärkein dokumentti) + riskien käsittely	Oletteko laatineet tietoturvariskien käsittelyprosessin, soveltuvuuslausunnon ja käsittelysuunnitelman? Miten vaatimukset täyttyvät niissä? Ovatko ne dokumentoituna? Missä?			

	6.2 Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu		Asetettava asiankuuluville toiminnoille ja tasoille tietoturvatavoitteet, joiden on täytettävä seuraavat vaatimukset - yhdenmukaisuus tietoturvapolitiikan kanssa - mitattavia, jos mahdollista - huomioida soveltuvat tietoturvavaatimukset sekä riskien arvioinnin ja käsittelyn tulokset - niistä on viestittävä - niitä on päivitettävä tarvittaessa. Tietoturvatavoitteista on säilytettävä dokumentoitua tietoa. Tietoturvatavoitteen saavuttamisen suunnittelussa on määritettävä mitä tehdään, mitä resursseja tarvitaan, ketkä ovat vastuussa, milloin työ on valmiina ja kuinka tuloksia arvioidaan. Tietoturvallisuuden hallintajärjestelmään on harkittava seuraavia suunnitelmia: - tietoturvallisuuden hallintajärjestelmän parantamista koskevat suunnitelmat kohdissa 6.1.1 ja 8.1 - tunnistettujen riskien käsittelyä koskevat suunnitelmat kohdissa 6.3.1 ja 8.3 kuvatun mukaisesti - kaikki muut suunnitelmat, joita pidetään tarpeellisina vaikuttavuuden kannalta.	Tietoturvapolitiikka ja sen tavoitteet + riskien käsittely	Oletteko laatineet tietoturvatavoitteet? Millaisia ne ovat? Ovatko ne vaatimustenmukaisia? Onko tietoturvatavoitteiden saavuttaminen suunniteltua? Miten osoitatte sen?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
7. Tukitoiminnot	7.1 Resurssit		Määritettävä ja varattava tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen tarvittavat resurssit.		Onko teillä riittävästi resursseja hallintajärjestelmään luomiseen, ylläpitoon ja kehittämiseen? Miten pystytte vahvistamaan ja näyttämään sen? Onko teillä esimerkiksi luokiteltuna resurssit, kuten taloudelliset resurssit, toimenpiteitä edistävät ja suorittavat henkilöt, infrastruktuuri?			
	7.2 Pätevyys		Organisaation on - määritettävä millainen niiden työntekijöiden pätevyys pitää olla, joiden työ vaikuttaa tietoturvallisuuden tasoon - varmistettava pätevyys soveltuvan koulutuksen, harjoittelun tai kokemuksen perusteella - tarvittaessa hankittava vaadittava pätevyys ja arvioitava toimenpiteiden vaikuttavuutta - säilytettävä dokumentoitua tietoa pätevyyksistä. Pätevyys on kyky soveltaa tietoa ja taitoja halutun tuloksen saavuttamiseksi. Siihen vaikuttavat tieto, kokemus ja arvostelukyky. Korkeampia tai uusia pätevyyksiä ja taitoja voi saavuttaa sisäisesti ja ulkoisesti kokemusten, harjoittelun, mentoroinnin, siirtäminen toisiin työtehtäviin, ulkoisten henkilöiden palkkaamisen tai heidän palveluidensa ostamisen avulla.	Luettelo henkilökunnan koulutuksista, taidoista, kokemuksesta ja osaamisesta	Ovatko pätevyysvaatimukset määritettynä? Missä? Millaisia ne ovat? Miten pätevyydet varmistetaan?			
	7.3 Tietoisuus		Organisaation työntekijöiden on oltava tietoisia tietoturvapolitiikasta, miten he voivat osaltaan lisätä järjestelmän vaikuttavuutta, mitä hyötyä tietoturvallisuuden tason parantamisesta on ja seuraukset vaatimusten noudattamatta jättämisestä.		Ovatko organisaation työntekijät tietoisia tietoturvapolitiikasta, vaikuttavuuden lisäämisestä ja tason parantamisen hyödyistä? Ovatko he tietoisia seurauksista, joita voi olla vaatimusten noudattamatta jättämisellä? Miten olette toteuttaneet tämän?			

	7.4 Viestintä		Määritettävä hallintajärjestelmän kannalta tarvittava sisäinen ja ulkoinen viestintä, kuten mistä viestitään, milloin, keiden kanssa, ketkä viestittävät ja minkälaiset prosessit on toteutettava.		Onko sisäinen ja ulkoinen viestintä määritelty? Mitä ne ovat? Missä?			
	7.5 Dokumentoitu tieto							
		7.5.1 Yleistä	Dokumentoitava ISO/IEC 27001 -standardissa edellytetyt tiedot ja organisaation määrittelemät tietoturvallisuuden hallintajärjestelmän vaikuttavuuden kannalta välttämättömät tiedot.	(Dokumentoidun tiedon hallintaprosessi ja dokumenttienhallinnan kontrollit)	Onko teillä käytäntöjä dokumentoimisesta tai dokumentoitavista tiedosta? Mitä ja millaisia ne ovat? Oletteko dokumentoineet ISO/IEC 27001 -standardissa edellytetyt tiedot?			
		7.5.2 Dokumentoidun tiedon luominen ja päivittäminen	Varmistettava dokumentoidun tiedon asianmukainen merkintä ja kuvaus, talletusmuoto, tallennusväline sekä soveltuvuuden ja riittävyyden tarkistaminen ja hyväksyminen.		Miten varmistatte dokumentoidun tiedon asianmukaisuuden?			
		7.5.3 Dokumentoidun tiedon hallinta	Varmistettava dokumentoidun tiedon saatavuus sopivassa muodossa ja se on suojattava asianmukaisesti esimerkiksi estämällä asiaton käyttö, tiedon oltava muuttumatonta ja tietoa ei saa luovuttaa luvatta. Dokumenttien hallinnan on katettava jakelu, pääsy tietoihin, esille saanti, käyttö, varastointi ja säilytys, muutostenhallinta, säilyttäminen ja hävittäminen. Ulkopuolinen dokumentoitu tieto, joka on tarpeellinen tietoturvallisuuden hallintajärjestelmän kannalta, on yksilöitävä ja hallittava.		Miten teillä varmistetaan tiedon saatavuus ja suojataan tietoa? Miten hallitsette ja yksilöitte ulkopuolisen dokumentoidun tiedon?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
8. Toiminta	8.1 Toiminnan suunnittelu ja ohjaus		Suunniteltava ja toteutettava prosessit tietoturvan vaatimusten täyttämiseen ja kohdan 6.1 määritettyjen toimenpiteiden toteuttamiseen, sekä ohjattava niitä. Suunnitelmat on toteutettava siten, että saavutetaan kohdassa 6.2 määritetyt tietoturvatavoitteet. Jotta voidaan osoittaa prosessien toteuttaminen suunnitelmien mukaan, on säilytettävä dokumentoitua tietoa. Suunniteltuja muutoksia on hallittava ja arvioitava tahattomien muutosten seurauksia ja pyrittävä lieventämään haittavaikutuksia. On varmistettava, että ulkoiset prosessit ovat määritettynä ja niitä on valvottava.		Oletteko suunnitelleet prosessit tietoturvan vaatimusten täyttämiseen sekä tietoturvariskien arviointi- ja käsittelyprosessiin liittyviin toimenpiteisiin? Mitkä ne ovat? Miten ohjaatte niitä? Miten hallitsette ja arvioitte muutoksia? (Tietoturvariskien arviointi- ja käsittelyprosessi, kohdat 6.1.2 ja 6.1.3)?			
	8.2 Tietoturvariskien arviointi		Suoritettava tietoturvariskien arviointi ennen tai jälkeen merkittävien muutosten tai tehdä suunnitelluin aikavälein. Arvioinnin on täytettävä kohdan 6.1.2 kriteerit. Arviointien tuloksista on säilytettävä dokumentoitua tietoa.	Riskien arvioinnin ja käsittelyn raportointi	Suoritetaanko teillä tietoturvariskien arviointi säännöllisesti vai ennen tai jälkeen, kun merkittäviä muutoksia on syntynyt? Miten arviointi suoritetaan? (Arviointiprosessin laatiminen kohta 6.1.2)			
	8.3 Tietoturvariskien käsittely		Otettava käyttöön tietoturvariskien käsittelysuunnitelma, jonka tulokset on dokumentoitava.	Riskien käsittely + riskien arvioinnin ja käsittelyn raportointi	Onko teillä käytössä tietoturvariskien käsittelysuunnitelma? Miten dokumentoinnista huolehditaan? (Käsittelysuunnitelman laatiminen kohta 6.1.3.)			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
9. Suorituskyvyn arviointi	9.1 Seuranta, mittaus ja analysointi		Arvioitava tietoturvan tasoa ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta ja määritettävä - mitä seurataan ja mitataan (mukaan lukien tietoturvaprosessit ja hallintakeinot) - millä seuranta-, mittaus-, analysointi- tai arviointimenetelmillä on kelvollinen tulos - milloin seuranta ja mittaus on toteuttava - ketkä sen toteuttavat - milloin tulokset on analysoitava ja arvioitava ja ketkä ne suorittavat. Seurannan ja mittaamisen tulokset on dokumentoitava todisteeksi.	Seurannan ja mittausten tulokset	Mitä, miten, milloin ja millä mittaatte tietoturvan tasoa ja vaikuttavuutta? Onko teillä tietyt mittarit? Millaiset? Ketkä suorittavat mittaukset ja arvioivat ne? Missä dokumentteja säilytetään?			
	9.2 Sisäinen auditointi		Suoritettava sisäisiä auditointeja suunnitelluin aikavälein, jotta niiden tietojen perusteella voidaan määrittää - noudattaako tietoturvallisuuden hallintajärjestelmä järjestelmän ja ISO/IEC 27001 -standardin vaatimuksia - onko se toteutettu ja ylläpidetty jatkuvasti. Organisaation on - suunniteltava, laadittava, toteutettava ja ylläpidettävä auditointiohjelma, jossa määritellään auditointien taajuus, menetelmät, vastuut, suunnitteluvaatimukset ja raportointi ottaen huomioon prosessien tärkeys ja edellisten auditointien tulokset - määriteltävä auditointikriteerit ja soveltamisala. Auditointikriteerit ovat toimintaperiaatteita, menetelmiä tai vaatimuksia, joita käytetään vertailukohtana auditointinäytölle, ts. ne kuvaavat auditoijan odotuksia - valittava auditoijat ja suoritettava auditointiprosessit siten, että prosessien objektiivisuus ja puolueettomuus varmistuvat - varmistettava auditointien tulosten raportoinnista asiaankuuluville johdon henkilöille - säilytettävä dokumentoitua tietoa tuloksista todisteena. Sisäisten auditointien laajuus ja taajuus riippuvat organisaation koosta ja luonteesta sekä hallintajärjestelmän luonteesta, monimutkaisuudesta ja kypsyystasosta.	Sisäisen auditoinnin prosessi, sisäisen auditoinnin tulokset (Sisäisen auditoinnin työjärjestys)	Suoritetaanko teillä sisäisiä auditointeja säännöllisesti ja ovatko ne suunniteltuja tuleviksi vuosiksi (kohde ja ajankohta)? Miten olette toteuttaneet sen? Noudattavatko ne vaatimuksia? Minkälainen auditointiohjelma teillä on? Oletteko määritelleet auditointikriteerit? Millaiset? Kuka tai ketkä suorittavat auditoinnin? Missä säilytätte dokumentteja?			
	9.3 Johdon katselmus		Varmistettava suunnitelluin aikavälein tietoturvallisuuden hallintajärjestelmän soveltuvuus, asianmukaisuus ja vaikuttavuus. Johdon katselmuksissa on otettava huomioon - aiempien katselmusten takia käynnistettyjen toimenpiteiden tilanne - olennaiset ulkoisten ja sisäisten asioiden muutokset (ks. kohta 4.1) - tietoturvan tasoa koskeva palaute, johon sisältyvät poikkeamat, korjaavat toimenpiteet, seurannan, mittauksen ja auditointien tulokset sekä tietoturvatavoitteiden täyttyminen - sidosryhmien antama palaute - riskien arvioinnin tulokset ja riskinkäsittelysuunnitelman tilanne - jatkuvan parantamisen mahdollisuudet. Johdon katselmuksen tuloksiin on sisällyttävä päätökset jatkuvan parantamisen mahdollisuuksista ja muutostarpeista. Katselmuksen tuloksista on säilytettävä dokumentoitua tietoa.	Johdon katselmuksen tulokset	Miten varmistatte tietoturvallisuuden hallintajärjestelmän soveltuvuuden, asianmukaisuuden ja vaikuttavuuden? Onko se säännöllistä? Onko teillä selkeä rutiini siihen? Millainen?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Tavoitteet	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
10. Parantaminen	10.1 Poikkeamat ja korjaavat toimenpiteet		Kun poikkeama havaitaan - organisaation on reagoitava ja ryhdyttävä toimiin sen hallitsemiseksi sekä käsiteltävä seurauksia - arvioitava tarvittavat toimenpiteet poikkeaman syiden, toistuvuuden tai muualla esiintymisen poistamiseksi - toteutettava tarvittavat toimenpiteet ja arvioitava niiden vaikuttavuus - tehtävä tarvittaessa muutoksia hallintajärjestelmään. Prosessiin on sisällytettävä seuraavat asiat: - tunnistetaan poikkeaman laajuus ja vaikutus - päätetään korjauksista poikkeaman vaikutuksen rajoittamiseksi - viestintä olennaisten henkilöstön kanssa sen varmistamiseksi, että korjaukset suoritetaan - korjaukset suoritetaan päätöksen mukaan - tilannetta seurataan, jotta voidaan varmistua siitä, että korjauksilla on tarkoitettu vaikutus eikä tahattomia sivuvaikutuksia - jatketaan toimintaa poikkeaman korjaamiseksi, ellei sitä ole vielä korjattu - viestitään muiden olennaisten sidosryhmien kanssa tarvittaessa.	Poikkeamien korjausten tulokset (Poikkeamien korjausten työjärjestys)	Onko teillä työjärjestystä tai toimintaohjetta poikkeaman korjaamiseen, kun se havaitaan? Tietävätkö henkilöt mitä pitää tehdä, kun poikkeama ilmenee? Missä säilytätte dokumentteja?			
	10.2 Jatkuva parantaminen		Parannettava jatkuvasti tietoturvallisuuden hallintajärjestelmän soveltuvuutta, riittävyyttä ja vaikuttavuutta.		Miten osoitatte tietoturvallisuuden hallintajärjestelmän soveltuvuuden, riittävyyden ja vaikuttavuuden jatkuvan parantamisen? Miten toimitte?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.5 Tietoturvapolitiikat	A.5.1 Johdon ohjaus tietoturvallisuutta koskevissa asioissa		Tarjota johdon ohjausta ja tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti.						
		A.5.1.1 Tietoturvapolitiikat		Tietoturvallisuudelle on määriteltävä joukko johdon hyväksymiä poliitikkoja, jotka julkaistaan henkilökunnan ja asiaankuuluvien organisaation ulkopuolisten osapuolten käyttöön ja joista tiedotetaan henkilökunnalle ja muille osapuolille.		Oletteko määritelleet johdon hyväksymät poliitikot tietoturvallisuudelle? Mitä nämä dokumentit ovat? Miten tietoturvapolitiikasta tiedotetaan muille? Onko se tarvittavien henkilöiden saatavissa? (Ks. Kohta 7.3 Tietoisuus)			
		A.5.1.2 Tietoturvapolitiikkojen katselmointi		Tietoturvapolitiikat on katselmoitava suunnitelluin aikavälein tai kun merkittäviä muutoksia tapahtuu, jotta varmistetaan, että ne ovat edelleen soveltuvia, asianmukaisia ja vaikuttavia.		Tarkistetaanko tietoturvapolitiikat säännöllisesti? Miten tarkastukset toteutetaan? Kuinka usein? Ketkä sen suorittavat?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.6 Tietoturvallisuuden organisointi	A.6.1 Sisäinen organisaatio		Luoda hallintarakenne, jolla aloitetaan tietoturvallisuuden toteuttaminen ja käyttö organisaatiossa ja hallitaan sitä.						
		A.6.1.1 Tietoturvaroolit ja -vastuut		Kaikki tietoturvavastuut on määriteltävä ja jaettava.		(Ks. kohta 5.3 Organisaation roolit, vastuut ja valtuudet)			
		A.6.1.2 Tehtävien eriyttäminen		Ristiriidassa olevien tehtävien ja vastuualueiden on oltava eriytettyjä, jotta vähennetään organisaation suojattavan omaisuuden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä.		Ovatko ristiriitaiset tehtävät eriytettyjä? Miten?			
		A.6.1.3 Yhteydet viranomaisiin		Asiaankuuluviin viranomaisiin on ylläpidettävä tarkoituksenmukaisia yhteyksiä.		Pidättekö yhteyttä asiaankuuluviin viranomaisiin? Kehen? Oletteko laatinet menettelyt, jossa määritellään milloin ja kenen on otettava yhteyttä viranomaisiin? Missä?			
		A.6.1.4 Yhteydet osaamisyhteisöihin		Osaamisyhteisöihin tai muihin turvallisuusasiantuntijaryhmiin ja ammatillisiin järjestöihin on ylläpidettävä tarkoituksenmukaisia yhteyksiä.		Entä osaamisyhteisöihin? Kehen?			
		A.6.1.5 Tietoturvallisuus projektinhallinnassa		Projektinhallinnassa on käsiteltävä tietoturvallisuutta projektin tyypistä riippumatta.		Käsitteletkö aina tietoturvallisuutta projektinhallinnassa? Millä tavalla tietoturvallisuus on liitetty projektinhallintaan?			
	A.6.2 Mobiililaitteet ja etätyö		Varmistaa etätyön ja mobiililaitteiden käytön turvallisuus.						
		A.6.2.1 Mobiililaitteita koskeva politiikka		On otettava käyttöön politiikka ja sitä tukevat turvallisuuskäytännöt, joilla hallitaan mobiililaitteiden käytöstä syntyviä riskejä.	(Mobiililaitteiden ja etätyön politiikka) (Omien laitteiden tuomisen politiikka)	Oletteko määritelleet mobiililaitteita koskevan politiikan? Entä omien laitteiden politiikan? Missä? Miten niissä huomioidaan laitteiden henkilökohtainen käyttö ja työkäyttö? Järjestättekö koulutusta, jossa selvitetään työskentelytavasta aiheutuvia erityisriskejä ja käyttöön otettavia hallintakeinoja? Miten koulutus toteutetaan?			
		A.6.2.2 Etätyö		On otettava käyttöön politiikka ja sitä tukevat turvallisuuskäytännöt, joilla suojataan etätyöpaikalla käytettyä, käsiteltyä tai säilytettävää tietoa.		Oletteko määritelleet etätyötä koskevan politiikan ja siihen liittyvät ehdot ja rajoitukset? Missä?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.7 Henkilöstöturvallisuus	A.7.1 Ennen työsuhteen alkua		Varmistaa, että työntekijät ja vuokratyöntekijät ymmärtävät velvollisuutensa ja ovat sopivia heille harkittuihin tehtäviin.						
		A.7.1.1 Taustatarkistus		Kaikkien työnhakijoiden tausta on tarkastettava asianmukaisten lakien, määräysten ja eettisten normien mukaisesti. Tarkastukset on myös suhteutettava liiketoiminnallisiin vaatimuksiin, käsiteltävän tiedon luokitukseen ja oletettuihin riskeihin.		Tarkastetaanko työntekijöiden tausta? Mitä keinoja käytätte? Oletteko laatineet taustatarkistuksen kriteerit ja menettelyt?			
		A.7.1.2 Työsopimuksen ehdot		Työntekijöiden ja vuokratyöntekijöiden kanssa tehdyissä sopimuksissa on eriteltävä työntekijän tai vuokratyöntekijän ja organisaation vastuut tietoturvallisuudesta.	Turvallisuuden roolien ja vastuiden määrittely	Oletteko eritelleet työntekijöiden ja organisaation vastuut tietoturvallisuudesta? Miten viestitte niistä työnhakijoille?			
	A.7.2 Työsuhteen aikana		Varmistaa, että työntekijät ja vuokratyöntekijät ovat tietoisia tietoturvavastuistaan ja täyttävät ne.						
		A.7.2.1 Johdon vastuut		Johdon on edellytettävä, että kaikki työntekijät ja vuokratyöntekijät toimivat tietoturvallisesti organisaation olemassa olevien politiikkojen ja menettelyjen mukaisesti.		Miten johto huolehtii, että työntekijät toimivat politiikkojen ja menettelyjen mukaisesti? Mitä keinoja käytätte?			
		A.7.2.2 Tietoturvatietoisuus, -opastus ja -koulutus		Kaikkien organisaation työntekijöiden sekä tarvittaessa vuokratyöntekijöiden on saatava asianmukainen tietoturvatietoisuusopastus ja -koulutus, ja heidän tietojaan organisaation politiikkojen ja menettelyjen muutoksista on päivitettävä säännöllisesti, mikäli se on heidän toimikuvansa kannalta merkityksellistä.		Saavatko työntekijät säännöllisesti tietoturvatietoisuusopastusta ja -koulutusta? Kuinka usein ja mitä asioita niissä esimerkiksi käsitellään? Miten koulutukset toteutetaan? Päivitetäänkö heidän tietojaan?			
		A.7.2.3 Kurinpitoprosessi		Organisaatiolla on oltava muodollinen ja tiedossa oleva kurinpitoprosessi, jonka perusteella toimitaan, kun työntekijä on syyllistynyt tietoturvarikkomukseen.		Onko teillä muodollista kurinpitoprosessia? Noudatetaanko kurinpitoprosessissa asteittaista toimintamallia?			
	A.7.3 Työsuhteen päättyminen tai muuttuminen		Suojata organisaation etuja osana työsuhteen päättymis- tai muutosprosessia.						
		A.7.3.1 Työsuhteen päättyminen tai vastuiden muuttuminen		On määritettävä tietoturvavastuut ja -velvollisuudet, jotka jäävät voimaan työsuhteen päättymisen tai muuttumisen jälkeen. Niistä on tiedotettava työntekijälle tai vuokratyöntekijällä ja niiden noudattaminen on varmistettava.		Oletteko määritelleet tietoturvavastuut ja -velvollisuudet, kun työsuhde päättyy tai muuttuu? Ovatko ne sisällytetty työsopimuksen ehtoihin? Miten tämä on toteutettu? Miten sitä seurataan?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.8 Suojattavan omaisuuden hallinta	A.8.1 Vastuu suojattavasta omaisuudesta		Yksilöidä organisaation suojattava omaisuus ja määritellä asianmukaiset suojausvastuut.						
		A.8.1.1 Suojattavan omaisuuden luetteloiminen		Tieto sekä tietoon ja tietojenkäsittelypalveluihin liittyvä suojattava omaisuus on yksilöitävä. Suojattava omaisuus on luetteloitava ja tätä luetteloa on ylläpidettävä.	Suojattavan omaisuuden luettelo	Oletteko laatineet luettelon suojattavasta omaisuudesta koko tiedon elinkaaren ajalta (luominen, käsittely, varastointi, siirtäminen, poistaminen ja tuhoaminen)? Missä? Miten huolehditte sen päivittämisestä?			
		A.8.1.2 Suojattavan omaisuuden omistajuus		Omaisuusluettelossa olevalla suojattavalla omaisuudella on oltava omistaja.		Oletteko nimenneet kullekin yksilöidylle suojattavalle omaisuudelle omistajan? Huolehtivatko ne suojattavan omaisuuden luetteloinnista, luokittelusta, pääsyrajoituksista ja luokituksista? Miten tämä toteutuu?			
		A.8.1.3 Suojattavan omaisuuden hyväksyttävä käyttö		Tiedon sekä tietoon ja tietojenkäsittelypalveluihin liittyvän suojattavan omaisuuden hyväksyttävän käytön säännöt on yksilöitävä, dokumentoitava ja toteutettava.	Suojattavan omaisuuden hyväksyttävä käyttö	Oletteko laatineet säännöt suojattavan omaisuuden hyväksyttävästä käytöstä? Missä? Miten suojattavaa omaisuutta käyttävät henkilöt tai siihen käsiksi pääsevät henkilöt ovat tietoisia sen hyväksyttävästä käytöstä?			
		A.8.1.4 Suojattavan omaisuuden palauttaminen		Kaikkien työntekijöiden ja organisaation ulkopuolisten käyttäjien on palautettava kaikki hallussaan oleva organisaation suojattava omaisuus työtehtävän, työsuhteen tai sopimuksen päättyessä.		Miten suojattava omaisuus palautetaan, kun työtehtävä päättyy? Miten tarkistatte, että kaikki suojattava omaisuus on palautettu? Oletteko laatineet päättymisprosessin? Missä?			

	A.8.2 Tietojen luokittelu		Varmistaa, että tiedon suojaustaso on riittävä. Riittävä suojaustaso määräytyy sen perusteella, miten merkittävää tieto on organisaatiolle.		(Tietojen luokittelupolitiikka)				
		A.8.2.1 Tiedon luokittelu		Tieto on luokiteltava lakisääteisten vaatimusten, tiedon arvon ja kriittisyyden sekä sen luvattoman paljastumisen tai muokkaamisen aiheuttamien vaikutusten perusteella.		Oletteko luokitelleet tiedon vaatimustenmukaisesti? Sisältävätkö ne luokittelukäytännöt ja kriteerit tuleville katselmoinneille? Miten olette huomioineet luokittelussa liiketoiminnan tarpeet tiedon jakamisen ja rajoittamisen suhteen sekä lakisääteiset vaatimukset? Oletteko liittäneet luokittelun osaksi prosesseja? Onko teillä laadittuna tietojen luokittelupolitiikka? Missä?			
		A.8.2.2 Tiedon merkintä		Tiedon merkitsemistä koskevat asianmukaiset menettelyt on laadittava ja otettava käyttöön organisaation määrittelemien tiedon luokitteluperusteiden mukaisesti.		Oletteko laatineet tiedon merkintää koskevat menettelyt? Missä? Noudatatteko niitä fyysisessä ja sähköisessä tiedostoissa?			
		A.8.2.3 Suojattavan omaisuuden käsittely		Suojattavan omaisuuden käsittelemistä koskevat menettelyt on laadittava ja otettava käyttöön organisaation määrittelemien tiedon luokitteluperiaatteiden mukaisesti.		Oletteko laatineet ja ottaneet käyttöön suojattavan omaisuuden käsittelyä koskevat menettelyt? Missä? Mihin asioihin olette kiinnittäneet huomiota politiikassa (esim. pääsyrajoitukset, luettelon ylläpitäminen, suojattavien omaisuuksien varastointi, tietovälinekopioiden luvallista vastaanottajaa koskeva selkeä merkintä)?			

	A.8.3 Tietovälineiden luokittelu		Estää tietovälineille tallennettujen tietojen luvaton paljastuminen, muuttuminen, poistaminen tai tuhoutuminen.						
		A.8.3.1 Siirrettävien tietovälineiden hallinta		On laadittava siirrettävien tietovälineiden hallintaa koskeva asianmukainen ohjeistus organisaation määrittelemien luokitteluperiaatteiden mukaisesti.		Oletteko laatineet siirrettävien tietovälineiden politiikan ja menettelyt? Onko se asianmukainen? Missä?			
		A.8.3.2 Tietovälineiden hävittäminen		Tarpeettomat tietovälineet on hävitettävä turvallisella tavalla muodollisten menettelyjen mukaisesti.	(Tietovälineiden hävittämispolitiikka)	Onko laatineet käytännöt tietovälineiden hävittämiseen? Poltatteko tai silppuatteko tietovälineitä? Hyödynnättekö tietovälineiden keräys- ja hävityspalveluja?			
		A.8.3.3 Fyysisten tietovälineiden siirtäminen		Tietoa sisältävät tietovälineet on suojattava luvattomalta pääsyltä, väärinkäytöltä ja turmeltumiselta siirron aikana.		Oletteko suojanneet tietovälineet siirron ajaksi? Mitä keinoja hyödynnätte?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.9 Pääsynhallinta	A.9.1 Pääsynhallinnan liiketoiminnalliset vaatimukset		Hallita pääsyä tietoon ja tietojenkäsittelypalveluihin.						
		A.9.1.1 Pääsynhallintapolitiikka		Pääsynhallinnan periaatteet on laadittava, dokumentoitava ja katselmoitava liiketoiminnallisten vaatimusten ja tietoturvavaatimusten perusteella.	Pääsynhallintapolitiikka	Oletteko laatineet pääsynhallintapolitiikan? Onko se vaatimustenmukainen? Missä määritelty?			
		A.9.1.2 Pääsy verkkoihin ja verkkopalveluihin		Käyttäjille on sallittava pääsy ainoastaan niihin verkkoihin ja verkkopalveluihin, joihin heille on nimenomaisesti myönnetty pääsyoikeudet.		Oletteko laatineet verkkopalvelujen käyttöpolitiikan? Kattaako se vaadittavat tiedot?			
	A.9.2 Pääsyoikeuksien hallinta		Varmistaa valtuutettujen käyttäjien pääsy järjestelmiin ja palveluihin sekä estää luvaton pääsy niihin.						
		A.9.2.1 Käyttäjien rekisteröinti ja poistaminen		On toteutettava muodollinen käyttäjien rekisteröinti- ja poistamisprosessi, jonka avulla pääsyoikeudet jaetaan.	(Salasanapolitiikka)	Oletteko laatineet muodollisen käyttäjien rekisteröinti- ja poistamisprosessin, kuten yksilölliset käyttäjätunnukset ja niiden jäädyttämisen tai poistamisen heti, kun niiden haltijat eivät ole enää organisaatiossa?			
		A.9.2.2 Pääsyoikeuksien jakaminen		On toteutettava muodollinen pääsyoikeuksien jakoprosessi, jonka avulla kyetään antamaan tai kumoamaan pääsyoikeus minkä tahansa tyyppiseltä käyttäjältä mihin tahansa järjestelmään tai palveluun.	(Salasanapolitiikka)	Oletteko toteuttaneet pääsyoikeuksien jakoprosessin? Mitä asioita olette sisällyttäneet siihen?			
		A.9.2.3 Ylläpito-oikeuksien hallinta		Ylläpito-oikeuksien jakamista ja käyttöä on rajoitettava ja valvottava.		Miten olette rajoittaneet ylläpito-oikeuksien jakoa ja käyttöä?			
		A.9.2.4 Käyttäjien tunnistautumistietojen hallinta		Tunnistautumistietojen jakamista on valvottava muodollisen hallintaprosessin avulla.	(Salasanapolitiikka)	Valvotteko tunnistautumistietojen jakamista hallintaprosessin avulla? Mitä vaatimuksia olette sisällyttäneet siihen?			
		A.9.2.5 Pääsyoikeuksien uudelleenarviointi		Suojattavan omaisuuden omistajien on uudelleenarvioitava pääsyoikeuksia säännöllisin aikavälein.		Arvioitteko uudelleen pääsyoikeuksia? Miten usein? Mihin asioihin kiinnitätte huomioita?			
		A.9.2.6 Pääsyoikeuksien poistaminen tai muuttaminen		Kaikkien työntekijöiden ja organisaation ulkopuolisten osapuolten käyttäjien pääsyoikeudet tietoon ja tietojenkäsittelypalveluihin on poistettava heidän työtehtävänsä, työsuhteensa tai sopimuksensa päättyessä tai pääsyoikeuksia on muutettava muutosten mukaisesti.		Muutatteko tai poistatteko pääsyoikeudet, kun työsuhde päättyy tai muuttuu? Miten tämä toteutuu?			
	A.9.3 Käyttäjien vastuut		Saattaa käyttäjät vastuullisiksi omien tunnistautumistietojensa turvaamisesta.						
		A.9.3.1 Tunnistautumistietojen käyttö		Käyttäjien on tunnistautumistietojen käytössä noudatettava organisaation käytäntöjä.		Noudattavatko käyttäjät tunnistautumistiedoissaan organisaation käytäntöjä? Miten olette opastaneet käyttäjiä?			

	A.9.4 Järjestelmien ja sovellusten pääsynhallinta		Estää luvaton pääsy järjestelmiin ja sovelluksiin.						
		A.9.4.1 Tietoihin pääsyn rajoittaminen		Pääsyä tietoihin ja sovellusjärjestelmien toimintoihin on rajoitettava pääsynhallintapolitiikan mukaisesti.		Oletteko rajoittaneet tietoihin pääsyä? Millä tavoin?			
		A.9.4.2 Turvallinen kirjautuminen		Pääsyä järjestelmään ja sovelluksiin on hallittava turvallisella kirjautumismenettelyllä, kun pääsynhallintapolitiikassa niin velvoitetaan.		Käytättekö turvallista kirjautumismenettelyä? Millaista?			
		A.9.4.3 Salasanojen hallintajärjestelmä		Salasanojen hallintajärjestelmän on oltava vuorovaikutteinen, ja sen on edellytettävä vahvojen salasanojen käyttöä.	(Salasanapolitiikka)	Oletteko laatineet salasanojen hallintajärjestelmän? Millaisen? Edellyttääkö se vahvojen salasanojen käyttöä?			
		A.9.4.4 Ylläpito- ja hallintasovellukset		Järjestelmän ja sovellusten hallintakeinot ohittamaan kykenevien apuohjelmien käyttöä on rajoitettava, ja niitä on hallittava tarkasti.		Oletteko rajoittaneet apuohjelmien käyttöä, jotka kykenevät ohittamaan järjestelmän ja sovellusten hallintakeinot? Millä tavoin?			
		A.9.4.5 Lähdekoodin suojaaminen pääsynvalvonnalla		Pääsyä ohjelmien lähdekoodeihin on rajoitettava.		Miten olette rajoittaneet pääsyä ohjelmien lähdekoodeihin? Miten valvontaa toteutetaan?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.10 Salaus	A.10.1 Salauksen hallinta		Varmistaa salauksen asianmukainen ja vaikuttava käyttö, jotta tiedon luottamuksellisuutta, aitoutta ja eheyttä kyetään suojaamaan.						
		A.10.1.1 Salauksen käytön periaatteet		On laadittava ja toteutettava politiikka, jota noudatetaan, kun tietoa suojataan salauksen avulla.		Oletteko laatineet salauksen käyttöön liittyvät periaatteet (salauspolitiikan)? Missä?			
		A.10.1.2 Salausavainten hallinta		Salausavainten käytöstä, suojaamisesta ja käyttöiästä on laadittava politiikka, ja tätä politiikkaa on noudatettava salausavainten koko käyttöiän ajan.		Oletteko laatineet salausavainten hallintaan liittyvä politiikan? Millaisia prosesseja siihen liittyy? Missä? Noudatetaanko sitä?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.11 Fyysinen turvallisuus ja ympäristön turvallisuus	A.11.1 Turva-alueet		Estää luvaton tunkeutuminen organisaation tietoaineistoihin ja tietojenkäsittelypalveluihin sekä estää niiden vahingoittuminen ja toiminnan häiriintyminen.						
		A.11.1.1 Fyysinen turva-alue		Turva-alueet on määriteltävä ja niitä on noudatettava paikoissa, jotka sisältävät joko arkaluonteisia tai kriittisiä tietoja ja tietojenkäsittelypalveluita.		Ovatko turva-alueet määriteltynä? Mitä asioita huomioitte fyysisissä turva-alueissa? Noudatetaanko niitä?			
		A.11.1.2 Kulunvalvonta		Turva-alueet on suojattava asianmukaisella kulunvalvonnalla, jotta varmistetaan, että vain luvan saaneet henkilöt pääsevät alueelle.		Ovatko turva-alueet suojattu asianmukaisella kulunvalvonnalla? Millaisella? Mihin kiinnitätte huomiota?			
		A.11.1.3 Toimistojen, tilojen ja laitteistojen suojaus		Toimistojen, tilojen ja laitteistojen fyysinen turvallisuus on suunniteltava ja toteuttava.		Miten toimistojen, tilojen ja laitteistojen fyysinen turvallisuus on suunniteltu?			
		A.11.1.4 Suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan		On suunniteltava ja toteutettava fyysiset suojakeinot luonnon katastrofien, vihamielisten hyökkäysten tai onnettomuuksien varalta.		Millaiset fyysiset suojakeinot teillä on käytössä? Millä tavalla olette hyödyntäneet asiantuntijoiden apua?			
		A.11.1.5 Turva-alueilla työskentely		On suunniteltava ja toteutettava menettelyt, joiden mukaisesti turva-alueilla työskennellään.	(Turva-alueilla työskentelyn menettelyohje)	Onko teillä menettelyohje turva-alueilla työskentelemiseen? Millainen?			
		A.11.1.6 Toimitus- ja kuormauslauseet		Kulkualueita, kuten toimitus- ja kuormausalueita, sekä muita pisteitä, joiden kautta luvattomat henkilöt saattavat päästä tiloihin, on valvottava, ja ne on mahdollisuuksien mukaan eristettävä tietojenkäsittelypalveluista, jotta niihin ei pääse luvatta.		Valvotaanko kulkualueita? Ovatko kulkuealueet erillään tietojenkäsittelypalveluista? Jos ei, miten palveluihin pääseminen luvatta on estetty?			

	A.11.2 Laitteet		Estää omaisuuden katoaminen, vahingoittuminen, varastaminen tai vaarantuminen sekä organisaation toimintojen keskeyttäminen.						
		A.11.2.1 Laitteiden sijoitus ja suojaus		Laitteistot on sijoitettava ja suojattava siten, että ympäristöuhkien ja luvattoman tunkeutumisen riskejä pienennetään.		Miten olette huolehtineet laitteistojen suojaamisen ja sijoittamisen? Onko pääsy työskentelyalueille mahdollisimman vähäinen, onko arkaluonteista tietoa käsittelevät tietojenkäsittelypalvelut sijoitettu siten, että luvattomat henkilöt eivät näkisi tietoa, estetäänkö varastoalueille luvaton pääsy jne.			
		A.11.2.2 Peruspalvelut		Laitteet on suojattava sähkökatkoilta ja muilta peruspalveluiden vikojen aiheuttamilta häiriöiltä.		Oletteko suojanneet laitteet sähkökatkoilta ja muilta peruspalveluiden häiriöiltä? Arvioitteko, tarkastatteko ja testaatteko säännöllisesti laitteet? Miten tämä toteutuu?			
		A.11.2.3 Kaapeloinnin turvallisuus		Sähkökaapelointi sekä tietoa siirtävä tai tietotekniikkapalveluilta tukeva tietoliikennekaapelointi on suojattava salakuuntelulta, häirinnältä ja vahingoittumiselta.		Miten olette huolehtineet kaapeloinnin turvallisuudesta? Maanalainen kaapelointi? Ovatko sähkökaapelit erillään tietoliikennekaapeleista?			
		A.11.2.4 Laitteiden huolto		Laitteet on huollettava asianmukaisesti, jotta niiden jatkuva käytettävyys ja eheys voidaan varmistaa.		Miten toteutatte laitteiden huollon? Suorittaako sen organisaation ulkopuolinen taho? Pidättekö kirjaa kaikista epäilyistä ja sattuneista vioista sekä ehkäisevistä ja korjaavista toimenpiteistä?			
		A.11.2.5 Suojattavan omaisuuden poistaminen		Laitteita, tietoaineistoja ja ohjelmistoja ei saa poistaa toimipaikalta ilman ennalta saatua valtuutusta.		Oletteko yksilöineet henkilöt, joilla on lupa sallia suojattavan omaisuuden siirtäminen? Onko siirtämiselle asetettu aikarajat? Millä tavalla osoitatte palautusten aikarajojen noudattamisen?			
		A.11.2.6 Toimitilojen ulkopuolelle vietyjen laitteiden ja suojattavan omaisuuden turvallisuus		Toimitilojen ulkopuolella olevan suojattavan omaisuuden turvallisuus on varmistettava. Tässä on otettava huomioon, että organisaation tilojen ulkopuolella työskentelyyn liittyvät riskit ovat erilaisia.		Jätetäänkö laitteita julkisiin tiloihin ilman valvontaa? Noudatatteko aina valmistajan ohjeita laitteiden suojauksessa? Miten suojattava omaisuus on varmistettu tilapäisissä toimitiloissa, koti- ja etätyöskentelyssä (esim. lukittavat tallennuskaapistot, puhtaan pöydän periaate, tietokoneiden pääsynhallinta)?			
		A.11.2.7 Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen		Kaikki laitteiden tallennettua tietoa sisältävät osat on tarkistettava, jotta voidaan varmistua siitä, että arkaluonteinen tieto ja tekijänoikeuden suojaamat ohjelmistot on poistettu tai tuhottu turvallisesti ennen laitteen käytöstä poistamista tai kierrättämistä.	(Tietovälineiden hävittämispolitiikka)	Tarkastatteko laitteet ennen käytöstä poistamista tai kierrättämistä? Kuka huolehtii siitä? Jos luotettavaa tietoa, miten toimitte? (Katso kohta A.8.3.2, Tietovälineiden hävittäminen)			

		A.11.2.8 Ilman valvontaa jäävät laitteet		Käyttäjien on varmistettava, että ilman valvontaa jäävät laitteet on suojattu asianmukaisesti.		Ovatko käyttäjät tietoisia menettelyistä, jolla suojataan ilman valvontaa jääviä laitteita? Ohjataanko heitä esim. päättämään aktiivinen istunto, kirjautumaan ulos sovelluksesta tai lukitsemaan käyttämätön tietokone työn päättyessä? Miten toteutatte käyttäjien ohjaamisen?			
		A.11.2.9 Puhtaan pöydän ja puhtaan näytön periaate		On otettava käyttöön papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan näytön periaate sekä tietojenkäsittelypalveluja koskeva puhtaan näytön periaate.	(Puhtaan pöydän ja näytön periaatteen ohje)	Onko teillä ohjetta puhtaan pöydän ja näytön periaatteesta? Otetaanko niissä huomioon tietoluokitukset (ks. kohta A.8.2), lainsäädäntöön ja sopimuksiin sisältyvät vaatimukset (ks. kohta A.18.1) sekä niiden mukaiset riskit ja organisaatiota koskevat näkökohdat? Missä? Noudatetaanko periaatteita, kuten arkaluontainen tieto lukitussa paikassa ja tieto poistetaan tulostimista välittömästi?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.12 Käyttöturvallisuus	A.12.1 Toimintaohjeet ja velvollisuudet		Varmistaa tietojenkäsittelypalveluiden asianmukainen ja turvallinen toiminta.						
		A.12.1.1 Dokumentoidut toimintaohjeet		Toimintaohjeet on dokumentoitava ja niiden on oltava kaikkien niitä tarvitsevien käyttäjien saatavilla.	IT:n hallinnoinnin toimintaohjeet	Oletteko dokumentoineet toimintaohjeet? Ovatko ne kaikkien saatavilla? Missä?			
		A.12.1.2 Muutoksenhallinta		Tietoturvallisuuteen vaikuttavia organisaatioon, liiketoimintaprosesseihin ja tietojenkäsittelypalveluihin ja -järjestelmiin tehtäviä muutoksia on hallittava.	(Muutoksenhallintapolitiikka)	Miten hallitsette muutoksia? Onko teillä tietyt käytännöt siihen? Oletteko laatineet muutoksenhallintapolitiikan?			
		A.12.1.3 Kapasiteetinhallinta		Resurssien käyttöä on tarkkailtava ja säädettävä ja on tehtävä ennusteita tulevista kapasiteettivaatimuksista, jotta voidaan varmistaa, että järjestelmän suorituskyky vastaa vaadittua.		Miten hallitsette ja tarkkailette kapasiteettia? Mitä keinoja?			
		A.12.1.4 Kehitys-, testaus- ja tuotantoympäristöjen erottaminen		Kehitys-, testaus- ja tuotantoympäristöt on erotettava toisistaan, jotta pienennetään tuotantoympäristön luvattoman käytön tai muuttamisen riskiä.		Millä tavalla olette eritelleet kehitys-, testaus- ja tuotantoympäristöt toisistaan? Onko teillä esimerkiksi tiettyjä sääntöjä, ajetaanko ohjelmistot eri järjestelmillä tai testaatteko muutoksia testausympäristössä?			
	A.12.2 Haittaohjelmilta suojautuminen		Varmistaa, että tiedot ja tietojenkäsittelypalvelut on suojattu haittaohjelmilta.						
		A.12.2.1 Haittaohjelmilta suojautuminen		Haittaohjelmilta suojaavat havaitsemis-, esto- ja palautusmekanismit on toteutettava, ja käyttäjien tietoisuutta haittaohjelmista on ylläpidettävä.		Oletteko toteuttaneet haittaohjelmilta suojaavat toimenpiteet? Millaiset? Miten ylläpidätte käyttäjien tietoisuutta haittaohjelmistoista? Oletteko laatineet politiikan luvattomien ohjelmien käytöstä tai riskeiltä suojautumiseen, kun tiedostoja hankitaan ulkopuolisista verkoista?			

	A.12.3 Varmuuskopiointi		Suojautua tiedon menettämiseltä.						
		A.12.3.1 Tietojen varmuuskopiointi		Tiedoista, ohjelmistoista ja järjestelmistä on otettava säännöllisesti varmuuskopiot, jotka on testattava sovittujen varmuuskopiointiperiaatteiden mukaisesti.	(Varmuuskopiointipolitiikka)	Oletteko laatineet varmuuskopiointipolitiikan? Missä? Testaatteko varmuuskopioita varmuuskopiointiperiaatteiden mukaisesti? Kuinka usein? Kuka sen suorittaa?			
	A.12.4 Kirjaaminen ja seuranta		Tallentaa tapahtumat ja luoda seurantatietoja.						
		A.12.4.1 Tapahtumien kirjaaminen		On luotava tapahtumalokeja, joihin tallennetaan käyttäjien suorittamat toiminnot sekä tapahtuneet poikkeamat, virheet ja tietoturvatapahtumat. Nämä lokit on säilytettävä ja niitä on katselmoitava säännöllisesti.	Käyttäjätapahtumien, poikkeamien ja tietoturvatapahtumien loki	Pidättekö lokia käyttäjätapahtumista, poikkeamista ja tietoturvatapahtumista? Tarkastellaanko niitä säännöllisesti? Kuinka usein? Ketkä tarkistuksen toteuttavat?			
		A.12.4.2 Lokitietojen suojaaminen		Lokitiedot ja niiden kirjauspalvelut on suojattava peukaloimiselta ja luvaton pääsy niihin on estettävä.		Miten olette suojanneet lokitiedot luvattomalta pääsyltä ja vääristämiseltä?			
		A.12.4.3 Pääkäyttäjä- ja operaatiolokit		Järjestelmän pääkäyttäjien ja operaattorien toiminnoista on pidettävä lokia. Nämä lokit on suojattava ja niitä on katselmoitava säännöllisesti.	Käyttäjätapahtumien, poikkeamien ja tietoturvatapahtumien loki	Pidättekö lokia pääkäyttäjien ja operaattorien toiminnoista? Ovatko ne suojattu? Tarkastellaanko niitä säännöllisesti? Kuinka usein? Ketkä sen suorittavat?			
		A.12.4.4 Kellojen synkronointi		Kaikkien samassa organisaatiossa tai samalla turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on asetettava saman viiteaikalähteen mukaisesti.		Oletteko synkronoineet kellot saman viiteaikalähteen mukaisesti, jotta taattaisiin tapahtumalokien täsmällisyys? Miten tämä on toteutettu? Oletteko dokumentoineet ajan esittämistä, synkronointia ja tarkkuutta koskevat sisäiset ja ulkopuoliset vaatimukset? Missä? Oletteko määritelleet organisaatiossa käytettävän vertailuajan?			
	A.12.5 Tuotantokäytössä olevien ohjelmistojen hallinta		Varmistaa tuotantokäytössä olevien järjestelmien kehitys.						
		A.12.5.1 Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin		On luotava menettelyt, joilla valvotaan ohjelmistojen asentamista tuotantokäytössä oleviin järjestelmiin.		Oletteko laatineet menettelyt ohjelmistojen asentamisesta tuotannossa oleviin järjestelmiin? Kuka huolehtii ohjelmistojen ylläpidosta?			
	A.12.6 Teknisten haavoittuvuuksien hallinta		Estää teknisten haavoittuvuuksien hyväksikäyttö.						
		A.12.6.1 Teknisten haavoittuvuuksien hallinta		Käytettävien tietojärjestelmien teknisistä haavoittuvuuksista on hankittava ajantasaista tietoa. Organisaation altistuminen näille haavoittuvuuksille on arvioitava, ja niihin liittyviin riskeihin on vastattava asianmukaisilla toimenpiteillä.		Millä tavalla hankitte tietoa teknisistä haavoittuvaisuuksista? Oletteko laatineet toimenpiteet tai prosessit teknisten haavoittuvaisuuksien vastaamiseen? Missä?			
		A.12.6.2 Ohjelmien asentamisen rajoittaminen		On laadittava ja otettava käyttöön käyttäjien suorittamaa ohjelmien asentamista koskevat säännöt.		Oletteko laatineet ohjelmien asentamiseen koskevat säännöt tai politiikan? Missä? Käytättekö niitä?			

	A.12.7 Tietojärjestelmien auditointinäkökohtia		Varmistaa, että auditointitoiminnot vaikuttavat käytössä oleviin järjestelmiin mahdollisimman vähän.						
		A.12.7.1 Tietojärjestelmien auditointimekanismit		Auditointivaatimukset ja -toiminnot, jotka sisältävät tuotantokäytössä olevien järjestelmien todentamisia, on suunniteltava huolellisesti ja hyväksyttävä, jotta liiketoimintaprosesseja häiritään mahdollisimman vähän.		Oletteko suunnitelleet ja hyväksyttäneet auditointivaatimukset ja -toiminnot yhdessä johdon kanssa? Mitä vaatimukset ja toiminnot ovat? Missä?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.13 Viestintäturvallisuus	A.13.1 Verkon turvallisuuden hallinta		Varmistaa verkossa liikkuvan tiedon ja sen tukena olevien tietojenkäsittelypalveluiden suojaaminen.						
		A.13.1.1 Verkon hallinta		Verkkoja on hallittava ja valvottava, jotta voidaan suojata järjestelmissä ja sovelluksissa oleva tieto.		Miten hallitsette ja valvotte verkkoja? Miten varmistatte, että verkoissa käsiteltävät tiedot ja niihin liittyvät palvelut on suojattu luvattomalta pääsyltä?			
		A.13.1.2 Verkkopalvelujen turvaaminen		Kaikkien verkkopalvelujen turvamekanismit, palvelutasot ja hallintavaatimukset on yksilöitävä ja sisällytettävä verkkopalvelusopimuksiin riippumatta siitä, tuotetaanko näitä palveluita organisaation sisällä vai onko ne ulkoistettu.		Miten olette sisällyttäneet ja yksilöineet verkkopalvelujen turvamekanismit, palvelutasot ja hallintavaatimukset? Kuinka usein tarkastelette niitä?			
		A.13.1.3 Ryhmien eriyttäminen verkossa		Verkoissa olevat tietojenkäsittelypalvelujen, käyttäjien ja tietojärjestelmien ryhmät on eriytettävä toisistaan.		Pidättekö tietojenkäsittelypalvelut, käyttäjät ja tietojärjestelmien ryhmät erillään? Hyödynnättekö siinä erillisiä verkkoalueita? Miten se toteutuu?			
	A.13.2 Tietojen siirtäminen		Ylläpitää organisaation sisällä tai jonkin ulkopuolisen osapuolen kanssa siirretyn tiedon suojausta.						
		A.13.2.1 Tiedonsiirtopolitiikat ja -menettelyt		Kaikentyyppisillä viestintäpalveluilla tapahtuvaa tiedon siirtämistä on suojattava määriteltyjen tiedonsiirtopolitiikan ja tiedonsiirron menettelyiden ja hallintakeinojen avulla.	(Tiedonsiirtopolitiikka)	Oletteko laatineet vaatimustenmukaiset tiedonsiirtopolitiikat ja -menettelyt? Missä?			
		A.13.2.2 Tiedonsiirtoa koskevat sopimukset		Sopimusten on katettava liiketoimintatietojen turvallinen siirtäminen organisaation ja ulkopuolisten osapuolten välillä.	(Tiedonsiirtopolitiikka)	Oletteko laatineet tiedonsiirtosopimukset ja sisällyttäneet siihen vaadittavat asiat, kuten hallintavastuut ja menettelyt, joilla varmistetaan jäljitettävyys ja kiistettävyys? Missä?			
		A.13.2.3 Sähköinen viestintä		Sähköisesti viestitettyä tietoa on suojattava asianmukaisesti.	(Tiedonsiirtopolitiikka)	Suojaatteko riittävästi sähköistä viestintää? Mitä keinoja hyödynnätte?			
		A.13.2.4 Salassapito- ja vaitiolositoumukset		Organisaation tiedonsuojaustarpeita kuvastavat vaatimukset salassapito- ja vaitiolositoumuksille on yksilöitävä, katselmoitava säännöllisesti ja dokumentoitava.	Turvallisuuden roolien ja vastuiden määrittely -> ks. kohta 5.3	Oletteko yksilöineet, dokumentoineet ja tarkastelleet säännöllisesti salassapito- ja vaitiolositoumukset? Kuinka usein? Ketkä sen suorittavat? Missä ne ovat?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.14 Järjestelmien hankkiminen, kehittämien ja ylläpito	A.14.1 Tietojärjestelmiä koskevat turvallisuusvaatimukset		Varmistaa, että tietoturvallisuus on olennainen osa tietojärjestelmiä koko niiden elinkaaren ajan. Tähän sisältyvät myös palveluita julkisten verkkojen välityksellä tarjoavia tietojärjestelmiä koskevat turvallisuusvaatimukset.						
		A.14.1.1 Tietoturvavaatimusten analysointi ja määrittely		Tietoturvallisuuteen liittyvät vaatimukset olisi sisällytettävä uusia tai parannettavia tietojärjestelmiä koskeviin vaatimuksiin.		Ovatko tietoturvallisuuteen liittyvät vaatimukset sisällytetty tietojärjestelmiä koskeviin tapahtumiin? Ovatko tietoturvavaatimukset yksilöity ja määritelty vaatimustenmukaisesti? Mitä menetelmiä olette hyödyntäneet?			
		A.14.1.2 Sovelluspalveluiden suojaaminen julkisissa verkoissa		Julkisten verkkojen kautta siirrettävää sovelluspalveluihin kuuluvaa tietoa on suojattava vilpilliseltä ja sopimuksen vastaiselta toiminnalta ja luvattomalta paljastumiselta ja muuttumiselta.		Mitä asioita huomioitte suojatessa sovelluspalveluita julkisissa verkoissa? Miten usein päivitätte ja katselmoitte tätä?			
		A.14.1.3 Sovellustapahtumien suojaaminen		Sovelluspalvelutapahtumiin liittyvää tietoa on suojattava, jotta estetään niiden epätäydellinen lähetys, väärään paikkaan ohjautuminen, luvaton viestien muuttaminen ja luvaton paljastuminen sekä viestin luvaton kopiointi tai toisto.		Millä tavalla suojaatte sovellustapahtumien tietoa?			

	A.14.2 Kehitys- ja tukiprosessien turvallisuus		Varmistaa, että tietoturvallisuutta suunnitellaan ja toteutetaan tietojärjestelmien kehittämisen elinkaaren osana.						
		A.14.2.1 Turvallisen kehittämisen politiikka		Ohjelmien ja järjestelmien kehittämistä koskevat säännöt on laadittava, ja niitä on sovellettava organisaation sisällä toteuttaviin kehitysprojekteihin.		Oletteko laatineet turvallisen kehittämisen politiikan? Missä? Miten hyödynnätte niitä kehitysprojekteissa? Miten olette hankkineet vakuuden, että ulkoinen taho noudattaa turvallisen kehittämisen sääntöjä?			
		A.14.2.2 Järjestelmään tehtävien muutosten hallintamenettelyt		Järjestelmiin niiden kehittämisen elinkaaren aikana tehtäviä muutoksia on hallittava muodollisilla muutoksenhallintamenettelyillä.		Oletteko laatineet muutoksenhallintamenettelyt? Mitä kaikkia vaiheita prosessiin kuuluu? Hyödynnättekö automaattisia päivityksiä myös kriittisiin järjestelmiin?			
		A.14.2.3 Sovellusten tekninen katselmointi käyttöalustan muutosten jälkeen		Liiketoiminnan kannalta kriittiset sovellukset on tarkistettava ja testattava käyttöalustan muutosten yhteydessä, jotta varmistetaan, ettei muutoksilla ole haitallisia vaikutuksia organisaation toimintaan tai turvallisuuteen.		Millä tavalla suoritatte sovellusten tarkistamisen ja testaamisen? Missä suunnitelma on?			
		A.14.2.4 Ohjelmistopakettien muutoksia koskevat rajoitukset		Ohjelmistopaketteihin tehtäviä muutoksia on vältettävä, ja ne on rajoitettava vain välttämättömiin muutoksiin, minkä lisäksi kaikkia muutoksia on hallittava tarkasti.	(Muutoksenhallintapolitiikka)	Millä tavalla olette rajoittaneet ohjelmistopaketteihin tehtäviä muutoksia? Jos olette tehneet muutoksia, oletteko huomioineet yhteensopivuuden toisien ohjelmistojen kanssa, tietoisia vastamaan ohjelmiston ylläpidosta muutosten takia, mahdollisesti kysyneet myyjältä lupaa tai saaneet tarvittavat muutokset tavanomaisina ohjelmistopäivityksinä. (Ks. kohta 12.1.2 Muutoksenhallinta)			

		A.14.2.5 Turvallisen järjestelmäsuunnittelun periaatteet		Turvallisten järjestelmien toteuttamisen periaatteet on laadittava ja dokumentoitava. Niitä on ylläpidettävä ja niitä on sovellettava kaikkiin tietojärjestelmien kehitystoimiin.	Turvallisen järjestelmäsuunnittelun periaatteet	Oletteko laatineet ja dokumentoineet turvallisen järjestelmäsuunnittelun periaatteet? Missä? Kuinka usein tarkastatte? Miten olette varmistaneet, että toimittajan turvallisuuden kehittämisperiaatteet vastaavat organisaation omia periaatteita? Oletteko soveltaneet turvallisuuden kehittämisperiaatteita ulkoistettuihin tietojärjestelmiin?			
		A.14.2.6 Turvallinen kehitysympäristö		Organisaatioiden on luotava ja asianmukaisesti suojattava kehitysympäristö, jota hyödynnetään järjestelmän kehittämisessä ja integroinnissa ja joka kattaa järjestelmän koko kehityselinkaaren.		Oletteko laatineet turvallisen kehitysympäristön, joka sisältää henkilöt, prosessit ja teknologian? Mihin asioihin olette kiinnittäneet huomiota? Huomioitteko turvalliseen kehitysympäristöön liittyvät asiat?			
		A.14.2.7 Ulkoistettu kehittäminen		Organisaation on valvottava ja seurattava ulkoistettuja järjestelmän kehitystoimintoja.		Miten seuraatte ja valvotte ulkoistettuja järjestelmän kehitystoimintoja?			
		A.14.2.8 Järjestelmän turvallisuustestaus		Kehitystyön aikana on testattava turvallisuustoiminnallisuudet.		Miten suoritatte turvallisuustestaukset? Onko teillä käytössä riippumaton hyväksymistestaus? Miten suoritatte riippumattoman hyväksymistestauksen ulkoistettuihin kehitystoimiin?			
		A.14.2.9 Järjestelmän hyväksymistestaus		Uusille tietojärjestelmille, päivityksille ja uusille versioille on laadittava hyväksymistestausohjelmat ja niihin liittyvät kriteerit.		Oletteko laatineet hyväksymistestausohjelmat ja niihin liittyvät kriteerit? Missä ne ovat? Hyödynnättekö koodin analysointityökaluja tai haavoittuvuusskannereita?			

	A.14.3 Testiaineisto		Varmistaa testaukseen käytettävän tiedon suojaus.						
		A.14.3.1 Testiaineiston suojaaminen		Testiaineistot on valittava huolellisesti ja niitä on suojattava ja hallittava.		Miten suojaatte testiaineistot? Valitsetteko testiaineistot huolellisesti? Vältättekö luottamuksellista tietoa, kuten henkilötietoja testauksissa?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.15 Suhteet toimittajiin	A.15.1 Tietoturvallisuus toimittajasuhteissa		Varmistaa, että organisaation toimittajien käytettävissä oleva suojattava omaisuus on suojattu.						
		A.15.1.1 Toimittajasuhteiden tietoturvapolitiikka		Tietoturvavaatimuksista, joilla vähennetään toimittajan pääsyoikeudesta organisaation suojattavaan omaisuuteen aiheutuvia riskejä, on sovittava yhdessä toimittajan kanssa, ja ne on dokumentoitava.	Toimittajien tietoturvapolitiikka	Miten olette sopineet toimittajien kanssa tietoturvapolitiikasta ja laatineet tietoturvavaatimukset? Käsittävätkö ne kaikki prosessit ja menettelyt? Missä ne ovat dokumentoituna?			
		A.15.1.2 Toimittajasopimusten turvallisuus		Kaikki olennaiset tietoturvavaatimukset on laadittava ja hyväksyttävä jokaisen toimittajan kanssa, jolla saattaa olla pääsy organisaation tietoihin tai joka saattaa käsitellä tai viestiä näitä tietoja tai toimittaa niihin liittyviä IT-infrastruktuurin osia.		Oletteko hyväksyttäneet tietoturvavaatimukset jokaisen toimittajan kanssa? Miten hyväksyttäminen on toteutettu?			
		A.15.1.3 Tieto- ja viestintätekniikan toimitusketju		Toimittajien kanssa tehtävien sopimusten on sisällettävä vaatimukset, joilla vastataan tieto- ja viestintätekniikkapalveluihin ja tuotteen toimitusketjuihin liittyviin tietoturvariskeihin.		Oletteko laatineet vaatimustenmukaisesti tieto- ja viestintätekniikan toimitusketjut? Mihin asioihin olette kiinnittäneet huomiota niissä? Mitä ne sisältävät?			
	A.15.2 Toimittajien palveluiden hallinta		Ylläpitää toimittajasopimusten mukaista sovittua tietoturvatasoa ja palveluiden toimitustasoa.						
		A.15.2.1 Toimittajien palvelujen seuranta ja katselmointi		Organisaatioiden on säännöllisesti seurattava, katselmoitava ja auditoitava toimittajan palveluiden toteuttamista.		Miten suoritatte säännöllisen toimittajien palvelujen seurannan ja katselmoinnin? Onko teillä laadittuna jokin yhteistyöprosessi?			
		A.15.2.2 Toimittajan palveluihin tulevien muutosten hallinta		Toimittajan palvelujen tarjoamista koskevia muutoksia, mukaan lukien olemassa olevan tietoturvapolitiikan, menettelyjen ja hallintakeinojen ylläpitoa ja kehitystä, on hallittava ottaen huomioon kyseisten liiketoimintatietojen, -järjestelmien ja -prosessien kriittisyys ja riskien uudelleenarviointi.		Miten hallitsette toimittajan palveluihin tulevien muutosten hallinnan? Mihin näkökohtiin kiinnitätte huomiota?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.16 Tietoturvahäiriöiden hallinta	A.16.1 Tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinta		Varmistaa, että tietoturvahäiriöiden hallinnan toimintamalli on johdonmukainen ja vaikuttava ja että siihen sisältyy myös tietoturvatapahtumista ja -heikkouksista viestiminen.						
		A.16.1.1 Vastuut ja menettelyt		On määriteltävä hallintavastuut ja luotava menettelyt, joilla taataan pikainen, tehokas ja järjestelmällinen reagointi tietoturvahäiriöihin.		Oletteko määritelleet hallintavastuut? Mitkä ne ovat? Minkälaiset menettelyt olette luoneet tietoturvahäiriöiden reagoimiseen?			
		A.16.1.2 Tietoturvatapahtumien raportointi		Tietoturvatapahtumista on raportoitava mahdollisimman nopeasti ja asiaankuuluvaa hallintokanavaa pitkin.		Millä tavalla raportoitte tietoturvatapahtumista? Käytättekö asiaankuuluvaa hallintokanavaa?			
		A.16.1.3 Tietoturvaheikkouksien raportointi		Organisaation tietojärjestelmiä ja palveluita käyttävien työntekijöiden ja vuokratyöntekijöiden on kiinnitettävä huomiota kaikkiin järjestelmissä tai palveluissa oleviin tai epäiltyihin tietoturvaheikkouksiin ja raportoitava niistä.		Miten kiinnitätte huomiota epäiltyihin tai palveluissa oleviin tietoturvaheikkouksiin? Mihin niistä raportoidaan?			
		A.16.1.4 Tietoturvatapahtumien arviointi ja niitä koskevien päätösten tekeminen		Tietoturvatapahtumat on arvioitava, minkä jälkeen on tehtävä päätös siitä, luokitellaanko ne tietoturvahäiriöiksi.		Millä tavalla luokittelette tietoturvahäiriöt? Onko teillä selkeät ohjeet siitä, että onko häiriö tietoturvariski vai ei? Millainen luokitteluasteikko teillä on käytössä?			
		A.16.1.5 Tietoturvahäiriöihin vastaaminen		Tietoturvahäiriöihin on reagoitava menettelyohjeen mukaisesti.	Toimintaohje tietoturvahäiriöistä	Oletteko laatineet menettelyohjetta tietoturvahäiriöistä? Missä?			
		A.16.1.6 Tietoturvahäiriöistä oppiminen		Tietoturvahäiriöiden analysoinnista ja ratkaisemisesta saatua tietämystä on hyödynnettävä tulevien häiriöiden todennäköisyyden vähentämisessä ja niiden vaikutusten pienentämisessä.		Yritättekö oppia tietoturvahäiriöistä? Miten olette toteuttaneet tämän? Onko laadittuna jokin menettelyohje?			
		A.16.1.7 Todisteiden kokoaminen		Organisaation on määriteltävä ja toteutettava menettelyt todistusaineistoksi soveltuvan tiedon yksilöimiseen, keräämiseen, hankkimiseen ja säilyttämiseen.		Oletteko laatineet menettelyt todistusaineiston kokoamiseen? Missä? Huomioidaanko siinä hallussapitoketju, todisteiden ja henkilöstön turvallisuus, asiaan liittyvien henkilöiden roolit ja vastuut, henkilöstön pätevyys, dokumentaatio ja selonteot?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.17 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia	A.17.1 Tietoturvallisuuden jatkuvuus		Tietoturvallisuuden jatkuvuuden on sisällytettävä organisaation liiketoiminnan jatkuvuuden hallintajärjestelmiin.						
		A.17.1.1 Tietoturvallisuuden jatkuvuuden suunnittelu		Organisaation on määriteltävä tietoturvallisuutta ja sen jatkuvuutta epäsuotuisissa tilanteissa koskevat vaatimukset.	(Liiketoiminnan keskeytysanalyysi)	Oletteko määritelleet liiketoiminnan keskeytysanalyysin? Miten olette suunnitelleet tietoturvallisuuden jatkuvuuden epäsuotuisissa tilanteissa? Jos ei, onko tietoturvavaatimukset samat myös epäsuotuisissa tilanteissa, kun niitä verrataan normaaleihin toimintaolosuhteisiin?			
		A.17.1.2 Tietoturvallisuuden jatkuvuuden toteuttaminen		Organisaation on laadittava, dokumentoitava, toteuttava ja ylläpidettävä prosesseja, menettelyjä ja hallintamekanismeja, joilla varmistetaan, että tietoturvallisuuden jatkuvuuden vaadittu taso säilyy epäsuotuisissa tilanteissa.	Tietoturvan jatkuvuuden toimintaohjeet	Oletteko laatineet tietoturvan jatkuvuudesta toimintaohjeet? Miten toteutatte tietoturvallisuuden jatkumisen epäsuotuisissa tilanteissa?			
		A.17.1.3 Tietoturvallisuuden jatkuvuuden todentaminen, katselmointi ja arviointi		Organisaation on todennettava laaditut ja toteutetut tietoturvallisuuden jatkuvuuden hallintamekanismit säännöllisin aikavälein, jotta voidaan varmistaa, että ne ovat päteviä ja vaikuttavia epäsuotuisissa tilanteissa.	(Tietoturvan harjoittelu ja testaussuunnitelma) (Tietoturvan katselmointi ja tarkastussuunnitelma)	Tarkastatteko säännöllisesti tietoturvallisuuden jatkuvuuden hallintamekanismit? Miten toteutatte sen? Oletteko laatineet dokumentit testaussuunnitelmasta ja tarkastussuunnitelmasta? Missä?			
	A.17.2 Vikasietoisuus		Varmistaa, että tietojenkäsittelypalvelut ovat saatavilla.						
		A.17.2.1 Tietojenkäsittelypalvelujen saatavuus		Tietojenkäsittelypalvelut on toteutettava niin vikasietoisina, että saatavuusvaatimukset täyttyvät.	(Liiketoiminnan jatkuvuusstrategia)	Oletteko määritelleet liiketoiminnan jatkuvuusstrategian? Ovatko tietojenkäsittelypalvelut toteutettu mahdollisimman vikasietoisiksi? Millä tavalla?			

Vaatimusala	Vaatimuskohta	Vaatimuksen alakohta	Hallintatavoite	Hallintakeino	Vaadittavat dokumentit	Kysymykset	Lähtötilanne	Puutteet	Suositeltavat toimenpiteet
A.18 Vaatimustenmukaisuus	A.18.1 Lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen		Kaikkien tietoturvallisuuteen liittyvien lakien ja asetusten, säännösten ja sopimusten velvoitteiden sekä mahdollisten turvallisuusvaatimusten noudattaminen.						
		A.18.1.1 Sovellettavien lakisääteisten ja sopimuksellisten vaatimusten yksilöiminen		Kaikki asiaankuuluvat lakien ja viranomaisten ja sopimusten asettamat vaatimukset sekä organisaation toimintamalli niiden täyttämistä varten on yksilöitävä yksiselitteisesti ja dokumentoitava sekä pidettävä ajan tasalla kutakin tietojärjestelmää ja organisaatiota varten.	Lakisääteiset ja sopimukselliset vaatimukset	Oletteko yksilöineet ja dokumentoineet lakisääteiset ja sopimukselliset vaatimukset sekä organisaation toimintamallin? Missä ne ovat? Miten pidätte niitä ajan tasalla ja kuka siitä huolehtii?			
		A.18.1.2 Immateriaalioikeudet		On toteutettava asianmukaiset menettelyt, joilla varmistetaan, että immateriaalioikeuksiin ja tekijänoikeuksilla suojattujen ohjelmistotuotteiden käyttöön liittyvien lakien, viranomaisten ja sopimusten asettamia vaatimuksia noudatetaan.		Miten osoitatte, että noudatatte immateriaali- ja tekijänoikeuksilla suojattuja ohjelmistotuotteita ja niihin liittyviä vaatimuksia ja lakeja?			
		A.18.1.3 Tallenteiden suojaaminen		Tallenteet on suojattava katoamiselta, tuhoutumiselta, väärentämiseltä, luvattomalta käytöltä ja luvattomalta levittämiseltä lakien, viranomaisten, sopimusten ja liiketoiminnan asettamien vaatimusten mukaisesti.		Miten suojaatte tallenteet? Luokitteletteko ne eri tallennetyypeittäin (esim. kirjanpito- ja tietokantatallenne, tapahtuma- ja lokitiedostoihin) Noudatatteko suojaamisessa lakeja ja vaatimuksia?			
		A.18.1.4 Tietosuoja ja henkilötietojen suojaaminen		Tietosuoja ja henkilötietojen suojaus on varmistettava asiaankuuluvien lakien ja viranomaisten asettamien vaatimusten mukaisesti.		Miten varmistatte tietosuojan ja henkilötietojen suojauksen? Noudatteko suojaamisessa lakeja ja vaatimuksia?			

		A.18.1.5 Salaustekniikan hallintaa koskevat säädökset		Salaustekniikan hallintamekanismeja on käytettävä kaikkien asianmukaisten lakien, viranomaisten ja sopimusten asettamien vaatimusten mukaisesti.		Käytättekö salaustekniikan hallintamekanismeja säädösten mukaisesti?			
	A.18.2 Tietoturvallisuuden katselmoinnit		Varmistaa, että tietoturvallisuus on toteutettu ja että sitä noudatetaan organisaation politiikkojen ja menettelyjen mukaisesti.						
		A.18.2.1 Tietoturvallisuuden riippumaton katselmointi		Organisaation tietoturvallisuuden toimintamalli ja sen toteuttaminen (eli tietoturvallisuuteen liittyvät hallintatavoitteet, hallintakeinot, politiikat, prosessit ja menettelyt) on katselmoitava riippumattomasti suunnitelluin aikavälein tai kun tapahtuu merkittäviä muutoksia.		Tarkastetaanko teillä riippumattomasti ja säännöllisesti tietoturvallisuuden toimintamalli? Miten osoitatte riippumattomuuden (esim. sisäinen auditointi, riippumaton esimies tai katselmuksiin erikoistunut ulkopuolinen organisaatio)? Kuinka usein?			
		A.18.2.2 Turvallisuuspolitiikkojen ja -standardien noudattaminen		Esimiesten on säännöllisesti katselmoitava, ovatko heidän vastuualueillaan olevat tietojenkäsittelymenettelyt ja muut menettelyt tarkoituksenmukaisen turvallisuuspolitiikan ja -standardien sekä muiden mahdollisten turvallisuusvaatimusten mukaisia.		Millä tavalla osoitatte, että noudatatte turvallisuuspolitiikkoja ja standardeja? Onko teillä mittaus- tai raportointityökaluja katselmoinnin toteuttamista varten?			
		A.18.2.3 Teknisten vaatimustenmukaisuuden katselmointi		Tietojärjestelmien vaatimustenmukaisuus organisaation tietoturvapolitiikkojen ja -standardien suhteen on katselmoitava säännöllisesti.		Tarkastatteko säännöllisesti tietojärjestelmien tekniset vaatimukset? Kuinka usein? Kuka sen suorittaa?			