

ISO/IEC 27001 -standardointiin valmistautuminen

Kirsi Lehmuskanta

Tekijä(t) Kirsi Lehmuskanta	
Koulutusohjelma Tietojärjestelmäosaamisen koulutusohjelma, tradenomi (ylempi AMK)	
Raportin/Opinnäytetyön nimi ISO/IEC 27001 -standardointiin valmistautuminen	Sivu- ja liitesivumäärä 28 + 1
Tiivistelmä <p>Opinnäytetyön tarkoituksena on selvittää ja kuvata ISO/IEC 27001 -standardin tarvittavat vaatimukset ALTEN Finlandille. Opinnäytetyössä käsitellään standardin eri osa-alueita ja nämä muodostavat teoriaosuuden opinnäytetyölle. Opinnäytetyössä käydään lävitse hallintatavoitteiden jaottelu ja peilataan ALTEN Finlandin valmiutta hakea standardia.</p> <p>Opinnäytetyö on luonteeltaan kehitystehtävä. Kehitystehtävän kohteena on suunnittelutoimisto ALTEN Finland, jossa ollaan ottamassa ISO 27001 -standardi käyttöön vuosien 2018-2019 aikana.</p>	
Asiasanat ISO/IEC 27001, tietoturvallisuus, hallintajärjestelmä	

Author(s) Kirsi Lehmuskanta	
Degree program Master's Degree in Business Information Technology	
The title of thesis Preparing for the ISO/IEC 27001 Standardization	Number of pages and appendices 28 + 1
<p>Abstract</p> <p>The purpose of the thesis is to determine and depict the necessary requirements of the ISO/IEC 27001 standard for ALTEN Finland. The various aspects of the standard are discussed and they form the theoretical part of the thesis. The thesis goes through the division of the management objectives and examines ALTEN Finland's readiness to apply for the standard.</p> <p>The thesis is a development project for ALTEN Finland, an engineering and technology consulting company, which is adopting the ISO/IEC 27001 standard during 2018-2019.</p>	
<p>Key words ISO/IEC 27001, information security, management system</p>	

Sisällys

1	Johdanto	1
2	Opinnäytetyön tavoitteet ja rakenne	2
3	Toimeksiantajan esittely	3
3.1	ALTEN Finland.....	3
3.2	ALTEN Finlandin historiaa	4
3.3	ALTEN Finlandin henkilöstö.....	4
3.3.1	ALTEN kansainvälisesti.....	5
4	ISO/IEC 27001 -standardi	6
4.1	Yleistä standardista.....	6
4.2	Prosessimainen toimintamalli.....	7
4.3	Tietoturvallisuuden hallintajärjestelmä.....	8
4.4	Johdon vastuut.....	8
4.5	Sisäinen auditointi ja johdon katselmointi	9
4.6	Jatkuva parantaminen.....	10
5	Hallintatavoitteiden ja –keinojen viiteluettelo	11
5.1	Tietoturvapoliitikat	11
5.2	Tietoturvallisuuden organisointi	11
5.3	Mobiililaitteet ja etätyö.....	11
5.3.1	Mobiililaitteet	11
5.3.2	Etätyö.....	12
5.4	Henkilöstöturvallisuus	13
5.5	Suojattavan omaisuuden hallinta	14
5.6	Pääsynhallinta.....	14
5.7	Salaus.....	15
5.8	Fyysinen turvallisuus ja ympäristön turvallisuus	15
5.9	Käyttöturvallisuus.....	16
5.10	Viestintäturvallisuus	17
5.11	Järjestelmien hankkiminen, kehittäminen ja ylläpito	17
5.12	Suhteet toimittajiin.....	18
5.13	Tietoturvahäiriöiden hallinta	18
5.14	Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia.....	19
5.15	Vaativuustentmukaisuus	19
6	Sertifiointi	20
6.1	Sertifiointiprosessi.....	20
6.1.1	Sertifiointihakemus.....	20
6.1.2	Suunnittelukokous.....	20
6.1.3	Ennakkoarviointi.....	21

6.1.4	Sertifiointiarviointi	21
6.1.5	Uusinta-arviointi	22
6.1.6	Seuranta-arvioinnit	22
7	ALTEN Finlandin tilanne.....	23
8	Kysely	24
8.1	Kyselyn yhteenveto	24
8.2	ALTEN Finlandin kehityskohteet	24
8.3	Pohdinta ja jatkotoimenpiteet ALTEN Finlandille	25
9	Lähteet	27
	Liitteet.....	29
	Kysely	29

1 Johdanto

Tietoturvallisuuden merkitys on noussut organisaatioissa hyvin tärkeään rooliin lisääntyvien tietoturvauhkien vuoksi. Organisaatioiden toimintaan kohdistuu tietoturvauhia organisaatioiden ympäristöjen ja –toimintatapojen johdosta. Organisaatioiden toiminta on riippuvainen tietojärjestelmien toiminnasta.

Tietojärjestelmien toiminnan riippuvuus organisaatiossa asettaa tietojärjestelmien ja tietoturvallisuuden hallinnan merkittäväksi asiaksi sekä organisaation sisäisen toiminnan, että eri sidosryhmien välisen toiminnan suhteen. Tietoturvan hallintaan on panostettava merkittävässä määrin organisaation koosta, tyypistä tai toiminta-alueesta huolimatta. ISO/IEC 27001 mahdollistaa kattavat ja hyvät menetelmät tietoturvallisuuden hallintaan kaiken tyyppisille ja -kokoisille organisaatiolle. Kaikki organisaatiot keräävät, käsittelevät, tallentavat ja siirtävät tietoa monissa muodoissa, mukaan lukien sähköisesti, fyysisesti ja suullisesti. Tieto on arvokkaampaa kuin numerot, kuvat ja painetut sanat.

Tietoturvallisuus saavutetaan toteuttamalla soveltuva hallintakeinojen järjestelmä, joka koostuu prosesseista, menettelyistä, organisaatorakenteesta, politiikasta sekä ohjelmisto- ja laitteistotoiminnoista. Tätä varten on laadittava ja otettava käyttöön hallintakeinot ja niitä on seurattava, katselmoitava ja tarvittaessa parannettava, jotta saavutetaan organisaation määrittelemät turvallisuus- ja liiketoimintatavoitteet. ISO/IEC 27001 antaa puitteet ja hallintakeinot tehdä tietojärjestelmät standardin mukaisesti turvallisiksi.

2 Opinnäytetyön tavoitteet ja rakenne

Opinnäytetyön tavoitteena on kuvata ALTEN Finlandille (myöhemmin viitattuna ALTEN) ISO/IEC 27001:2013-standardin vaatimukset sekä käydä niitä lävitse päätasolla ja valmistautua ISO 27001 -projektin läpiviemiseen. Tarkoituksena on myös selvittää, tarvitaanko henkilöstölle lisää koulutusta tietoturvan osalta.

Asiakkaiden vaatimuksena on kasvavassa määrissä, että yrityksellä on olemassa ISO 27001 -standardi käytössä ja että työskentely tehdään standardia mukaillen. Tämä on puolueeton tapa osoittaa yhteistyökumppaneille tietoturvan toteutuminen ja tuo kasvavassa kilpalutilanteessa etulyöntiaseman yritykselle.

3 Toimeksiantajan esittely

3.1 ALTEN Finland

ALTEN Finland on osa suurta ranskalaista suunnittelutoimistoa ALTEN Groupia. ALTEN tarjoaa suunnittelu- sekä ICT-alan asiantuntemusta alansa johtaville yrityksille. Maailmanlaajuisen verkoston ja vahvan paikallisen markkina-aseman ansiosta ALTEN pystyy tuottamaan asiakkailleen heidän tarpeisiinsa räätälöityjä ratkaisuja. (ALTEN Finland. 2017a.)

Suomessa ALTEN on kehittänyt työntekijöidensä osaamista strategisesti merkittävillä teollisuudenaloilla vuodesta 1969 lähtien. Pitkän kokemuksensa ansiosta ALTEN on alallaan kilpailukykyinen palveluntarjoaja. ALTENin suurimmat asiakkaat toimivat prosessi- ja energiatekniikan, valmistavan teollisuuden ja rakennustekniikan alalla. ALTEN vastaa asiakkaidensa tarpeisiin tarjoamalla kattavan valikoiman palveluja kyseisillä toimialoilla. (ALTEN Finland 2017a.)

ALTENin suunnittelijat tarjoavat laajan skaalan palveluita esi- ja konseptisuunnittelusta aina työn toimeenpanoon ja projektinhallintaan asti. ALTEN tarjoaa suunnittelupalveluja kaikenkokoisille projekteille, ja ALTENin suunnittelijat voivat työskennellä joko ALTENin tai asiakkaan tiloissa. ALTENin menestys kumpuaa liiketoimintamallista, joka antaa työntekijöilleen paljon valinnanvapautta ja vastuuta. ALTENin palvelulupaus on, että asiakas löytää aina yrityksensä tarpeisiin sopivat, motivoituneet asiantuntijat. (ALTEN Finland 2017c.)



Kuvio 1. ALTEN Finlandin toiminta-alueet (ALTEN Finland 2017b).

3.2 ALTEN Finlandin historiaa

Yritys, joka nykyisin tunnetaan ALTEN Finlandina, sai alkunsa vuonna 1969. Tarmo Soralahden perustama yritys aloitti silloin toimintansa nimellä ALTE Oy. Vuonna 1973 yrityksen johtoon astui Seppo Soralahti joka luotsasi yritystä aina vuoteen 2014 asti, jolloin ranskalainen suunnittelutoimisto ALTEN Group osti toiminnan. Vuosina 2003–2017 ALTEN Finlandin toimitusjohtajana toimi Keijo Hämäläinen. Hänen siirtyessä pois toimitusjohtajan tehtävästä, tehtävän otti vastaan Juha Sillanpää elokuussa 2017. (Soralahti, Hämäläinen & Jokinen 2009.)



Kuvio 2. ALTE Groupin historian kulku (ALTEN Finland 2017a).

3.3 ALTEN Finlandin henkilöstö

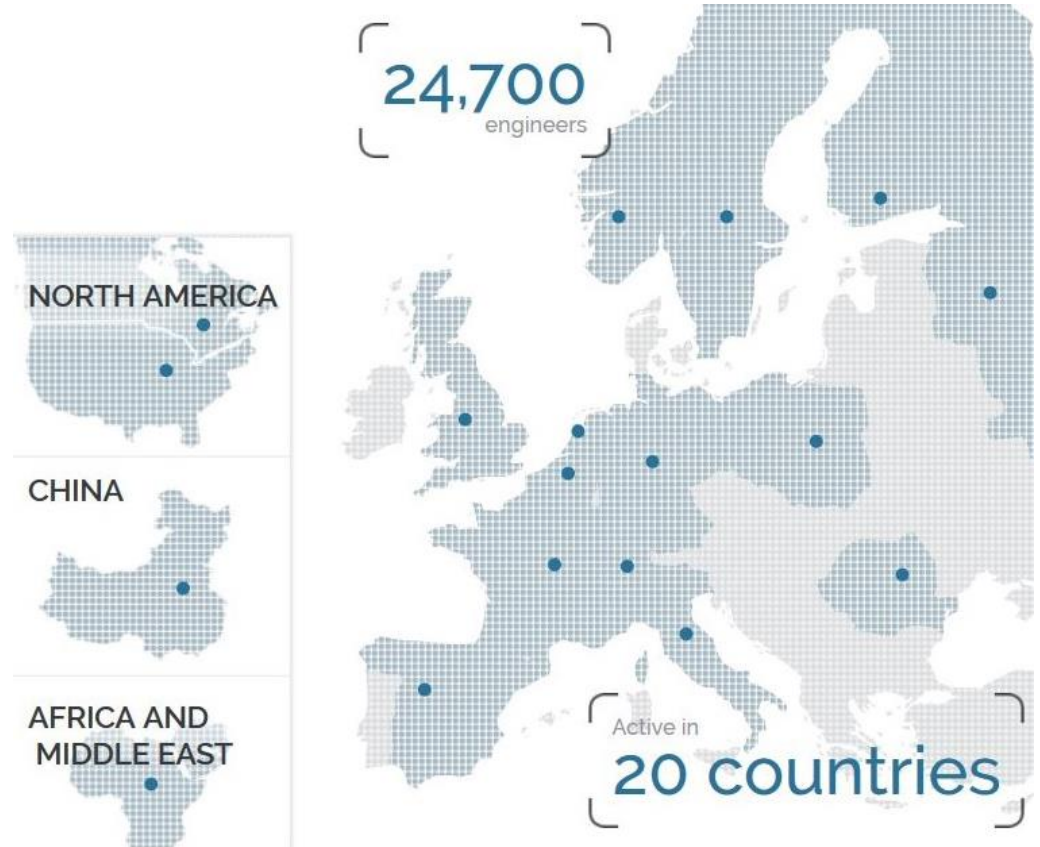
ALTEN Finlandilla työskentelee n. 450 henkilöä erilaisissa suunnittelutehtävissä. Tällä hetkellä ALTENilla on kymmenen toimipistettä ja uusien toimipisteiden avaaminen on suunnitteilla. ALTEN Finlandin tavoitteena on kasvattaa henkilöstömääräänsä 1 000 työntekijään vuoteen 2022 mennessä. (ALTEN Finland 2017c.)



Kuvio 3. ALTEN Finlandin toimistot (ALTEN Finland 2017c).

3.3.1 ALTEN kansainvälisesti

ALTENilla työskentelee kansainvälisesti yli 24 700 asiantuntijaa erilaisissa tehtävissä. Yrityksellä on toimintaa 20 maassa. ALTEN on perustettu vuonna 1988 ja yhtiön pääkonttori sijaitsee Pariisissa. Tällä hetkellä yhtiön toimitusjohtajana toimii Simon Azoulay. (ALTEN Group 2017b.)



Kuvio 4. ALTEN Group kansainvälisesti (ALTEN Group 2017a).

4 ISO/IEC 27001 -standardi

ISO/IEC 27001 on tietoturvallisuuden hallinnan riippumattomasti sertifioitava laatujärjestelmä. Kansainvälisen ISO/IEC 27001 -standardin mukainen sekä sertifioitu tietoturvallisuuden hallintajärjestelmä osoittaa, että organisaatio johtaa tietojensa turvaamista pitääkseen ne virheettöminä, hyvin suojattuna sekä helposti käytettävissä. ISO/IEC 27001 kertoo asiakkaille ja muille sidosryhmille tietoturvallisuudesta, organisaation panostuksesta riskien hallintaan ja luotettavuudesta yhteistyökumppanina. Standardi sisältää joukon tietoturvakontroleja, joilla voidaan varmistaa tietoturvallisuus organisaatiossa. ISO/IEC 27001:2013 -standardissa on 114 tietoturvakontrollia, jotka jakautuvat 14 eri osa-alueeseen. (Väestörekisterikeskus. 2018.)

4.1 Yleistä standardista

ISO/IEC 27001 on kansainvälisten ISO- ja IEC-standardisointiorganisaatioiden luoma standardi tietoturvallisuuden hallinnalle organisaatiossa. Tässä kansainvälisessä standardissa esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset. Tietoturvallisuuden hallintajärjestelmän käyttöönotto on organisaatiossa aina strateginen päätös. Tietoturvallisuuden hallintajärjestelmän luomiseen ja toteuttamiseen vaikuttavat organisaation tavoitteet ja tarpeet, turvallisuusvaatimukset, käytettävät prosessit sekä organisaation koko ja rakenne. (SFS-EN ISO/IEC 27001 2013.)

ISO/IEC 27001 on perheessä tunnetuin standardi, joka sisältää tietoturvallisuuden hallintajärjestelmän (ISMS) vaatimukset. Tietoturvallisuuden hallintajärjestelmä suojaa tiedon luottamuksellisuutta, eheyttä ja saatavuutta riskien hallintaprosessin avulla, sekä vahvistaa sidosryhmien luottamusta siihen, että riskejä hallitaan asianmukaisesti. (SFS-EN ISO/IEC 27001 2013.)

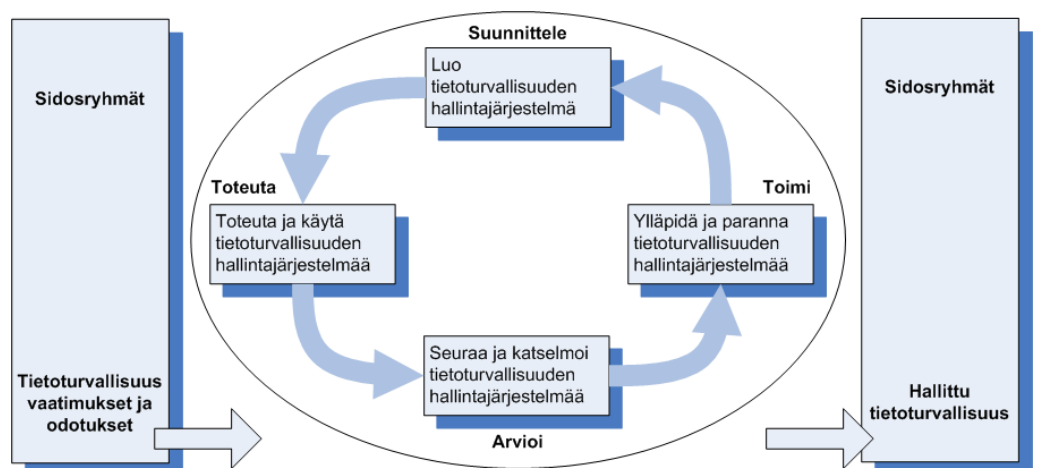
ISO/IEC 27001 -standardin tämänhetkinen tuorein versio on ISO/IEC 27001:2013, joka pohjautuu aiempaan ISO/IEC 27001:2006 -versioon. Tätä tuoreinta versiota käytetään tässä opinnäytetyössä. Tämän lisäksi tässä työssä viitataan vanhempaan versioon, koska se on tiedoiltaan laajempi.

4.2 Prosessimainen toimintamalli

ISO/IEC 27001 käyttää PDCA-mallia (plan-do-check-act). Tätä mallia kutsutaan myös jatkuvan kehittämisen malliksi, sillä ISMS:ää tarkastellaan säännöllisesti tätä mallia käyttämällä. Näin organisaatiossa voidaan varmistua, että tehdyt toimenpiteet ovat tehokkaita. (SFS-EN ISO/IEC 27001 2006.)

PDCA-malli on tarkoitettu sekä ISMS:in parannuksiin, että sen sertifiointitarkoituksiin. PDCA-malli koostuu neljästä vaiheesta: (SFS-EN ISO/IEC 27001 2006.)

- Suunnittele (Plan): Määrittele tietoturvapoliittikka, päämäärät, prosessit ja menettelytavat sekä tavoitteet, jotka ovat oleellisia riskien hallinnalle ja tietoturvallisuuden kehittämiseksi organisaation yleisten tavoitteiden ja politiikan mukaisesti.
- Toteuta (Do): Toteuta ja käytä tietoturvapoliittikkaa, turvamekanismeja, prosesseja ja menettelytapoja.
- Arvio (Check): Seuraa ja mittaa soveltuvien osien prosessien suorituskkyä, vertaa tuloksia tavoitteisiin, tietoturvapoliittikkaan ja käytännön kokemukseen sekä raportoi johdolle tuloksista.
- Toimi (Act): Ylläpidä tietoturvallisuuden hallintajärjestelmää sekä paranna sitä ryhtymällä korjaaviin ja ehkäiseviin toimenpiteisiin sisäisen tietoturvallisuuden hallintajärjestelmän auditoinnin ja johdon katselmusten tulosten tai muun olennaisen tiedon perusteella, jotta tietoturvallisuuden hallintajärjestelmää voidaan jatkuvasti kehittää.



Kuvio 5. PDCA-malli (Standardisoinnin oppilaitosportaali SFSedu 2018).

4.3 Tietoturvallisuuden hallintajärjestelmä

ISO/IEC 27001 -standardin olennainen osa on sellaisen tietoturvallisuuden hallintajärjestelmän luominen, jonka avulla varmistetaan ja toteutetaan tietojen luottamuksellisuus, käytettävyys ja eheys. Tietoturvallisuuden hallintajärjestelmällä pyritään takaamaan liiketoiminnan jatkumo sekä minimoimaan tietoturvahäiriöt ja niistä aiheutuvat seuraamukset. (SFS-EN ISO/IEC 27001 2006.)

Hallintajärjestelmän luomisessa sekä dokumentoinnissa on olennaista määritellä järjestelmän kattavuus ja rajat ottaen huomioon liiketoiminnan tarpeet sekä organisaation suojattaviin kohteisiin liittyvät erityispiirteet. Tietoturvallisuuden hallintajärjestelmä kattaa sopimukset sekä lainsäädännölliset ja hallinnolliset vaatimukset tietoturvalle. Hallintajärjestelmän pitää olla johdon hyväksymä. (SFS-EN ISO/IEC 27001 2006.)

Tietoturvallisuuden hallintajärjestelmässä on olennaista organisaation tietoturvapolitiikka ja -tavoitteet, riskien hallinnan menetelmät ja toimintatavat. Tietoturvallisuuden hallintajärjestelmä koostuu seuraavista dokumenteista: (SFS-EN ISO/IEC 27002 2017; Kuivalainen 2011.)

- Tietoturvapolitiikan dokumentointi, josta selviää tavoitteet, toteutustavat, vastuut, seuranta ja mahdolliset sanktiot.
- Tietoturvallisuuden hallinnan kattavuus.
- Hallintajärjestelmän prosessit, menetelmät ja turvamekanismit.
- Riskien hallinnan menettelytavat, suunnitelmat ja arviointi.
- Soveltamissuunnitelma.
- Dokumentointi, jonka avulla organisaatio varmistaa tietoturvaprosessien käytön, valvonnan ja suunnittelun.
- Raportti riskien hallinnasta ja arvioinnista.
- Viranomaisvaatimukset ja lait.

4.4 Johdon vastuut

Ylimmän johdon on osoitettava sitoutumisensa tietoturvallisuuden hallintajärjestelmään. Johdon on varmistettava, että laaditaan tietoturvapolitiikka ja asetetaan tietoturvatavoitteet. Johdon tulee myös varmistaa, että tietoturvatavoitteet ovat yhtenäiset organisaation strategian kanssa. Tämän lisäksi tulee huolehtia, että tietoturvallisuuden hallintajärjestelmän vaatimukset yhdistetään organisaation prosesseihin. Tarvittavien resurssien on oltava olemassa, jotta

hallintajärjestelmä toimii. Johdon on myös ohjattava työntekijöitään kehittämään tietoturvallisuuden hallintajärjestelmän eteenpäin ja antaa heille tarvittava tuki, jotta tämä onnistuu. Näin saadaan toteutettua hallintajärjestelmän jatkuva paraneminen. (SFS-EN ISO/IEC 27001 2013.)

Yrityksen ylimmän johdon on laadittava tietoturvapoliittikka, joka soveltuu organisaation toiminta-ajatukseen. Tietoturvapoliittikka sisältää annetut tavoitteet sekä sitoutumisen vaatimusten täytäntöön ja hallintajärjestelmän jatkuvaan parantamiseen. Tietoturvapoliittikan on oltava dokumentoitu ja koko organisaation tiedossa. Tarvittaessa myös sidosryhmillä on oikeus saada tietoturvapoliittikka nähtäville. (SFS-EN ISO/IEC 27001 2013.)

4.5 Sisäinen auditointi ja johdon katselmointi

Organisaation on tehtävä sisäisiä auditointeja säännöllisin väliajoin, jotta tiedetään toiminnan olevan standardin vaatimusten mukaista sekä organisaation omien tietoturvallisuuden hallintajärjestelmän vaatimuksia täyttävä. Katselmoinnissa selviää myös, onko hallintajärjestelmä toteutettu ja ylläpidetty annettujen vaatimusten mukaisesti. (SFS-EN ISO/IEC 27001 2013.)

Organisaation on laadittava, suunniteltava, toteutettava ja ylläpidettävä auditointiohjelmaa, jossa määritellään auditointien taajuus, vastuut, raportointi, menetelmät ja suunnitteluvaatimukset, sekä otettava huomioon aikaisempien auditointien tulokset. Auditointiin on valittava puolueettomat ja auditointiprosessin tuntevat henkilöt, jotta auditointikriteerit täyttyvät. Sisäisistä auditoinneista on raportoitava johdolle ja säilytettävä dokumentit todisteena organisaation auditointiohjelmasta ja sen tuloksista. (SFS-EN ISO/IEC 27001 2013.)

Ylimmän johdon on katselmoitava tietoturvallisuuden hallintajärjestelmää ja heidän on otettava siinä huomioon: (SFS-EN ISO/IEC 27001 2013.)

- Aikaisempien katselmusten käynnistettyjen toimenpiteiden tilanne
- Hallintajärjestelmän kannalta olennaisten ulkoisten ja sisäisten asioiden muutokset
- Poikkeamat ja niiden korjaavat toimenpiteet
- Seurannan ja mittauksen tulokset
- Auditointien tulokset
- Tietoturvatavoitteiden täyttyminen
- Sidosryhmien palaute

- Riskinkäsittelysuunnitelman tilanne sekä riskien arvioinnin tulokset
- Jatkuvan parantamisen tuomat mahdollisuudet.

4.6 Jatkuva parantaminen

Jatkuva parantaminen on tärkeä osa ISO/IEC 27001 -standardin mukaista toimintaa. Organisaation on parannettava tietoturvallisuuden hallintajärjestelmän riittävyttä, soveltavuutta ja vaikuttavuutta jatkuvasti. Kun organisaatiossa havaitaan poikkeama, siihen on reagoitava välittömästi ja tilanteesta riippuen ryhdyttävä korjaaviin toimiin ja käsiteltävä siitä aiheutuvat seuraukset. On arvioitava, tarvitseeko toimenpiteitä kehittää ja voidaanko kehittämällä poistaa poikkeaman syyt sen toistumisen estämiseksi. Dokumentoinnin on oltava ajan tasalla, jotta voidaan todentaa korjaavat toimenpiteet. (SFS-EN ISO/IEC 27001 2013.)

5 Hallintatavoitteiden ja –keinojen viiteluettelo

Hallintatavoitteiden ja –keinojen viiteluettelo on velvoittava liite ISO/IEC 27001 –standardissa. Organisaation on otettava tämä viiteluettelo huomioon. Hallintatavoitteet koostuvat 14 pääkohdasta ja 114 turvamekanismista. Hallintatavoitteiden osa-alueet on kuvattu seuraavissa alaluvuissa. (SFS-EN ISO/IEC 27001 2013.)

5.1 Tietoturvapoliitikat

Johdon ohjaus on tietoturvallisuutta koskevissa asioissa erittäin tärkeää. Johdon tulee tarjota ohjausta ja tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien asetusten ja lakien mukaisesti. Tietoturvallisuudelle on määriteltävä johdon hyväksymiä politiikkoja, jotka julkaistaan henkilökunnan ja asiaankuuluvien organisaation ulkopuolisten osapuolten käyttöön sekä joista tiedotetaan asiankuuluville tahoille. Tietoturvapoliitikat on katselmoitava suunnitelluin aikavälein tai kun tapahtuu merkittäviä muutoksia, jotta voidaan varmistua politiikkojen asianmukaisuudesta, vaikuttavuudesta ja soveltuvuudesta. (SFS-EN ISO/IEC 27001 2013.)

5.2 Tietoturvallisuuden organisointi

Tietoturvallisuuden organisoinnissa luodaan hallintarakenne, jolla aloitetaan tietoturvallisuuden käyttö ja toteuttaminen organisaatiossa. Tietoturvaroolit ja –vastuut on määriteltävä ja jaettava oikeiden henkilöiden kesken. Tehtävät on eriytettävä, jotta ristiriidassa olevien tehtävien ja vastuualueiden kanssa ei tule omaisuuden luvaton tai tahaton väärinkäyttöä. Organisaation on pidettävä jatkuvasti yhteyttä asiaankuuluviin viranomaisiin, osaamisyhteisöihin, turvallisuusasiantuntijaryhmiin sekä ammatillisiin järjestöihin. Organisaation projektinhallinnassa on käsiteltävä tietoturvallisuutta projektin tyypistä riippumatta. (SFS-EN ISO/IEC 27001 2013.)

5.3 Mobiililaitteet ja etätyö

5.3.1 Mobiililaitteet

Organisaatiossa on otettava käyttöön mobiililaitteiden politiikka ja sitä tukevat turvallisuuskäytännöt, joilla hallitaan mobiililaitteiden käytöstä syntyviä riskejä.

Mobiililaitteiden käytössä on noudatettava erityistä varovaisuutta, jotta pystytään estämään liiketoimintatietojen vaarantuminen. (SFS-EN ISO/IEC 27002 2017.)

Mobiililaitteiden politiikassa tulisi ottaa huomioon riskit, jotka aiheutuvat mobiililaitteilla työskentelemisestä suojaamattomissa ympäristöissä. Mobiililaitteita koskevassa politiikassa tulisi käsitellä seuraavat asiat: (SFS-EN ISO/IEC 27002 2017.)

- Mobiililaitteiden rekisteröinti
- Fyysinen suojaus
- Ohjelmistojen asentamisen rajoitus
- Ohjelmistojen versioiden vaatimus ja päivitysten asennus
- Rajoitukset tietojenkäsittelypalveluihin
- Pääsynhallinta
- Salaustekniikka
- Haittaohjelmilta suojautuminen
- Etäsammutus, -poistaminen tai -lukitseminen
- Varmuuskopiointi
- Verkkopalveluiden ja -sovellusten käyttö.

Mobiililaitetta käyttävälle henkilökunnalle tulisi järjestää koulutusta ja kertoa mahdollisista hallintakeinoista sekä opastaa heidät mobiililaitteen turvalliseen käyttöön. Mobiilipolitiikassa on myös otettava kantaa siihen, sallitaanko henkilökohtaisten laitteiden käyttö yrityksen verkossa. (SFS-EN ISO/IEC 27002 2017.)

5.3.2 Etätyö

Etätyössä tulee ottaa käyttöön politiikka ja sitä tukevat turvallisuuskäytännöt, joilla suojataan etätyöpaikalla käsiteltyä, käytettyä tai säilytettyä tietoa. Etätyöpolitiikassa tulee määritellä etätyötä koskevat ehdot ja rajoitukset. Seuraavat asiat tulisi ottaa huomioon siltä osin kuin ne katsotaan soveltuviksi ja ovat lain mukaisia: (SFS-EN ISO/IEC 27002 2017.)

- Etätyöpaikan fyysinen turvallisuus ja ympäristö
- Tietoliikenteen turvallisuusvaatimukset, ottaen huomioon organisaation sisäisten järjestelmien etäkäyttötarve, arkaluonteisuus sekä siirrettävien tietojen arkaluonteisuus

- Pääsy virtuaalityöpöydälle, joka estää henkilökohtaisissa laitteissa tiedon käsittelyn sekä sen tiedon tallentamisen niihin
- Muiden henkilöiden aiheuttama tiedon luvaton käyttö ja aiheuttama uhka
- Kotiverkon käyttöä ja langattoman verkkopalveluiden konfiguraatioita koskevat vaatimukset ja rajoitukset
- Poliitiikat ja menettelyt, joilla otetaan kantaa ja ehkäistään henkilökohtaisella laitteella kehitetyn aineettoman omaisuuden oikeuksia koskevat kiistat
- Pääsy henkilökohtaisiin laitteisiin
- Ohjelmistolisenssisopimukset, jonka mukaan organisaatiot saattavat olla vastuussa asiakasohjelmistolisensseistä, jotka ovat työntekijöiden tai ulkopuolisten käyttäjien henkilökohtaisesti omistamissa työasemissa
- Haittaohjelmilta suojautumista ja palomuuria koskevat vaatimukset.

5.4 Henkilöstöturvallisuus

Henkilöturvallisuuden tavoitteena on varmistaa, että organisaatiossa työntekijät, vuokratyöntekijät ja ulkoiset sidosryhmät ymmärtävät vastuunsa organisaation tietoturvallisuudesta koko heidän työ- tai palvelussuhteen elinkaaren ajan. Kaikkien työnhakijoiden taustat olisi tarkastettava määräysten ja eettisten normien sekä asianmukaisen lainsäädännön mukaan. Tarkistukset tulee suhteuttaa liiketoiminnallisiin vaatimuksiin, käsiteltävän tiedon luokituksen ja oletettujen riskien mukaan. Taustatarkistuksissa on otettava huomioon tietosuojaan, henkilötietojen suojaamiseen ja työsuhteisiin liittyvä lainsäädäntö. Seuraavat asiat olisi sisällytettävä mukaan, jos ne ovat sallittuja: (SFS-EN ISO/IEC 27002 2017.)

- Riittävä henkilösuositusten saatavuus
- Hakijan ansioluettelon täydellisyys ja oikeellisuuden tarkistaminen
- Väitetyt koulutuksen ja ammatillisen pätevyyden tarkistaminen
- Henkilöllisyyden tarkistaminen (passi tai muu vastaava asiakirja)
- Yksityiskohtaisempi tarkistus, kuten rikosrekisterin ja luottotietojen tarkistus.

Mikäli työtehtävät sisältävät käyttöoikeuksia tietojenkäsittelypalveluihin tai arkaluonteisten tietojen käsittelyyn, tulisi organisaation harkita yksityiskohtaisempia lisätarkistuksia kyseiselle henkilölle. Organisaatiossa olisi määriteltävä taustatarkistuksen rajoitukset ja kriteerit, esim. kenellä organisaatiossa on oikeus tehdä taustatarkistuksia ja tarkistaa ihmisten tietoja sekä milloin, miten ja miksi taustatarkistuksia tehdään. Kyseisen prosessin tulee olla sellainen, että

sitä voidaan käyttää myös vuokratyöhenkilöiden taustojen tarkistukseen. (SFS-EN ISO/IEC 27002 2017.)

Organisaation johdon on varmistettava, että työntekijät ja vuokratyöntekijät saavat asianmukaista tietoturvaopastusta ja -koulutusta sekä säännöllistä päivitystä heidän saamiinsa tietoihin. Organisaatiossa tulee olla myös muodollinen ja tietoinen kurinpitoprosessi, minkä perusteella toimitaan työntekijän syylistyessä tietoturvarikkomukseen. Työsuhteen päättyessä tai työntekijän vastuun muuttuessa on organisaatiossa määriteltävä tietoturvavastuut ja -velvollisuudet, jotka jäävät voimaan työsuhteen päättymisen tai muuttumisen jälkeen. Näistä kaikista on tiedotettava ja varmistettava, että niitä noudatetaan. (SFS-EN ISO/IEC 27002 2017.)

5.5 Suojattavan omaisuuden hallinta

Tietoon tai tietojenkäsittelypalveluihin liittyvä omaisuus on suojattava ja yksilöitävä organisaatiossa. Suojattava omaisuus on luetteloitava ja luetteloa on ylläpidettävä säännöllisesti. Omaisuusluettelolla tulee olla omistaja, joka vastaa sen ylläpidosta ja hallinnasta. Suojattavan omaisuuden hyväksyttävä käyttö sekä omaisuuteen liittyvät säännöt on yksilöitävä, toteutettava ja dokumentoitava. Kaikkien työntekijöiden sekä organisaation ulkopuolisten käyttäjien on palautettava kaikki hallussaan oleva organisaation omaisuus työtehtävän, työsuhteen tai sopimuksen päättyessä. Organisaatiossa on varmistettava, että tiedon suojaustaso on riittävä. Suojaustaso määräytyy sen mukaan, kuinka merkittävää tieto on. Tieto on luokiteltava lakisääteisten vaatimusten, kriittisyyden ja tiedon arvon mukaan. Fyysiset tietovälineet on suojattava luvottomalta pääsylvä, väärinkäytöltä sekä turmeltumiselta. (SFS-EN ISO/IEC 27001 2013.)

5.6 Pääsynhallinta

Organisaatiossa on laadittava pääsynhallintapolitiikka, joka on dokumentoitava ja katselmoitava liiketoiminnallisten vaatimusten perusteella. Suojattavan omaisuuden omistajien on määriteltävä asianmukaiset pääsynhallintasäännöt, pääsyoikeudet ja rajoitukset käyttäjärooleille koskien heidän suojattavaa omaisuuttaan. Pääsynhallintakeinot ovat fyysisiä sekä loogisia. Pääsynhallinnassa lähestymismallina käytetään rooliperustaista pääsynhallintaa, jolla saa yhdistettyä onnistuneesti pääsyoikeudet liiketoimintarooleihin. (SFS-EN ISO/IEC 27001 2013; SFS-EN ISO/IEC 27002 2017.)

Käyttäjille on sallittava pääsy vain niihin verkkoihin ja verkkopalveluihin, joihin heille on nimenomaisesti myönnetty pääsyoikeudet. Ylläpito-oikeuksien jakamista ja käyttöä on valvottava ja rajoitettava. Kaikkien käyttäjien on pidettävä huolta omien tunnistautumistietojensa turvallisuudesta organisaation käytännön mukaisesti. Salasanojen hallintajärjestelmän on oltava vuorovaikutteinen ja sen on edellytettävä vahvojen salasanojen käyttöä. Pääsyoikeudet on poistettava, kun työntekijän työtehtävä, työsuhde tai sopimus päättyy. Pääsyoikeudet on katselmoitava säännöllisin väliajoin sekä dokumentoitava. (SFS-EN ISO/IEC 27001 2013; SFS-EN ISO/IEC 27002 2017.)

5.7 Salaus

Salauksen hallinnasta on laadittava ja toteutettava politiikka, jota noudatetaan, kun tietoa suojataan salauksen avulla. Politiikassa tulisi ottaa kantaa salauksen hallintakeinojen käytöstä koko organisaatiossa, mobiililaitteiden tai siirrettävien tietovälineiden arkaluonteisen tiedon salaamisesta, kuinka salausavainten hallinta on järjestetty sekä kuinka toimia, kun salausavaimet vaarantuvat, vaurioituvat tai katoavat. Tätä politiikkaa on noudatettava koko käyttöiän ajan. (SFS-EN ISO/IEC 27001 2013.)

5.8 Fyysinen turvallisuus ja ympäristön turvallisuus

Standardissa fyysinen turvallisuus ja ympäristön turvallisuus jakaantuvat kahteen osa-alueeseen: toimitilojen ja turva-alueiden fyysinen suojaus sekä laitteistojen turvallisuus. Näiden tarkoituksena on estää luvaton pääsy yrityksen toimitiloihin ja tietoihin sekä estää vahingoittuminen ja häiriintyminen. Tämän lisäksi pyrkimyksenä on estää fyysisen omaisuuden vahingoittuminen, varastaminen, häviäminen tai muu vaarantuminen. (SFS-EN ISO/IEC 27001 2013.)

Organisaation tulee suojata toimitilansa valvonnalla ja pääsynhallinnalla sekä varmistaa, että organisaatiossa on varauduttu ympäristöstä aiheutuviin mahdollisiin uhkiin. Ympäristöstä aiheutuvia uhkia ovat esim. luonnonilmiöistä aiheutuvat seuraamukset. Valvonnan ja pääsynhallinnan puolelta konkreettisia esimerkkejä ovat kulunvalvonnan sekä videovalvonnan toteutukset. (Miettinen 2002, 91-100.)

Laiteturvallisuuden puolella standardissa määritellään organisaatiolle käytännöt, joilla suojataan tietojenkäsittelyyn liittyvät laitteistot. Laitteistoa tulee huoltaa säännöllisesti käytettävyyden ja eheyden turvaamiseksi. Laitteistot tulee

sijoittaa suojattuun tilaan, jotta laitteisiin ei kohdistu väärinkäytöksiä, vaurioita tai salakuuntelua. Laitteet tulee suojata sähkökatkoilta ja muilta peruspalveluiden vikojen aiheuttamilta häiriöiltä sekä varmistaa, että varavirtalähteet toimivat moitteettomasti. Tietotekniikkapalveluita tukeva tietoliikennekaapelointi tulisi suojata salakuuntelulta, häirinnältä ja vahingoittumiselta. Laiteturvallisuuden avulla suojataan toimitilojen ulkopuolella olevat laitteet sekä tiedot. Laiteturvallisuudella varmistetaan, että käytöstä poistettavista laitteista tuhotaan kaikki suojattava tieto, materiaali tuhotaan fyysisesti tai tieto poistetaan, tuhoaan tai päällekirjoitetaan käyttäen tekniikoita, jotka estävät alkuperäisen tiedon palauttamisen. (SFS-EN ISO/IEC 27001 2013.)

5.9 Käyttöturvallisuus

Käyttöturvallisuudessa laaditaan toimintaohjeet tietokoneiden käynnistys- ja sammutusmenettelyä, tiedonvarmistusta, tietovälineiden käsittelyä, laitteiden huoltoa sekä tietokonehuoneen turvallisuutta ja hallintaa varten. Käyttöturvallisuuden toimintaohjeet on dokumentoitava ja niiden pitää olla kaikkien käyttäjien saatavilla tarvittaessa. (SFS-EN ISO/IEC 27001 2013.)

Muutostenhallinnassa on tärkeää olla prosessi, jossa muutokset tunnistetaan, testataan ja suunnitellaan tietoturva vaikutukset huomioiden. Tämän lisäksi tulee olla muutoslokien automaattinen tallennus, jotta yksityiskohtainen tieto tehdyistä muutoksista olisi saatavilla. Kapasiteetin hallinnassa resurssien käyttöä tulee seurata ja säätää, jotta voidaan varmistaa järjestelmien suorituskyky. Kapasiteettivaatimukset tulee yksilöidä ja ottaa myös huomioon kyseisen järjestelmän kriittisyys liiketoiminnan kannalta. Kehitys-, testaus- ja tuotantoympäristöt tulee erottaa toisistaan, jotta tuotantoympäristön luvaton käyttö estetään. (SFS-EN ISO/IEC 27001 2013.)

Haittaohjelmilta suojautumisen on perustuttava haittaohjelmien havaitsemis- ja korjausohjelmistoihin, tietoturvatietoisuuteen, tehokkaaseen muutosten hallintaan ja järjestelmiin pääsyn riittävään valvontaan. Yrityksen tulisi laatia muodollinen politiikka, jossa kielletään luvattomien ohjelmistojen käyttö ja toteutetaan hallintakeinot. Nämä hallintakeinot estävät tai havaitsevat tiettyjen tai epäiltyjen haitallisten verkkosivustojen käytön. (SFS-EN ISO/IEC 27001 2013.)

Tietojen varmuuskopiointi tulee suorittaa tiedoista, ohjelmistoista ja järjestelmistä säännöllisesti. Tapahtumien kirjaamisen on oltava käytössä ja niistä syntyvät lokitiedot on säilytettävä ja niiden katselmointi on suoritettava säännöllisesti. Kaikki lokitiedot on suojattava peukaloimiselta ja luvaton pääsy lokitietoihin on estettävä. Järjestelmän pääkäyttäjien ja operaattorien toiminnasta on oltava lokitiedot tallessa ja nämä lokit on suojattava ja katselmoitava, jotta pääkäyttäjäoikeuksilla toimivan vastuu kyetään säilyttämään. (SFS-EN ISO/IEC 27001 2013.)

5.10 Viestintäturvallisuus

Viestintäturvallisuuden tehtävänä on varmistaa, että verkossa kulkeva tieto on suojattua. Verkkoja on valvottava ja hallittava, jotta järjestelmissä liikkuva tieto on varmasti suojattua. Verkkopalvelut on dokumentoitava ja niihin on yksilöitävä turvamekanismit, palvelutaso ja hallintavaatimukset. Nämä tiedot on säilytettävä riippumatta siitä, tuotetaanko palvelut organisaation sisällä vai onko ne ulkoistettu. Organisaatiossa tiedonsuojaustarpeita kuvastavat salassapito- ja vaitiolositoumuksien vaatimukset on katselmoitava säännöllisesti, dokumentoitava ja yksilöitävä. (SFS-EN ISO/IEC 27001 2013.)

5.11 Järjestelmien hankkiminen, kehittäminen ja ylläpito

Tietojärjestelmien turvallisuusvaatimukset ovat olennainen osa niiden koko elinkaaren ajan. Tietoturva-vaatimukset tulee yksilöidä erilaisilla menetelmillä, kuten johtamalla vaatimustenmukaisuusvaatimukset politiikoista ja säännöksistä, uhkamallinnuksella, häiriökatselmuksilla tai haavoittuvuuskynnyksiä käyttämällä. Niiden tulokset tulee dokumentoida ja kaikkien sidosryhmien tulee katselmoida ne. Järjestelmiin tehtävät kehitykset ja muutokset niiden elinkaaren aikana on tehtävä muodollisella muutoksenhallinnan menettelyllä. (SFS-EN ISO/IEC 27001 2013.)

Liiketoiminnan kannalta kriittiset sovellukset on testattava ja tarkistettava, jotta varmistetaan, ettei muutoksilla ole saatua aikaan haitallisia vaikutuksia organisaation toimintaan tai turvallisuuteen. Ohjelmistopaketteihin tehtäviä muutoksia tulee välttää ja ne on rajoitettava vain välttämättömiin muutoksiin, minkä vuoksi kaikkia muutoksia on hallittava tarkasti. (SFS-EN ISO/IEC 27001 2013.)

5.12 Suhteet toimittajiin

Organisaatiossa tulee määrittää ja yksilöidä tietoturvallisuuden hallintakeinot, joissa käsitellään toimittajien pääsyä käsiksi organisaation tietoihin. Näissä hallintakeinoissa tulee ottaa kantaa prosesseihin ja menettelyihin, joita toimittaja tulee tekemään. Toimittajan riittämätön tietoturvallisuuden hallinta saattaa altistaa tiedot riskeille. Näin ollen on syytä tunnistaa ja ottaa käyttöön hallintakeinot, joilla valvotaan toimittajan pääsyä tietojenkäsittelypalveluihin. Toimittajasopimukset on laadittava ja dokumentoitava. Sen tarkoituksena on varmistaa, että organisaation ja toimittajan välillä ei ole väärinymmärrystä ja että osapuolet on velvoitettu täyttämään tietoturva-vaatimukset. (SFS-EN ISO/IEC 27001 2013.)

5.13 Tietoturvahäiriöiden hallinta

Tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinnassa on oltava toimintamalli, joka on johdonmukainen, vaikuttava ja johon sisältyy viestiminen tietoturvatapahtumista ja –heikkouksista. Tietoturvahäiriöiden hallinnan tavoitteista tulee sopia johdon kanssa. Hallinnasta vastaavien henkilöiden on varmistettava, että he ymmärtävät organisaation prioriteetit tietoturvahäiriöiden käsittelyssä. (SFS-EN ISO/IEC 27002 2017.)

Tietoturvatapahtumista on raportoitava mahdollisimman nopeasti asiankuuluvaa hallintokanavaa käyttäen. Kaikkien työntekijöiden sekä vuokratyöntekijöiden on oltava tietoisia velvollisuudestaan raportoida tietoturvatapahtumista mahdollisimman pian. Heidän on myös tunnettava, kuinka toimia, menetellä ja raportoida tietoturvatapahtumista. (SFS-EN ISO/IEC 27002 2017.)

Tietoturvatapahtumia varten on oltava yhteydenottopiste, jossa arvioidaan ja luokitellaan kukin tietoturvatapahtuma tapauskohtaisesti sekä päätetään toimenpiteet. Häiriöiden luokittelulla ja priorisoinnilla voidaan edesauttaa häiriön vaikutuksen ja laajuuden selvittämistä. Häiriöihin vastaamisen tärkein tapahtuma on normaaliin turvallisuustasoon palautuminen sekä tarvittavien palautustoimien käynnistäminen. Tietoturvahäiriöistä tulee tehdä analysointi ja ratkaisusta saatua tietoa tulee käyttää ja hyödyntää tulevien häiriöiden vähentämisessä sekä vaikutusten pienentämisessä. (SFS-EN ISO/IEC 27002 2017.)

5.14 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia

Liiketoiminnan jatkuvuuden hallintajärjestelmiin on sisällytettävä tietoturvallisuuden jatkuvuus. Organisaatiossa on dokumentoitava, laadittava, toteutettava ja ylläpidettävä prosesseja, menettelyjä ja hallintamekanismeja, joilla pystytään varmistamaan tietoturvallisuuden jatkuvuuden vaaditun tason säilyvyys kaikissa tilanteissa. Tietoturvallisuuden jatkuvuuden prosesseja ja toimintoja on katselmoitava säännöllisesti, jotta voidaan varmistaa niiden pätevyys ja säilyttää jatkuvuuden taso. (SFS-EN ISO/IEC 27001 2013.)

5.15 Vaatimustenmukaisuus

Organisaatiossa tulee noudattaa asiaan kuuluvia, tietoturvallisuuteen liittyviä lakeja sekä viranomaisten ja sopimusten asettamia vaatimuksia. Organisaation on otettava huomioon ja toteutettava asianmukaiset toiminnot immateriaalioikeuksiin ja tekijänoikeuksiin suojattujen ohjelmistotuotteiden käytöstä. Talenteet tulee suojata katoamiselta, tuhoutumiselta, luvattomalta käytöltä, värentämiseltä sekä luvattomalta levittämiseltä liiketoiminnan asettamien vaatimusten mukaisesti. Tietosuoja- ja henkilötietojen suojaaminen on varmistettava annettujen lakien ja viranomaisten asettamien vaatimusten mukaisesti. (SFS-EN ISO/IEC 27002 2017.)

Tietoturvallisuuden katselmoinnit on tehtävä esimiesten toimesta säännöllisesti, jotta pystytään varmistamaan organisaation tietoturvallisuuden hallinnan tehokkuus, riittävyys ja sopivuus. Katselmoinneista saadut tulokset on dokumentoitava, tallennettava ja raportoitava johdolle. (SFS-EN ISO/IEC 27002 2017.)

6 Sertifiointi

ISO/IEC 27001 -sertifiointi on menettely, jossa puolueeton ja riippumaton kolmas taho antaa kirjallisen varmistuksen siitä, että menetelmä, palvelut tai tuote on määriteltyjen vaatimusten mukainen. Sertifiointissa tehdään kansainvälisten ja kansallisten standardien ja vaatimustenmukaisuuden arviointia. Suomessa sertifiointia tarjoaa Suomen mittaustekniikan keskuksen alaisen FINASin (Finnish Accreditation Service) akreditoimat yritykset. Näitä ovat Inspecta, Bureau Veritas, Nixu Certification Oy, VTT Expert Services ja 3 STEP IT. (Kuivalainen 2011.)

6.1 Sertifiointiprosessi

ISO/IEC 27001 -standardissa, kuten muissakin ISO-standardeissa, sertifiointiprosessi alkaa sertifiointihakemuksella sitä tuottavalle taholle. Prosessissa on kuusi kohtaa, jotka käydään alla lävitse. (Kuivalainen 2011.)

6.1.1 Sertifiointihakemus

Sertifiointihakemuksessa kuvataan sen organisaation toimintaa, jolle tullaan hakemaan sertifikaattia mahdollisin rajauksin. Hakemuksesta tulee selvittää perustiedot organisaatiosta, mahdolliset aikaisemmat sertifiointit, prosessit sekä organisaatiota koskevat määräykset, asetukset ja lait. (Kuivalainen 2011.)

6.1.2 Suunnittelukokous

Hakemusta seuraava vaihe sertifiointiprosessissa on suunnittelukokous yhdessä sertifioijan kanssa. Suunnittelukokouksessa käydään lävitse tietoturvalisuuruden tai laadun hallintajärjestelmän dokumentaatio kokonaisuudessaan. Hallintajärjestelmän materiaalit on annettava sertifioijalle tutustumista varten ennen suunnittelukokousta. Kokouksessa selvitetään sertifioitavan järjestelmän rajaukset ja kattavuus sekä siihen liittyvät toimipaikat ja prosessit. Kokouksessa arvioidaan myös katselmusten ja sisäisten auditointien tilanne ja käytännöt. (Kuivalainen 2011.)

6.1.3 Ennakkoarviointi

Ennakkoarviointi on organisaatiolle vapaaehtoinen. Se toteutetaan samalla tavalla kuin sertifiointiarvio, mutta suppeampana. Arviointi määritellään organisaation ja sertifioidijan välillä yhdessä. Ennakkoarvioinnissa löydettyjen ja todennettujen poikkeamien korjaavia toimenpiteitä ei sertifioidijalle tarvitse lähettää. Ennakkoarviointi on organisaatiolle harjoitus varsinaiseen sertifiointiin. Organisaatio saa samalla kuvan siitä, mitkä ovat sen valmiudet saavuttaa sertifikaatti. (Kuivalainen 2011.)

6.1.4 Sertifiointiarviointi

Sertifiointiarviointi suoritetaan etukäteen tehdyn arviointiohjelman mukaan. Arvioinnin ideologiana on saada tarvittava näyttö siitä, että organisaation toiminta vastaa standardin vaatimuksia sekä hallintajärjestelmän kuvauksia. Sertifiointin päätteeksi todetaan arvioinnin tulos organisaation hallintajärjestelmästä. Sertifiointin arviosta vastuussa oleva arvioija kertoo arvion tulokset ja voidaanko sertifikaatin myöntämisestä suositella organisaatiolle vai tarvitaanko korjaavia toimenpiteitä tai uusinta-arviota. Organisaatio saa arvioinnista kirjallisen arviointiselosteen ja poikkeamaraportin. (Kuivalainen 2011.)

Poikkeamat luokitellaan lieviin ja vakaviin. Vakavia poikkeamia ovat:

- standardin edellyttämä oleellinen asia puuttuu tai on kuvaamatta
- järjestelmä on keskeneräinen
- jossakin toiminnossa on liian monta lievää poikkeamaa.

Yksittäiset puutteet toiminnassa tai menettelyssä ovat lieviä poikkeamia. (Kuivalainen 2011.)

Organisaation tulee lähettää sertifioidijalle selvitys poikkeamien korjaavista toimenpiteistä määräajan kuluessa. Määräaika sovitaan samalla kun arviointiraportti luovutetaan. Korjaavista toimenpiteistä tulee toimittaa raportti sertifioidijalle ja sen tulee sisältää seuraavat asiat: (Kuivalainen 2011.)

- Mitä asioita on korjattu ja muutettu.
- Kuinka ohjeita on muutettu ja ohjeistettu.
- Milloin muutokset tulevat voimaan.
- Kuinka muutoksista on tiedotettu.
- Mitkä korvaavat toimenpiteet estävät poikkeaman uusiutumisen.
- Milloin ja ketkä ovat korjaukset ja muutoksien toteutumisen tarkistaneet.

Sertifioija tarkistaa korjaavien toimenpiteiden toteutumisen. Tarkastaminen tehdään korjaavien toimenpiteiden luonteesta riippuen saadun kirjallisen raportin perusteella tai uusinta-arvioinnin yhteydessä. (Kuivalainen 2011.)

6.1.5 Uusinta-arviointi

Vakavien poikkeamien korjaavien toimenpiteiden todentamiseksi tehdään uusinta-arviointi. Arvioinnissa arvioidaan korjaavien toimenpiteiden tehokkuus ja toteutuminen sekä ne järjestelmä osat, joihin muutokset ovat saattaneet vaikuttaa. Uusinta-arviointi tehdään laajempänä, jos järjestelmä on todettu keskeiseksi. (Kuivalainen 2011.)

6.1.6 Seuranta-arvioinnit

Sertifikaatin myöntämisen jälkeen suoritetaan seuranta-arviointeja vähintään kerran vuodessa ja niissä arvioidaan järjestelmän kriittisemmät muutokset ja kohteet. Ensimmäinen seuranta-arviointi tehdään 12 kuukauden kuluttua sertifiointiarvioinnista. Seurantoja on mahdollista tehdä myös kaksi kertaa vuodessa ja tämän sisältö on sovittava organisaation kanssa vuosittain. Ensimmäinen seuranta tehdään tällöin 6 kuukauden kuluttua sertifiointiarvioinnista. (Kuivalainen 2011.)

Jatkuvassa seuranta-arvioinnissa sovitaan organisaation kanssa vuosittain arvioinnin sisältö. Tämä malli sopii erityisesti isoille organisaatiolle, jolloin saadaan arviointikäynnit kohtuullisen kokoisiksi yhdellä kertaa. Seuranta-arvioinnin ajankohdat sovitaan organisaation kanssa etukäteen. Seuranta-arvioinnista raportoidaan normaalin käytännön mukaan, kuten sertifiointiarviossa. Jos raportissa todetaan vakava poikkeama, se käsitellään tapauskohtaisesti ja siitä tehdään päätös. Päätös voi olla sertifikaatin määräaikainen peruutus, kokonaan peruuttaminen tai uusinta-arvio. (Kuivalainen 2011.)

7 ALTEN Finlandin tilanne

ALTEN Finlandin lähtökohdat ja tavoitteet ISO/IEC 27001 -standardin ja tietoturvallisuuden hallintajärjestelmän käyttöönotolle on tuonut asiakkaiden vaatimukset ottaa standardi käyttöön. Suuremmat asiakkaat ovat alkaneet edellyttää yhteistyökumppaneiltaan tietoturvallisuuden osoittamista sertifiointin kautta. Sertifiointi on puolueeton tapa osoittaa yhteistyökumppaneille tietoturvan toteutuminen ja tuo kasvavassa kilpalutilanteessa etulyöntiaseman yritykselle.

ALTEN Finland kehittyä ja vastuualueet määritellään entistä tiiviimmin. Palveluja ja resursseja on taloushallinnossa, IT-osastolla, henkilöstöhallinnossa sekä sisäisellä oikeudellisella osastolla. GDPR-projekti on osaltaan vienyt eri osa-alueita eteenpäin. Tietosuojakoordinaattori sekä valittu tietosuojatyöryhmä vastaavat aihealueen kehittämisestä. ISO 9001 -sertifikaatti on myönnetty ja seuraavana askeleena on keskittyä IT:n ja ISO 27001:n tuomiin asioihin.

ALTEN Finlandin hallinto- ja manageri-tason henkilöstölle tehtiin kysely, jossa kyselylomakkeen perusteella selvitettiin ISO/IEC 27001 -standardin tuntemusta, yleistä tietoa tietoturvasta ALTENilla sekä pyydettiin antamaan kehitysehdotuksia.

8 Kysely

ALTEN Finlandilla suoritettiin kysely tietoturvan tilanteesta hallinnon, keskijohdon ja johdon kesken. Kysely suoritettiin avoimena kyselytutkimuksena sähköpostitse. Kyselyn tarkoituksena oli selvittää johdon ja hallinnon tuntemusta tietoturvakäytännöistä ALTEN Finlandilla.

8.1 Kyselyn yhteenveto

Tietoturva ALTEN Finlandilla on jäänyt pienempään rooliin kuin muu IT-kehitys. Yrityksellä ei ole olemassa selkeästi ymmärrettävää tietoturvapoliittikkaa eikä ohjeistusta. Kyselyn perusteella hallinnon ja johdon tieto ja ymmärrys tietoturvasta on kohtalainen.

Kyselyn vastausprosentti oli 40 %. Vastausprosentin alhaiseen tasoon vaikutti se, että kysely suoritettiin juuri kesälomakauden kynnyksellä. Vastaamiseen saattoi myös vaikuttaa se, että kolme yritystä fuusioitui vuonna 2017 muodostaen ALTEN Finlandin ja toimintatavat näissä yrityksissä ovat olleet erilaiset. Vastauksia saatiin pääasiassa Hyvinkään ja Espoon konttoreilta. Kyselyn otanta oli 35 henkilöä, joista kyselyyn vastasi 14 henkilöä.

8.2 ALTEN Finlandin kehityskohteet

ALTEN Finlandilla tulisi harkita erilaisten standardien toteuttamista yhtiön koon ja toiminnan kasvaessa. Yrityksen tavoitteena on päästä asiakkaiden avaintoimittajaksi ja kasvattaa allokoitavan asiakastyön osuutta. Tällaisten asiakassuhteiden luominen voi jatkossa edellyttää yhä enemmän standardein osoitettavaa luotettavuutta. Standardeilla olisi positiivinen vaikutus jo olemassa olevien asiakassuhteiden syventämiseen sekä uusien asiakassuhteiden luomiseen. Standardi yhdenmukaistaisi sopimuksia ja niiden hankitaan liittyviä toimenpiteitä, toisi kilpailuetua ja antaisi hyvän merkin luotettavuudesta. Tietoturvallisuuden hallintajärjestelmän sekä prosessien kehittäminen toisi selkeyttä työtehtävien hoitamista varten henkilöstön osalta. Näin henkilöstöllä olisi selkeät toimintatavat ja ohjeet toimia, ja tehokkuus ja laatu paranisivat.

Yhtiössä tulisi kehittää yleisiä tietoturvakoulutuksia ja -ohjeita henkilöstölle. Yleisesti ottaen tietoturvaan pitäisi keskittyä enemmän sekä järjestää vuosittainen tietoturvakoulutus henkilöstölle. IT-henkilöstöllä tulisi olla selkeät vastuut

ja roolit tietoturvan hallinnassa. Tällä hetkellä kaikki IT-henkilöt toimivat tietoturvan piirissä ja näin ollen IT-osaston ohjeistus ei ole kunnollinen ja ajan tasalla. Yrityksellä tulisi olla tietoturvapääällikkö, joka vastaa tietoturvaprosessien kehittämisestä ja niiden jalkauttamisesta ALTEN Finlandilla.

ALTEN Finlandilla uuden työntekijän perehdytyksessä painotetaan tällä hetkellä salassapitovelvoitteita, salassapitositoumuksia ja luottamuksellisen tiedon ja materiaalin säilyttämistä. Näistä asioista tulisi kouluttaa henkilöstöä yleisesti säännöllisin väliajoin. Myös mahdollisuutta taustatietojen perusmuotoiseen tarkistukseen Suojelupoliisin kautta tulisi harkita.

ALTEN Finlandilla tulisi panostaa riskienhallintaan ja laadun tarkkailuun. Näillä toiminnoilla pitäisi olla oma vastuhenkilö. ALTEN Finlandilla tulisi kehittää laadun toimintoja ja siihen liittyviä prosesseja, sekä ottaa huomioon ISO 9001 –standardin vaatimukset päivittäisissä toiminnoissa.

8.3 Pohdinta ja jatkotoimenpiteet ALTEN Finlandille

Kansainvälinen standardi ISO/IEC 27001 tarjoaa organisaatiolle kattavat menetelmät tietoturvallisuuden hallintaan. Standardin avulla organisaatiot voivat varmistaa tietoturvallisuuden hallittavuuden ja toteutumisen kaikkien sidosryhmien kesken ja tietojen vaihdossa. ISO/IEC 27001 -standardi on kattava tietoturvallisuuden hallintaan keskittyvä standardi, joka vaatii organisaatiolta jatkuvaa sitoutumista sekä panostusta tietoturvan hallintaan.

Itse standardin käyttöönotto voi olla laaja ja raskas projekti, jos perusasiat eivät ole kunnossa tietoturvan osalta. Käyttöönottoa varten tulee tehdä projekti-suunnitelma, jossa selvitetään ja varmistetaan aikataulut, kustannukset sekä projektiin sitoutuneet resurssit. Jos organisaatiosta ei löydy tarvittavia resursseja tai mahdollisuutta tutustua standardin asettamiin vaatimuksiin, on suositeltavaa käyttää asiaan perehtynyttä konsulttia. Standardin käyttöönotolle tulee varata riittävästi aikaa, jotta organisaatiossa toteutuu riskien hallinta, dokumentointi, sisäinen auditointi ja toimintatapojen toteutus.

Standardissa annetaan selkeät tavat, määritelmät ja toimintaohjeet tietoturvallisuuden toteuttamiseen ja valvomiseen. Vaatimukset standardissa tarjoavat

soveltamismahdollisuutta sekä tiettyjen osa-alueiden rajaamisen pois. Näin olen pystytään varmistumaan yksinkertaisen ja selkeän kokonaisuuden muodostamisesta standardointiin.

Standardin käyttöönotto ja saaminen vaatii muutoksia organisaation toimintatapoihin. Henkilökunta tulisi pitää ajan tasalla viestinnällä ja sitouttaa noudattamaan tietoturvallisuuden hallintajärjestelmän prosesseja. Henkilökunnan tulisi olla mukana toiminnassa mahdollisimman laajasti kehittämässä omaa toimintaansa prosessien osa-alueilla, jotta ei kohdattaisi muutosvastarintaa.

ALTEN Finlandin tietoturvan puutteisiin vaikuttaa lyhyellä aikavälillä tehty yrittysosto ja isoon konserniin liittyminen. Yrityksessä on käynnissä ONE IT –projekti, jonka tavoitteena on yhtenäistää ja selkeyttää toimintoja ja ohjeita. Osa ohjelmistoista ja niiden tietoturva tulee konsernin puolelta jatkossa.

Konsernitasolla ALTEN Groupin tietoturva on selkeästi laadittu ja Groupissa on otettu käyttöön ISO/IEC 27001 -standardi. Tämä lopputyö on osa ALTEN Finlandin ISO 27001 -tavoitteen saavuttamiseen tehtävää selvitystä.

9 Lähteet

ALTEN Finland. 2017a. ALTE esittely. ALTEN Finland intranet. Vain sisäiseen käyttöön. Luettu: 28.12.2017.

ALTEN Finland. 2017b. ALTEN Finland. Luettavissa: <https://www.alten.fi/tieto-meista/alten-finland>. Luettu: 28.12.2017.

ALTEN Finland. 2017c. ALTEN Finland yleisesite. ALTEN Finlandin intranet. Vain sisäiseen käyttöön. Luettu: 10.12.2017.

ALTEN Group. 2017a. ALTEN Group. Luettavissa: <http://www.alten.com/>. Luettu: 28.12.2017.

ALTEN Group 2017b. ALTEN 2016 Registration Document. Luettavissa: <http://www.alten.com/>. Luettu: 28.12.2017.

Kuivalainen, M. 2011. Valmistautuminen ISO/IEC 27001 standardin sertifiointiin. Opinnäytetyö. Pohjois-Karjalan ammattikorkeakoulu. Teknologiaosaamisen johtamisen koulutusohjelma (Ylempi AMK). Luettavissa: <http://urn.fi/URN:NBN:fi:amk-201201051080>. Luettu: 1.7.2018.

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Kauppakaari.

Niemimaa, E. 2018. Miten toteutan ISO27001:n mukaisen tietoturvallisuuden hallintajärjestelmän sujuvasti? Luettavissa: https://www.secrays.com/tietoturvapalvelut/miten-toteutan-iso27001-sujuvasti/?gclid=EAlaIQob-ChMI7pX41uGm3AIVRqwYCh19CgMIEAAYASAAEgJy-_D_BwE. Luettu: 15.7.2018.

SFS-EN ISO/IEC 27001. 2006. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardoimisliitto SFS.

SFS-EN ISO/IEC 27001. 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardoimisliitto SFS.

SFS-EN ISO/IEC 27002. 2017 Informaatioteknologia. Turvallisuus. Tietoturval-
lisuuden hallintakeinojen menettelyohjeet. Suomen Standardoimisliitto SFS.

Soralhti, S., Hämäläinen, K. & Jokinen, P. 2009. Alte Oy – Ajatuksella luotua
tekniikkaa. Raahe: Alte Oy.

Standardisoinnin oppilaitosportaali SFSedu. 2018. Tietoturvallisuuden hallinta-
järjestelmä: ISO/IEC 2007. Luettavissa: [http://www.sfsedu.fi/files/121/ISO-
27000_2015.ppt](http://www.sfsedu.fi/files/121/ISO-27000_2015.ppt). Luettu: 22.6.2018.

Tervo, T. 2017. ISO/IEC 27001 –standardi yleisen tietosuojasetuksen kon-
tekstissa. Kandidaatintutkielma. Jyväskylän yliopisto. Informaatioteknologian
tiedekunta. Tietojärjestelmätieteen laitos. Luettavissa:
[https://jyx.jyu.fi/bitstream/han-
dle/123456789/55984/URN%3ANBN%3Afi%3Aju-201711234343.pdf?se-
quence=1&isAllowed=y](https://jyx.jyu.fi/bitstream/handle/123456789/55984/URN%3ANBN%3Afi%3Aju-201711234343.pdf?sequence=1&isAllowed=y). Luettu: 24.6.2018.

Väestörekisterikeskus. 2018. ISO/IEC 27001. Luettavissa: [https://suomi-
digi.fi/menetelmat/iso-iec-27001/](https://suomi-digi.fi/menetelmat/iso-iec-27001/). Luettu: 22.6.2018.

Liitteet

Kysely

Kirsi Lehmuskanta
Tietojärjestelmäosaamisen koulutusohjelma, YAMK
Haaga-Helia ammattikorkeakoulu

KYSELY
20.6.2018

Kysely tietoturvallisuuden hallintajärjestelmän ISO 27001 -standardin käyttöönottoa varten ALTEN Finlandin manageri – hallinnon henkilöstölle.

1. Kuinka hyvin tunnet tietoturvallisuuden hallintajärjestelmän ISO 27001 -standardin?
2. Kuinka tietoturvallisuuden hallintajärjestelmän ISO 27001 käyttöönotto tulisi vaikuttamaan asiakassopimuksiin ja niiden hankintaan?
3. Kuinka paljon tietoturvallisuuden hallintajärjestelmä ISO 27001 vaikuttaisi sinun työtehtäviesi hallintaan sekä työympäristössä toimimiseen?
4. Kuinka hyvin otat huomioon työskentelyssäsi tietoturvan tällä hetkellä?
5. Millaisella tasolla ALTEN Finlandin tietoturvataso on tällä hetkellä?
6. Oletko saanut tarvittavan tietoturvakoulutuksen tullessasi töihin ALTEN Finlandille?
7. Mitä haluaisit tietää tietoturvasta jatkossa, jotta työskentelysi olisi sujuvaa?