TIETOTURVALLISUUDEN SERTIFIOINTI ISO/IEC 27001 -TIETOTURVALLISUUS-STANDARDILLA

Case: Autovahinkokeskus Oy

LAHDEN AMMATTIKORKEAKOULU
Liiketalouden koulutusohjelma
Yrityshallinto
Opinnäytetyö
29.5.2009
Simo Kemppainen

Lahden ammattikorkeakoulu
Liiketalouden koulutusohjelma

SIMO KEMPPAINEN

Yrityksen tietoturvallisuuden sertifiointi ISO/IEC 27001 -tietoturvallisuus-standardilla
Case: Autovahinkokeskus Oy

Yrityshallinnon opinnäytetyö, 50 sivua, 13 liitesivua

Kevät 2009

TIIVISTELMÄ

Tämän opinnäytetyön aiheena on tutkia tietoturvallisuutta liiketoiminnassa, tietoturvallisuuden hallintajärjestelmän toteuttamista ja ylläpitoa, riskien arviointia sekä tietoturvallisuuden sertifiointivaatimuksia ISO/IEC 27001 -tietoturvallisuus-standardilla. Työssä tutkitaan myös, miten tietoa käsitellään tietoturvallisesti ja miten sitä kuuluu suojata.

Autovahinkokeskus Oy on vakuutusyhtiöiden lunastaminen ajoneuvojen realisointia harjoittava yritys, joka työllistää tällä hetkellä 49 henkilöä. Lähes jokainen henkilö käyttää tietojärjestelmiä työssään, minkä vuoksi tietoturvallisuuteen on aiheellista kiinnittää paljon huomiota. Autovahinkokeskus Oy:n tavoitteena oli selvittää tietoturvallisuuden sertifiointivalmiudet ISO/IEC 27001 -tietoturvallisuus-standardin mukaisesti.

Tutkimuksessa selvitettiin käytettävien tietojärjestelmien ja tietoteknisen infrastruktuurin nykytila ISO/IEC 27001 -tietoturvallisuusstandardin vaatimusten mukaan. Tutkimus osoitti tietojärjestelmien ja menettelytapojen olevan hyvää tasoa. Parannettavaa löytyi jonkin verran sekä teknisistä ratkaisuista että toimintatavoista, mutta eniten huomiota tulee kiinnittää dokumentointiin, tapahtumien seurantaan sekä tietojärjestelmien valvontaan.

Työssä tutkittiin myös henkilökunnan tietoisuutta käytössä olevien tietojärjestelmien tietoturvallisuudesta, yleisistä tietojenkäsittelypalvelujen käyttötottumuksista, ohjeistuksista ja koulutuksista. Tutkimuksessa paljastui tässä olevan suurin haaste lähitulevaisuudessa. Ohjeistusta ja koulutusta tarvitaan sekä tietoturvallisuuden että ohjelmistojen käyttöön.

Työn tuloksena on Autovahinkokeskus Oy:n tietojärjestelmien, toimintatapojen ja henkilöstön tietoturvatietoisuuden nykytilakartoitus sekä korjaus- ja parannusehdotuksia sertifioinnin aloittamista varten.

Avainsanat: Tietoturvallisuus, tietoturvallisuuden hallintajärjestelmä, riskit, johtaminen, sertifikaatti

Lahti University of Applied Sciences
Degree Programme in Faculty of Business Studies

SIMO KEMPPAINEN

The ISO/IEC 27001 Certification
Case: Autovahinkokeskus Oy

Bachelor´s Thesis in Business Management

50 pages, 13 appendixes

Spring 2008

ABSTRACT

The subject of this Bachelor's Thesis is to research into information security in business. Other questions are how to achieve and support an Information Security Management System, manage risks and survey requirements of the ISO/IEC 27001 standard. How to manage and secure this information is also the subject of this study.

Autovahinkokeskus Oy is specialized on realizing vehicles redeemed by insurance companies. The company employs 49 persons at the moment. The information systems are important tools in everyday work done by everyone. That makes it very important to focus on information security. The field of activity of the company was looking for facilities in order to certify the information security with the ISO/IEC 27001 standard.

In this study information systems and technological infrastructure with requirements of the ISO/IEC 27001 standard were analyzed. The research found information systems and procedures to be at a good level. There is some need to improve both the technical solutions and ways of working, but the main focus should be on the documentation, on the surveillance of the things that are happening at the moment and on the supervision of the data system as a whole.

The study took also under the investigation the security of the information system currently in use, the general usage of the data services, and the training in use. The research result here was that the biggest challenge is just this. Advice and training is needed, both concerning the data security and the use of software.

The result of the thesis is a survey of the current state of the information systems, practices and knowledge about the information security. There are also recommendations for improvements and development for the beginning of the certification process.

Key words: Information security, Information Security Management System, risks, management, certificate

SISÄLLYS

1 JOHDANTO

1.1 Taustaa

Turvallisuusjohtaminen on Suomessa varsin nuori käsite. Ensimmäiset turvallisuusjohtamisen vaikutteet ja määrittelyt tulivat 1980-luvulla, samoihin aikoihin kun liiketoiminta oli kansainvälistymässä. Tällöin otettiin käyttöön kaksi tärkeää turvallisuusjohtamisen työkalua: muutaman vuoden välein tehtävät laajat riskikartoitukset sekä suurten hankeinvestointien yhteydessä tehtävät poikkeamatarkastelut. Riskien kartoittamisen lisäksi aloitettiin myös riskien suuruuden tarkastelu. Lisäksi ymmärrettiin jatkuvan parantamisen tarpeellisuus saavutetun turvallisuuden tason ylläpitämisessä. Tietoturvallisuus on tärkeä osa turvallisuusjohtamista.

Tietojärjestelmät ovat keskeisessä asemassa tämän päivän organisaatioissa. Järjestelmien käyttövarmuus, turvallisuus sekä joustavuus ovat tärkeitä asioita päivittäisten tehtävien ja liiketoiminnan sujuvuuden kannalta.

Tietohallinnon merkittävä rooli liiketoiminnassa nostaa esiin kysymykset tietoturvallisuudesta. Nykyisiä järjestelmiä uusitaan tehokkaammiksi ja automaattisemmiksi sekä yhteystapoja sidosryhmien eri verkkoympäristöihin kehitetään tihein väliajoin turvallisemmiksi. Tietojärjestelmiä on rakennettu palvelemaan aina kyseisen ajankohdan tarpeita ja niiden skaalautuvuus vastaamaan tulevia muutostarpeita ja tietoturvallisuutta on jäänyt vähemmälle huomiolle. Tämä aiheuttaa tarpeen määräajoin suoritettaville suurille muutostöille.

Tämä opinnäytetyö keskittyy Autovahinkokeskus Oy:n (AVK) liiketoiminnan tietoturvallisuuteen. AVK on auto- ja liikennevakuutustoimintaa harjoittavien vakuutusyhtiöiden omistama yritys, joka realisoi lunastettuja ajoneuvoja ja niistä purettuja varaosia.

1.2 Tavoite, tutkimuskysymykset ja teoreettinen viitekehys

Opinnäytetyön tavoitteena on tutkia tietoturvallisuuteen vaikuttavia asioita AVK:n liiketoiminnassa, kartoittaa järjestelmien tietoturvallisuuden nykytila sekä henkilöstön sitoutuminen tietoturvallisuuteen. Tavoitteena on myös selvittää, miten yritys saa sertifioitua järjestelmien ja menetelmien tietoturvallisuuden ISO/IEC 27001 -tietoturvallisuusstandardilla.

Opinnäytetyön tavoitteiden saavuttaminen edellyttää vastauksia seuraaviin tutkimuskysymyksiin:

- Mikä on tietoturvallisuuden merkitys yrityksen liiketoiminnan kannalta
- Miten henkilöstö suhtautuu tietoturvallisuuteen tällä hetkellä?
- Miten nykyiset järjestelmät ja menetelmät vastaavat standardin mukaista
- tavoitetasoa?
- Millaisia muutoksia menetelmiin ja järjestelmiin on tehtävä ISO/IEC 27001 -tietoturvallisuusstandardin mukaiseen tavoitetasoon pääsemiseksi?

Tämä opinnäytetyö tutkii tietoturvaa osana yritysten liiketoimintaa. Tietoturva mielletään usein korkeana kustannuksena ja irrallisena yksittäisenä osana yrityksen tietohallintoa, mutta syvennyttäessä tarkemmin liiketoimintaan ja prosesseihin, tietoturva saa uuden merkityksen.

Tietoa pidetään yritysten tärkeimpänä voimavarana. Päivittäisen tekemisen ja liiketoiminnan jatkuvuuden kannalta on hyvin tärkeää suojella ja käyttää tietoa oikein. ISO/IEC 27001 -tietoturvallisuusstandardi määrittelee tietoturvallisuuden tarkoittavan tiedon luottamuksellisuutta, eheyttä ja käytetävvyyttä. Lisäksi tietoturvallisuuden muita ominaisuuksia ovat mm. aitous, vastuullisuus, kiistämättömyys ja luotettavuus.

ISO/IEC 27001 -tietoturvallisuusstandardin yleinen lähtökohta on toimivan tietoturvallisuuden hallintajärjestelmän luominen, ylläpitäminen sekä jatkuva noudattaminen ja valvominen. Se ottaa kantaa yrityksen hallinnollisiin, sopimuksellisiin sekä lakisääteisiin velvoitteisiin huolehtia tietoturvallisuudesta. Standardin ohjaa-

ma tietoturvallisuuden hallintajärjestelmä rakentuu liiketoimintalähtöisesti organisaation tarpeiden mukaan, ja on liiketoiminnan laajuudesta ja organisaation koosta riippumaton.

1.3 Tutkimusmenetelmät

Tutkimus on luonteeltaan kvalitatiivinen eli laadullinen. Työtä varten on valittu tutkimusmenetelmiksi kyselylomakkeet, henkilökohtaiset haastattelut sekä tietoturvallisuuden arviointi ISO/IEC 27001 -tietoturvallisuusstandardin vaatimusten mukaisesti.

Kyselylomakkeet

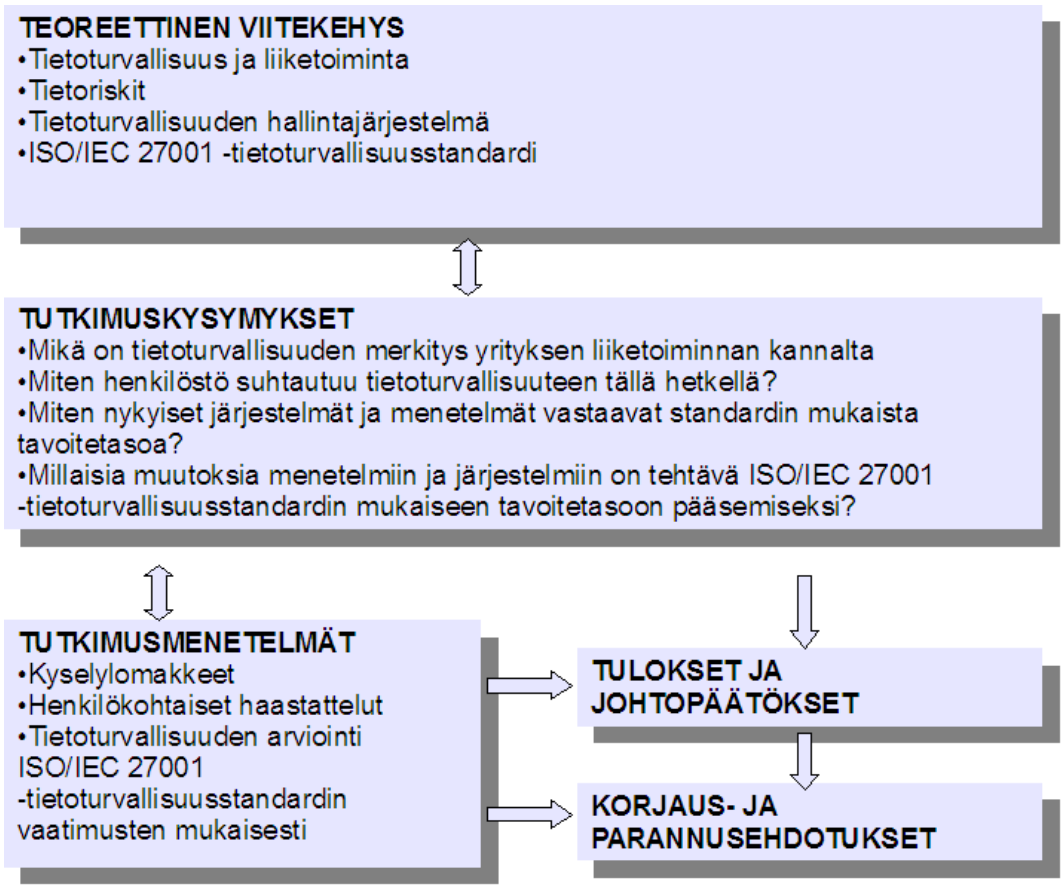
Kyselylomakkeiden avulla selvitetään henkilöstön suhtautumista tietoturvallisuuteen ja tietotekniikan käyttötottumuksiin. Lomakkeina käytetään VTT:n pk-yritysten riskienhallinnan työvälinesarjan lomakkeita, mitkä soveltuvat hyvin ISO/IEC 27001 -tietoturvallisuusstandardin vaatimustenmukaisuuden arviointiin. Nämä lomakkeet ovat liitteessä 1.

Henkilökohtaiset haastattelut

Henkilökohtaiset haastattelut suoritetaan sekä järjestelmiä työkseen käyttävien henkilöiden että operatiivisen johdon kanssa. Haastatteluiden avulla saadaan kuva organisaation liiketoiminnallisista tavoitteista sekä henkilöstön ja johdon suhtautumisesta tietoturvallisuuteen.

Tietoturvallisuuden arviointi ISO/IEC 27001 -tietoturvallisuusstandardin vaatimusten mukaisesti

Tietoturvallisuuden arviointi tehdään vertaamalla kyselyjen ja haastattelujen tuottamia tutkimustuloksia järjestelmien ja toimintatapojen osalta ISO/IEC 27001 -tietoturvallisuusstandardin vaatimuksiin. Arvioinnin kautta selvitetään toteutuneet kohdat sekä paikannetaan mahdolliset tietoturvallisuuteen liittyvät puutteet.



Kuvio 1: Opinnäytetyön tutkimusasetelma

1.4 Opinnäytetyön rakenne

Tämä opinnäytetyö koostuu teoria- ja tutkimusosista. Teoriaosassa käsitellään tietoturvallisuutta liiketoiminnan kannalta, käydään läpi prosesseja ja tietoturvallisuuden johtamiseen liittyviä seikkoja. Tutkimusosuudessa otetaan kantaa AVK:n nykytilaan, tutkin nykyisten järjestelmien hankintaperusteita sekä oman henkilöstön suhtautumista tietoturvallisuuteen. Tutkimusosan avulla kartoitetaan AVK:n valmiuksia sertifioida tietoturvallisuus ISO/IEC 27001 -tietoturvallisuusstandardilla.

2 TIETOTURVALLISUUS JA LIIKETOIMINTA

2.1 Tietoturvallisuuteen liittyviä käsitteitä

Hallinnollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus tarkoittaa niitä hallinnollisia toimenpiteitä, mitkä tähtäävät organisaation tietoturvallisuuden parantamiseen. Keinoja tämän toteuttamiseen ovat esimerkiksi organisaatiojärjestelyt, tehtävien ja vastuiden määrittely, ohjeistukset, koulutus sekä valvonta. Hallinnolliseen tietoturvallisuuteen kuuluvat oleellisesti tietoturvasuunnitelma sekä tietoturvapolitiikka. Tietoturvasuunnitelma määrittelee yksityiskohtaisesti kehittämisen aikataulut sekä toimenpiteet tietoturvapolitiikassa määriteltyjen tavoitteiden saavuttamiseksi. Näiden lisäksi on usein erillisiä tietoturvasuunnitelmaa täydentäviä ohjeita, esimerkiksi ohjeet poikkeamiin reagoimiseksi, ylläpitopolitiikka, sähköpostipolitiikka ja säännöt esimerkiksi kuolemantapausten varalle. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Henkilöstöturvallisuus

Henkilöstöturvallisuus tarkoittaa oman organisaation sekä ulkopuolisten henkilöiden inhimillisestä toiminnasta aiheutuvien tietoturvariskien hallintaa. Riskejä aiheuttavat tahallisen toiminnan (esimerkiksi anastukset, yritysvakoilu, petos ja kavallus) lisäksi myös osaamattomuudesta ja erehdyksistä aiheutuvat riskit. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Erityisen tärkeitä asioita henkilöstöturvallisuuteen liittyvässä riskienhallinnassa ovat toimintatavat, rekrytointi, toimenkuvat, käyttöoikeudet, koulutus, opastaminen ja valvonta. Kriittisissä tehtävissä toimenkuvien suunnittelun tulisi lähteä siltä pohjalta, että useampi kuin yksi henkilö on tietoinen asioista. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Henkilöstöturvallisuudessa on myös otettava huomioon sijaisjärjestelyt. Organisaatiossa ei saa muodostua tilannetta, jossa yrityksen toiminta pysähtyy esimerkiksi yhden avainhenkilön poistuttua organisaation palveluksesta. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Fyysinen turvallisuus

Fyysinen turvallisuus tarkoittaa laitteiden käyttöympäristöjen suojaamista esimerkiksi lukituksilla, kulunvalvonnalla, vartioinnilla ja muilla tilojen suojaustoimilla. Tarkoituksena on estää ja hidastaa esimerkiksi palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkoja. Fyysisen turvallisuuden huolehtiminen on aiheellista paitsi työpaikalla, myös muissa toimitiloissa ja etätyöpisteissä, esimerkiksi henkilön kotona. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan siirrettävän tiedon ja tietoa siirtävien laitteiden fyysistä turvallisuutta. Sen avulla pyritään varmistamaan tietojen muuttumattomuus, luottamuksellisuus ja todentamaan lähettävät ja vastaanottavat osapuolet. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Tietoliikenneturvallisuudessa tarkastellaan tiedonsiirtovälineitä, tiedonsiirtoprotokollia, verkkotopologioita, tietoturvatuotteita ja salausalgoritmeja. Tietoliikenneverkkojen turvallisuudessa on kiinnitettävä huomiota erityisesti eri organisaatioiden verkkojen liityntäpisteisiin, koska laitteistot, politiikat, osaamistasot ja suhtautuminen tietoturvallisuuteen vaihtelevat suuresti organisaatioittain. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmiin ja sovelluksiin liittyvää tietoturvallisuutta. Ohjelmistoturvallisuuteen vaikuttavia asioita ovat mm. tietokonearkkitehtuurit, käyttöjärjestelmät, kääntäjät, sovellukset, haittaohjelmat ja virukset sekä ohjelmavirheet ja näiden tietoturvapuutteet. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Ohjelmistojen tietoturvavaatimukset on otettava huomioon jo suunnitteluvaiheessa, sillä jälkikäteen niiden lisääminen on hyvin mutkikasta ja kallista. Usein tämä tekee valmiista ohjelmistoista liian kankeita, jolloin toteutetaan räätälöityjä tietojärjestelmiä. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan ainoastaan tietoihin kohdentuvaa turvallisuutta. Tiedot voivat olla missä muodossa tahansa. Tietoaineistoturvallisuudessa on tietojen ja tietovälineiden tunnistamista, turvallisuusluokitusta, säilytystä, varmistamista, käsittelyä ja tarpeettoman tiedon tuhoamista. Tarkoituksena on turvata tietojen eheys, muuttumattomuus, aitous, saatavuus ja luottamuksellisuus. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Tiedon turvaluokittelu on tärkeää ja on otettava huomioon tiedon turvaluokituksen muuttuminen ajan kuluessa, esimerkiksi salainen tieto voi muuttua julkiseksi. On myös aiheellista huolehtia tietojen eheydestä ja versioinnista. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan turvallisen käyttötavan, käyttöympäristön, tapahtumien valvonnan ja toiminnan jatkuvuuden hallintaa. Turvallinen käyttötapa edellyttää järjestelmien asennukselta ja ylläpidolta organisaation tietoturvasuunnitelman mukaista toimintaa. Turvallinen käyttöympäristö taas muodostuu järjestelmän ja laitteistoturvallisuuden ylläpidosta. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Tapahtumien valvonnalla tarkoitetaan esimerkiksi järjestelmän tapahtuminen kirjautumista lokeihin ja niiden seuraamista. Ongelmien aiheuttajat ovat näin jäljitettävissä ja niiden vaikutukset onnistutaan minimoimaan ja ehkäisemään tulevat ongelmat. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Jatkuvuuden hallinnalla tarkoitetaan dokumentointia ja jatkuvuussuunnitelman laadintaa. Jatkuvuussuunnitelma sisältää viittaukset dokumentteihin, josta löytyvät

toipumissuunnitelma, pääsynvalvonnan toteutus, järjestelmien mahdollisten lokitiedostojen sijainnit ja muut suojaustoimenpiteet. (Tietoturva-ammattilaisen osaamistarvekartoitus)

Tietoturvaloukkaus

Suomessa toimii Viestintäviraston alaisuudessa CERT-FI -tietoturvaviranomainen, jonka tehtävänä on ennaltaehkäistä, havainnoida, ratkaista sekä tiedottaa tietoturvauhkia. Viranomainen määrittelee tietoturvaloukkausten seuraavasti: *Tietoturvaloukkauksella tarkoitetaan tilannetta, jossa organisaation, yrityksen, yhteisön tai yksityisen henkilön tietojärjestelmän tietojen käytettävyyttä, eheyttä tai luottamuksellisuutta oikeudettomasti muutetaan. Tällä voidaan käsittää esimerkiksi toisen henkilön tai organisaation tietojärjestelmän toimivuuden tahallista vaikeuttamista tai estämistä. Tietoturvaloukkaukseksi voidaan myös tulkita tilanne, jossa organisaation, yrityksen, yhteisön tai käyttäjän tietojärjestelmiä tai tietoja käytetään ilman käyttäjän lupaa.* (CERT-FI 2009)

2.2 Tietoturvallisuuden vaikutukset liiketoiminnassa

Tietoturvallisuus tulkitaan usein pelkäksi menoeräksi organisaatioiden johdon tasolla. Kuitenkin on selvää, että sijoittamalla tietoturvallisuuteen, voidaan välttyä paljon suuremmalta taloudelliselta vahingolta. Näin ollen tietoturvallisuus on olennainen osa organisaation riskienhallintaa. Tietoturvaa voidaan pitää myös keskeisenä kilpailutekijänä. (Tietoturvan merkitys IT-sidonnaisissa liiketoimintaprosesseissa)

Organisaatioilla on nykyisin käytössään paljon aikaisempaa kehittyneemmät tekniset ratkaisut, jolloin harrastelijoiden tekemät hyökkäykset ja haavoittuvuuksien hyödyntämisyritykset on enimmäkseen saatu karsittua. Näiden ohella esiintyy kuitenkin ammattirikollisia, joilla on korkeatasoinen alan osaaminen ja laadukkaat tekniset työkalut. Heidän pysäyttämisensä on suuri haaste organisaatioissa sekä koko yhteiskunnassa. (Tietoturvan merkitys IT-sidonnaisissa liiketoimintaprosesseissa)

Organisaatioissa työskentelevät henkilöt käsittelevät yleensä aina tietoa, minkä turvallisuudesta huolehtiminen on ensisijaisen tärkeää. Usein ihmiset eivät ole riittävän tietoisia siitä, miksi tiedon luottamuksellisuudesta on tärkeää huolehtia ja minkälaisia vaikutuksia tiedon päätymisellä vääriin käsiin voi olla. Ihmiset ovat alttiita houkutuksille, lisäksi henkilöiden koulutuspohjalla sekä tietotekniikan käyttötaidoilla on keskeinen rooli tietoturvallisuuden kannalta. (Tietoturvan merkitys IT-sidonnaisissa liiketoimintaprosesseissa)

Organisaation ilmapiirillä on myös tärkeä merkitys. Jos esimerkiksi työntekijää uhkaa töiden loppuminen, voi henkilö virittää loogisen pommin työnantajalleen ”muistoksi” tilanteesta. Myös liiallista toimenpiteiden ja työtehtävien valvontaa voidaan pitää hiostavana, mikä vaikuttaa ilmapiiriin hyvin negatiivisesti. (Tietoturvan merkitys IT-sidonnaisissa liiketoimintaprosesseissa)

2.3 Tietoturvallisuuden organisointi ja vastuut

Organisaation ylin johto vastaa muiden liiketoiminnallisten asioiden lisäksi myös tietoturvallisuudesta. Hyvän päätöksenteon edellytyksenä kuitenkin on usein nimittää erikseen henkilö vastaamaan tietoturvallisuutta koskevan päätöksenteon valmisteluista sekä toteutuksista. Toimintojen johtajat vastaavat yleensä tietoturvallisuuden toteutumisesta sekä tietoturvapolitiikan noudattamisesta omilla vastuualueillaan. He vastaavat myös erityisvastuuhenkilöiden kanssa tehtävästä yhteistyöstä, tieto-oikeuksien määrittämisestä, tietojen luokittelusta sekä tietojenkäsittelyn jatkuvuuden varmistamisesta. (Kerko 2001, 226)

Tietoturvallisuus on osa muuta yritysturvallisuutta, mutta sen erityisluonteen ja laaja-alaisuuden vuoksi erityisasiantuntijoilla on kuitenkin merkittävä rooli verrattuna muihin yritysturvallisuuden osa-alueisiin. Organisaatiolla tulisi olla käytettävissään tietoturvallisuuden kaikki osa-alueet riittävän hyvin tunteva ammattihenkilö, joka antaa koko organisaatiota koskevia turvallisuusohjeita sekä järjestää

mm. kehittämisyhteistyötä, koulutusta, katselmointia ja tiedottamista. Kuitenkin ainoastaan suurilla organisaatioilla yleensä on tarvetta palkata päätoiminen tietoturvapäällikkö. (Kerko 2001, 226-227)

Tietoturvallisuuden asiantuntijoilla on yleensä vastuu oman vastuualueensa yleisistä asioista, joita ovat mm. koulutus, tiedotus ja ohjeistus. Samoin heidän tehtäviinsä kuuluu osallistuminen kehitystä, tavoitteiden toteutumista ym. koskeviin työryhmiin, omaa vastuualuettaan koskevien katselmusten toteuttaminen, avustaminen benchmarking-toiminnassa sekä avustaminen toiminnan mittaamisen, tunnuslukujen ja raporttien kehittämisessä.
(Kerko 2001, 227)

2.4 Tietoturvallisuuden lähtötilakatselmus

Lähtötilakatselmuksen tavoitteena on verrata olemassa olevia turvallisuusjohtamisperiaatteita turvallisuutta koskeviin lakisääteisiin vaatimuksiin, organisaatiossa vallitsevaan todelliseen tilanteeseen ja menettelytapoihin, parhaisiin käytäntöihin esimerkiksi saman toimialan organisaatioissa sekä todellisuudessa käytettävien voimavarojen tehokkuuteen ja vaikuttavuuteen. (Kerko 2001, 229)

Seuraavien kysymysten avulla tietoturvallisuuden tasoa verrataan mainittuihin vaatimuksiin.

Vertailu lakisääteisiin vaatimuksiin

1. Missä määrin nykytilassa noudatetaan tietosuojalainsäädännön vaatimuksia; onko esimerkiksi henkilöstörekistereistä tehty rekisteriseloste, ovatko henkilörekisterit lain vaatimusten mukaisia ja onko pyydetty asianomaisten lupa henkilörekisterien pitämiselle?
2. Onko dokumenttien ja menettelyjen perusteella pääteltävissä, että organisaatio osoittaa tahtoa lain kirjaimen ja tulkinnan edellyttämää riittävää suojaamistahtoa tietoturvallisuuden ylläpitämiseksi?

3. Onko sopimus- ym. asiakirjoissa huomioitu tietoturvallisuus ja onko niissä noudatettu yrityssalaisuuksia sisältävistä asiakirjoista säädettyjä lakeja
4. Täyttyvätkö organisaation toiminnassa arvopaperimarkkinalain ja pörssisäädösten vaatimukset?
5. Onko organisaatio tehnyt tietoturvallisuuden osalta riittävässä määrin pelastustoimilain edellyttämiä uhkia, vaaratilanteita ja riskien suuruutta käsittäviä kartoituksia ja selvityksiä?

(Kerko 2001, 229)

Tietoturvallisuusperiaatteiden vertailu todelliseen tilanteeseen ja menettelytapoihin

1. Onko organisaation kaikilla toiminta-alueilla keskeisimmät toiminnalliset prosessiketjut kartoitettu ja onko niihin liittyvät toimintarutiinit kuvattu ja dokumentoitu?
2. Onko organisaation kaikilla toimintoalueilla inventoitu keskeiset ja aineelliset ja aineettomat omaisuusarvot?
3. Ovatko kartoitettuihin prosesseihin ja omaisuusarvoihin sisältyvät tietoturvallisuuden kannalta merkittävät haavoittuvat alueet sekä riskin laukaisevat erityiset tilanteet ja olosuhteet saatu selville?
4. Missä määrin tietoturvallisuutta koskevat suojaukset on tehty?

(Kerko 2001, 229-230)

Turvallisuusperiaatteiden vertailu organisaatiossa käytössä olevien resurssien tehokkuuteen ja vaikuttavuuteen

1. Onko tietoturvallisuustoiminta organisoitu asianmukaisesti?
2. Onko tietoturvallisuustoiminta hyvin suunniteltua ja budjetoitua?
3. Onko organisaatiossa käytössä konkreettinen ja päivitetty tietoturvallisuuden kehittämisohjelma?
4. Onko organisaatiossa tehty olennaiset, tietojärjestelmien turvallisuutta koskevat suojausinvestoinnit?
5. Onko toimitilojen turvallisuusvarustelussa tietoisesti huomioitu tietoturvallisuuden vaatimukset?

(Kerko 2001, 230)

Omaisuuserien ja toimintaprosessien tunnistaminen

Mikäli organisaatio haluaa varmistaa, ettei tietoturvallisuuden kannalta oleellisia asioita ole jäänyt tarkastelun ulkopuolelle, on sen systemaattisesti selvitettävä ja dokumentoitava kaikki olennaiset toiminnalliset prosessit ja omaisuuserät. Työ lisää lähtötilakatselmukseen kuuluvaa työpanosta, mutta kerran tehtynä se helpottaa huomattavasti myöhemmin tehtäviä riskienarviointeja ja palvelee organisaatiota jopa vuosikymmeniä tietoturvallisuusriskien hallinnassa sekä monessa muussa toiminnan kehittämisessä ja rationalisoimisessa. Mikäli toimintaprosessikartoitukset on suoritettu jo aiemmin muista kuin tietoturvallisuuteen liittyvistä syistä, on tehtyä työtä helppoa soveltaa myös tietoriskien hallinnassa. Jokaiselle prosessille on valittava omistaja, joka on jatkossa vastuussa mm. prosessien tietoriskien hallinnasta. (Kerko 2001, 230-231)

Omaisuuserien kartoittamisen pääryhmät ovat tietokannoissa, tiedostoissa ja tallenteissa olevat tiedot, tietokoneohjelmistot, fyysinen omaisuus sekä henkilöstö. Toimintaprosessien tietoturvallisuusselvityksessä on kysymys siitä, että prosessivaiheita on paljon eikä ilman perusteellista selvitystä voida olla varmoja, ettei joku prosessin käyttämä tai tuottama tieto olisi jollain hetkellä vaarassa tuhoutua, hävitä tai joutua väärinkäytön tai manipuloinnin kohteeksi. Toimintaprosessien kartoitus tehdään asiantuntijaryhmissä organisaation johdon ohjauksessa. Työn tulokset voidaan dokumentoida kommenteilla varustetuiksi kaavioiksi, jotka täydentyvät prosessin kuluessa. Organisaatiolle syntyy näin täydellinen kuva sen käyttämistä toimintaketjuista. Tietoturvallisuus on näin vain yksi niistä monista asioista, joita toimintaprosessien hallinnalla voidaan saavuttaa.

Toimintaprosesseja voidaan muuttaa ja kehittää mm. seuraavilla tavoilla:

1. Tietoturvallisuuden kannalta vaarallinen toimintaketjun osa voidaan kenties kokonaan poistaa.
2. Vastaava työvaihe voidaan ehkä tehdä jossain muussa yhteydessä.
3. Työvaihetta voidaan ehkä muuttaa siten, että riski pienenee.
4. Tietoturvallisuuden kannalta haavoittuvan vaiheen suojausta voidaan parantaa.

(Kerko 2001, 231)

2.5 Riskienarviointi

Tietoturvallisuuden riskienarvioinnin tulee mahdollisuuksien mukaan olla osa organisaation normaalia riskienarviointia ja riskienhallinnasta vastaavat luonnollisesti samat henkilöt. Arviointi kohdistuu sekä omaisuuseriin (laitteet, ohjelmistot, järjestelmät) sekä toimintaprosesseihin (toiminnan organisointi ja järjestäminen.) Riskienarvioinnin tulee perustua riskienarviointiohjelmaan, missä jokaisella toiminnolla on vastuuhenkilö. Viime kädessä liiketoiminnan riskeistä vastaa organisaation ylin johto. (Kerko 2001, 232)

Riskienarvioinnin päävaiheet

Riskienarvioinnin päävaiheet ovat seuraavat niin tietoturvallisuudessa kuin muussakin riskien arvioinnissa.

1. lähtötiedot ja arvioinnin suunnittelu
2. vaaratekijöiden tunnistaminen
3. riskin suuruuden määrittäminen
4. tapahtuman seurausten vakavuus
5. tapahtuman todennäköisyys
6. lopullinen riskin määrittäminen
7. riskin hyväksyttävyydestä ja tarvittavista toimenpiteistä päättäminen.

(Kerko 2001, 233)

Vaaratekijöiden tunnistaminen

Vaaratekijöiden tunnistamiseen voidaan käyttää sitä varten erikseen kehitettyjä menetelmiä ja kysymyssarjoja, mutta usein ne löytyvät vapaan, eri osapuolten välillä käytävien keskustelujen avulla. Tunnistamisen apuna käytetään myös lähtökatselmuksessa syntyneitä raportteja. (Kerko 2001, 233)

Tunnistamisen tarkoituksena on tarkentaa mahdollisimman yksityiskohtaisesti vaaranlähteet ja selvittää erityiset tilanteet ja olosuhteet, missä normaalisti riittävä suojaus saattaa pettää. Aina pitää myös tutkia, voiko useita vaaratekijöitä olla voimassa samanaikaisesti. Vaaratekijöiden tunnistamisessa yhdistyvät käyttäjien, ar-

vioinnin vetäjän ja mahdollisesti paikalla olevan erityisasiantuntijan tiedot. (Kerko 2001, 233)

Riskin suuruuden määrittäminen

Riskin suuruus muodostuu sen vakavuudesta ja todennäköisyydestä. Sen määrittämistä kuvataan alla olevalla taulukolla.

TODENNÄKÖISYYS	**HAITALLISUUS**		
	LIEVÄ	HAITALLINEN	ERITTÄIN HAITALLINEN
EPÄTODENNÄKÖINEN	Merkityksetön	Vähäinen	**Kohtalainen**
MAHDOLLINEN	Vähäinen	**Kohtalainen**	**Merkittävä**
TODENNÄKÖINEN	**Kohtalainen**	**Merkittävä**	**Sietämätön**

Taulukko 1: Riskin suuruuden määrittäminen (Kerko 2001, 327)

Arvioidaan pahin mahdollinen seuraus ja luokitellaan se taulukossa olevien apumäärittelyjen perusteella johonkin luokista *lievä*, *haitallinen* tai *erittäin haitallinen*. Tapahtuman todennäköisyys taas arvioidaan sekin kolmeluokkaisella asteikolla *epätodennäköinen*, *mahdollinen* tai *todennäköinen*. (Kerko 2001, 327)

Riskin hyväksyttävyydestä ja mahdollisista toimenpiteistä päättäminen

Riskien hyväksyttävyyteen liittyvä päätös on aina tehtävä tietoisesti. Jos riski on *merkityksetön* tai *vähäinen*, riskin hallitsemiseen riittää jatkuvan parantamisen periaatteen mukainen työympäristön tarkkailu ja kehittäminen. Jos riski on *kohtalainen*, riskin pienentämiseksi on ryhdyttävä toimiin. Resurssien käyttö ja kustannukset on tarkasti mitoitettava sekä aikataulusta ja vastuista sovittava. Jos riski on *merkittävä* tai *sietämätön*, toimenpiteisiin on ryhdyttävä viipymättä. Riskin pienentämiseen voidaan joutua osoittamaan huomattavia lisäresursseja. Mikäli työhön sisältyvä riski on sietämätön, sen tekemistä ei saa aloittaa tai jatkaa ennen riskin pienentämistä. (Kerko 2001, 327-328)

3 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ

3.1 Tavoitteita

Tietoturvallisuuden hallintajärjestelmän tehtävänä on suojata tietojen luottamuksellisuutta, eheyttä sekä käytettävyyttä. Suojaamisen tavoitteena on liiketoiminnan jatkuvuuden takaaminen, turvallisuusloukkauksista aiheutuvien tappioiden minimoiminen sekä tuottojen ja liiketoiminnan mahdollisuuksien maksimoiminen. Jokaisella organisaatiolla on omat, toisten vaatimuksista poikkeavat vaatimukset valvonnan, luottamuksellisuuden, eheyden ja käytettävyyden tasoille. (ISO 27001 -koulutuksen luentomateriaali)

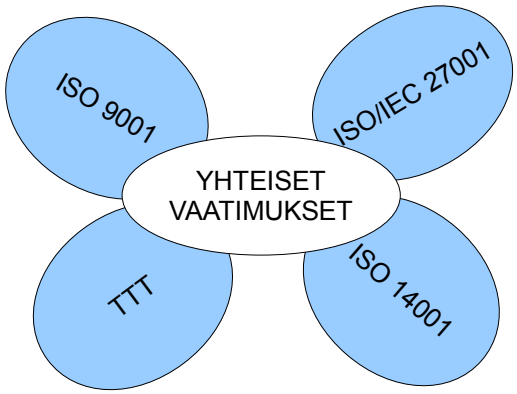
Standardin noudattamisen menettelytapoina ovat turvallisuusvaatimusten tunnistaminen, turvamekanismien valinta sekä järjestelmän toteuttaminen. Turvallisuusvaatimuksia tunnistetaan riskien arvioinnin, lainsäädännön, asetusten, säädösten, sopimusten vaatimuksien, tietojenkäsittelyn periaatteiden sekä tavoitteiden tuntemuksen avulla. (ISO 27001 -koulutuksen luentomateriaali)

Valittavia turvamekanismeja on esitelty ISO/IEC 27002 -menettelyohjeessa, sen ulkopuolelta voidaan myös valita lisää sopivia turvamekanismeja.
(ISO 27001 -koulutuksen luentomateriaali)

3.2 Muut hallintajärjestelmät

Kuviossa 2 olevat eri hallintajärjestelmät ovat luotu keskenään yhteensopiviksi ja ne voidaan arvioida yhdessä. Järjestelmistä voidaan myös luoda yhtenäinen toimintajärjestelmä, joka sisältää osat kustakin käyttöön otetusta hallintajärjestelmästä. Kuvassa on mukana ISO 9001 -standardin mukainen laatujärjestelmä, ISO 14001 -standardin mukainen ympäristöjärjestelmä, ISO/IEC 27001 -tietoturvalli-

suusstandardin mukainen tietoturvallisuuden hallintajärjestelmä sekä TTT – Työterverveys ja turvallisuusjärjestelmä.

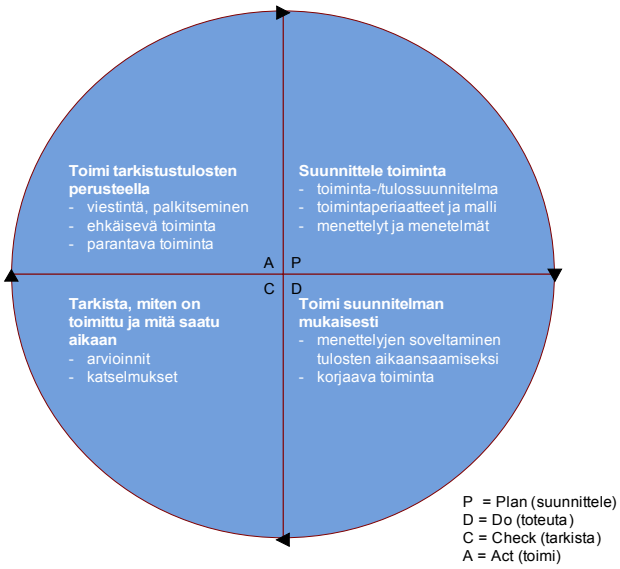


Kuvio 2: Eri hallintajärjestelmien yhteensopivuus (ISO 27001 -koulutuksen luentomateriaali)

Kaikki järjestelmät sisältävät seuraavia yhteisiä vaatimuksia:

- Prosessimainen toimintatapa, PDCA-malli (kuvio 3)
- Johdon sitoutuminen
- Jatkuva parantaminen
- 6 kuvattua menettelytapaa, joita ovat tallenteiden ohjaus, asiakirjojen ohjaus, sisäiset auditoinnit, johdonkatselmusmenettely, korjaavat sekä ehkäisevät toimenpiteet

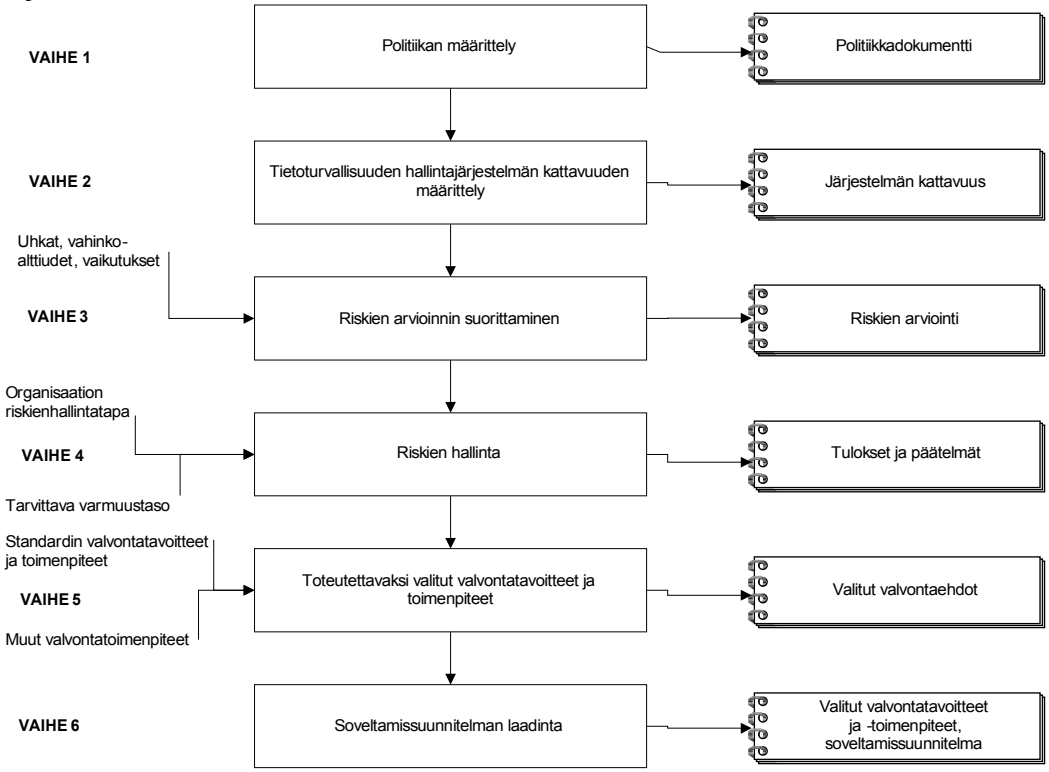
(ISO 27001 -koulutuksen luentomateriaali)



Kuvio 3: PDCA-malli

3.3 Tietoturvallisuuden hallintakehys

Kuvio 4 esittää tietoturvallisuuden hallintakehyksen luomisen työvaiheet. Kaikki järjestelmän luomiseen vaadittavat osat on dokumentoitava.



Kuvio 4: Tietoturvallisuuden hallintakehys (ISO 27001 -koulutuksen luentomateriaali)

Hallintakehyksen osat ovat:

1. Politiikan määrittely: määritellään organisaation tietoturvallisuuspolitiikka, sen tavoitteet, vastuut, toteutustavat, seurantatavat, ongelmien käsittelytavat ja sanktiot.
2. Järjestelmän kattavuuden määrittely: määritellään järjestelmän piiriin kuuluvat prosessit ja toiminnot.
3. Riskien arviointi: määritellään riskit ja niiden aiheuttamat seuraamukset sekä todennäköisyyden riskien toteutumiselle. Myös hyväksyttävät riskit määritellään.
4. Riskien hallinnan määrittely: kun riskit ovat tiedossa, määritellään suojaavat ja korjaavat toimenpiteet sekä arvioidaan hyväksyttävien riskien seuraamukset.
5. Valvontatavoitteet ja -toimenpiteet: määritellään järjestelmään valittavat standardin mukaiset valvontatavoitteet ja valvontatoimenpiteet. Standardin sisältämät, hallintajärjestelmän ulkopuolelle jätettävät valvontatavoitteet on myös sisällytettävä määritelmään ja perusteltava syyt niiden poisjättämiselle.
6. Soveltamissuunnitelman laadinta: luodaan tietoturvallisuuden hallintajärjestelmälle soveltamissuunnitelma ja aikataulut valittujen valvontatavoitteiden ja -toimenpiteiden perusteella.

(ISO 27001 -koulutuksen luentomateriaali)

3.4 Tietoturvallisuuden hallintajärjestelmän luominen

Tietoturvallisuuden hallintajärjestelmä luodaan organisaation tarpeisiin, eli yhtä oikeaa tapaa sen luomiseen ei ole. Järjestelmää suunniteltaessa otetaan huomioon organisaation koko, sijainti, liiketoiminnan erityispiirteet, suojattavat kohteet ja käytössä oleva teknologia. Järjestelmä on suunnilteltava organisaation kannalta riittävän kattavaksi mutta kuitenkin realistiseksi. Järjestelmää luotaessa huomioidaan organisaation omien tarpeiden ja vaatimusten lisäksi organisaatiota sitovat sopimukset ja voimassaoleva lainsäädäntö. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Järjestelmä velvoittaa organisaatiota tunnistamaan liiketoimintaan liittyvät riskit ja laatimaan niihin liittyvät toimintatavat. Organisaatiolla on oltava riskianalyysi ja toiminta-, jatkuvuus- sekä toipumissuunnitelmat riskien toteutumisen varalle. Riskejä ei koskaan voi poistaa kokonaan, vaan niiden toteutumisriskiä ja niiden toteutumisesta syntyviä haittoja voidaan pienentää. Kun organisaatio tuntee toimintansa riskit ja määrittelee, mitkä niistä voidaan hyväksyä ja miten niiden kanssa tulee toimia, on toiminta hyvin hallittua. Tietoturvallisuuden hallintajärjestelmän piiriin kuuluvien riskien hallinnassa oleellista on tunnistaa suojattavat kohteet ja niiden omistajat, niihin liittyvät uhkat, haavoittuvuudet sekä vaikutukset, jotka syntyvät kohteen luottamuksellisuuden, eheyden tai käytettävyyden menettämisen seurauksena. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Riskeille määritellään hyväksymiskriteerit, joiden mukaan riskejä voidaan hyväksyä tai toisaalta niiden varalle on tehtävä tarkemmat ehkäisy- ja torjumissuunnitelmat. Tietoturvallisuusstandardi antaa valmiita valvontatavoitteita ja turvamekanismeja riskienhallintaan, jotka on liitettävä tietoturvallisuuden hallintajärjestelmään. Riskejä, joiden varalle ei tehdä tarkempaa suunnitelmaa, kutsutaan jäännösriskeiksi. Kun ne on tunnistettu, ne on dokumentoitava ja niille on hankittava johdon hyväksyntä. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Tietoturvallisuuden hallintajärjestelmä on arvokas työkalu, mutta sen käyttöönotto vaatii soveltamissuunnitelman ennen kuin sitä voidaan todellisuudessa käyttää. Soveltamissuunnitelmaan kuuluu tietoturvallisuusstandardin mukaan sisällyttää valitut, jo käytössä olevat sekä mahdollisesti poisjätetyt valvontatavoitteet ja turvamekanismit perusteluineen. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Vaikka ulkopuolelle jätettyjen valvontatavoitteiden ja turvamekanismien dokumentointi voi tuntua oudolta, se todentaa sen, ettei mitään ole jätetty pois vahingossa. (ISO/IEC 27001 -tietoturvallisuusstandardi)

3.5 Toteuttaminen ja käyttäminen

Tietoturvallisuuden hallintajärjestelmälle on laadittava dokumentoitu soveltamissuunnitelma, mikä käsittää suunnitelmat riskien käsittelystä, turvamekanismien toteuttamistavoista, kouluttamisen ja perehdyttämisen toteuttamisesta sekä tietoturvallisuustapahtumiin reagoimisesta. Soveltamissuunnitelma, kuten hallintajärjestelmäkin, luodaan organisaation tarpeisiin ja on asetettujen tavoitteiden mukainen. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Soveltamissuunnitelmassa tulevat esille vaadittavat resurssit muutosten toteuttamiseen sekä tarpeet henkilöstön kouluttamiseen ja perehdyttämiseen. Järjestelmä kuitenkin pohjautuu jatkuvaan kehittämiseen, eli kun vaadittavat muutokset ja korjaukset on tehty, järjestelmän toimivuutta katselmoidaan ja arvioidaan määritellyin väliajoin uudelleen ja laaditaan tarpeen mukaan jatkokehitysehdotuksia. Katselmusten ja sisäisten auditointien aikataulut tulee määritellä ja dokumentoida ja ne on suoritettava näiden vaatimusten mukaan. (ISO/IEC 27001 -tietoturvallisuusstandardi)

4 ISO/IEC 27001 -TIETOTURVALLISUUSSTANDARDI

4.1 Turvallisuuspolitiikka

Organisaation on laadittava tietoturvapolitiikka eli sen määrittelyasiakirja ja soveltamisohjeet. Se on organisaation johdon hyväksymä julkinen asiakirja ja siitä tulee tiedottaa kaikille organisaatiossa työskenteleville henkilöille sekä merkittäville ulkopuolisille sidosryhmille.

Tietoturvallisuuden hallintajärjestelmään kuuluu tietoturvapolitiikan katselmoinnin suunnittelu. Suunnitelmassa määritellään, kuinka usein politiikka arvioidaan uudelleen ja suunnitellaan siihen tarvittavat muutokset. Muutostarpeita syntyy esimerkiksi liiketoiminnan laadun tai määrän muuttuessa, organisaation tai sidosryhmien muuttaessa tietoteknistä infrastruktuuriaan tai oman henkilöstön määrän tai työtehtävien muuttuessa oleellisesti. Politiikan tulee aina olla kyseiseen tilanteeseen asianmukainen ja soveltuva. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Tietoturvallisuuden organisoiminen

Tietoturvallisuusstandardi painottaa erityisesti johdon pitkäjänteistä sitoutumista sekä selkeää esimerkkiä tietoturvallisuuteen sitoutumisessa, vastuiden jakamisessa ja niiden tunnustamisessa. Vastuu tietoturvallisuudesta kuuluu jokaiselle organisaation jäsenelle, ja sen vuoksi niiden määrittely ja niistä informoiminen on tärkeää. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Standardi velvoittaa organisaatiota myös huolehtimaan salassapitositoumuksista, jolloin jokainen organisaation jäsen on selkeästi tietoinen organisaation kannalta kriittisten tietojen käsittelystä. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Yhteistyö asiaankuuluvien viranomaisten ja erityisintressiryhmien kanssa kuuluu myös tietoturvallisuuden organisoimiseen. Erityisintressiryhmiä ovat esimerkiksi

turvallisuusasiantuntijat, konsultit ja ammatilliset järjestöt. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Liiketoimintaprosesseissa mukana olevat ulkopuoliset tahot, kuten asiakkaat, sidosryhmät ja muut tahot (vierailijat, konsultit, kauppiaat) aiheuttavat osaltaan myös tietoturvallisuusriskejä ja ne on tunnettava samalla tavalla kuin omaan henkilöstöön kohdistuvat riskit. Riskejä muodostuu sekä fyysisessä ympäristössä että sähköisessä viestinnässä ja tietojenkäsittelyssä. Kaikista tunnetuista turvallisuusvaatimuksista sekä turvamekanismeista on huolehdittava ennen pääsyn sallimista suojattuihin kohteisiin. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Suojattavien kohteiden hallinta

Suojattavia kohteita ovat tiedot, tilat ja välineet joilla tietoja käsitellään. Näiden tulee olla luetteloituja ja luokiteltuja, eli kohteella on arkaluonteisuuden perusteella turvallisuusluokka ja sille on nimetty omistaja, joka on vastuullinen taho kohteen tuottamisesta, kehittämisestä, ylläpidosta, käytöstä ja turvallisuuden valvonnasta. Liiketoiminnan kannalta kriittiset tiedot tulee merkitä ja niille tulee laatia ohjeisto, mikä on organisaation luokitteluperiaatteiden mukainen. Luokitteluun voidaan käyttää esimerkiksi seuraavanlaista tapaa:

Erittäin salainen	Tieto on erittäin kriittistä yrityksen liiketoiminnan ja sen jatkuvuuden kannalta ja väärinkäytettynä aiheuttaa merkittäviä taloudellisia vahinkoja. Tietoja ei saa näyttää ulkopuolisille ja omalle henkilöstöllekin erittäin rajoitetusti.
Salainen	Salainen tieto on henkilölle henkilökohtaisesti annettu, hänen työtään koskeva tieto, jonka joutuminen vääriin käsiin aiheuttaisi vakavia ongelmia yrityksen liiketoiminnalle. Tietoa ei saa näyttää ulkopuolisille, omalle henkilöstöllekin sitä voi näyttää vain tarpeen vaatiessa.
Yhtiönsisäinen	Yhtiönsisäinen tieto on yrityksen henkilökunnan käyttöön annettu yrityksen liiketoimintaa koskeva tieto. Tietoja saa näyttää omalle henkilöstölle vapaasti ja ulkopuolisillekin organisaation eduksi.
Julkinen	Julkinen tieto on yrityksen valmistamaa tai saamaa tietoaineistoa, joka on julkista ja tarkoitettu olemaan ulkopuolisten saatavissa. Tietojen oikeellisuus on tärkeää ja sitä on pyrittävä käyttämään ainoastaan organisaation eduksi.

Taulukko 2: Luottamuksellisen tiedon luokittelutavat (Kerko 2001: 224)

4.2 Henkilöstöturvallisuus

Tietoturvallisuusstandardi jakaa henkilöstöturvallisuuden ohjeistuksen (valvontatavoitteet ja turvamekanismit) kolmeen osaan: ennen työsuhteen alkua, työsuhteen aikana ja työsuhteen päättymisen jälkeen toteutettavat valvontatavoitteet ja turvamekanismit. Jokaisessa tilanteessa edellytetään, että organisaatiolla on olemassa tietoturvapolitiikan mukainen malli jakaa turvallisuusroolit sekä vastuut. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Ennen työsuhteen alkua tulee lakien, määräysten ja eettisten normien mukaisesti, tarkistaa työnhakijoiden tausta. Standardi ei määrittele tarkemmin tarkistuksen laatua, eli sen tulee olla suhteutettu liiketoimintavaatimuksiin, käsiteltävien tietojen luokituksiin ja tiedossa oleviin riskeihin. Työsopimusten ehtoihin kirjataan organisaation sekä kyseessä olevan henkilön ja tehtävän vastuut tietoturvallisuudesta. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Työsuhteen aikana johdon tulee edellyttää kaikkien käyttäjien noudattavan organisaation ohjeita ja periaatteita. Niiden muuttuessa järjestetään tarvittaessa asiaankuuluva tiedostus ja koulutus jokaisen henkilön toimenkuvan kannalta tarkoituksenmukaisella tavalla. Standardi myös antaa ohjeen sanktiomenettelyn laatimisesta, tosin ei puutu tarkemmin sen laatuun vaan organisaatio päättää siitä itse. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Työsuhteen päättymis- tai muuttumistilanteessa johdon tulee määritellä ja jakaa selkeät vastuut asian hoitamiseen. Kaikkien työntekijöiden ja ulkopuolisten käyttäjien tulee palauttaa kaikki hallussaan oleva, suojattaviin kohteisiin luokiteltu materiaali työsuhteen tai sopimuksen päättyessä. Organisaation tulee myös huolehtia siitä, että kaikki käyttöoikeudet tietoon tai tietojenkäsittelypalveluihin poistetaan sopimuksen päättyessä. Vastaavasti toimenkuvan muuttuessa käyttöoikeudet tulee muuttaa uutta toimenkuvaa tai tilannetta vastaavaksi. (ISO/IEC 27001 -tietoturvallisuusstandardi)

4.3 Fyysinen turvallisuus ja ympäristön turvallisuus

Fyysinen turvallisuus tarkoittaa toimipisteiden ja alueiden suojausta, missä sijaitsee luokiteltua tietoa tai tietojenkäsittelypalveluita. Standardi käyttää tällaisesta tilasta termiä turva-alue. Turva-alueet tulee suojata käyttäen turvarajoja (seinät, kulkuportit, miehitetyt vastaanottopisteet) ja niihin pääsyä tulee rajoittaa kulunvalvonnalla. Samoin turva-alueet kuuluu suojata asiaankuuluvalla tavalla inhimillisiä tai luonnollisia uhkia vastaan, joita ovat esimerkiksi mellakat, tulipalot, tulvat ja vesivahingot. Samoin julkiset tilat, kuten lastauspaikat ja asiakaspalvelutilat, tulee suojata siten, etteivät ulkopuoliset henkilöt pääse käsiksi organisaation luokiteltuun tietoon. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Fyysisellä turvallisuudella tarkoitetaan myös tietokoneiden, palvelinten ja muiden tietojenkäsittelylaitteiden turvallista ja häiriötöntä toimintaa. Laitteistot tulee sijoittaa sellaiseen paikkaan, mihin ei ulkopuolisilla ole estotonta pääsyä ja huolehdittava kaapeleiden turvallisesta sijoituksesta. Laitteiden toiminta ja hallittu alasajo täytyy varmistaa myös sähkökatkosten tai muiden peruspalvelujen häiriöiden varalta, ettei organisaation tietoja tästä syystä pääse katoamaan. Laitteiden huolto täytyy myös suunnitella siten, että käytettävyys ja tietojen eheys säilyy. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Käytöstä poistettavien laitteiden kierrätys ja käytöstäpoisto tulee huolehtia siten, ettei organisaation luokiteltua tietoa tai tekijänoikeuksien ja lisenssien alaisia ohjelmistoja pääse tämän jälkeen hyödyntämään. Laitteiden fyysinen siirto pois työpaikalta vaatii valtuutusmenettelyn. (ISO/IEC 27001 -tietoturvallisuusstandardi)

4.4 Tietoliikenteen ja käyttötoimintojen hallinta

Tietojärjestelmien kehitys- ja testausalustat tulee selkeästi erottaa toisistaan, jotta pienennetään luvattoman käytön tai tietojen muuttumisen riskiä. Käytännössä tämä tarkoittaa tuotanto- ja kehitysympäristöjen sijoittamista esimerkiksi eri palvelimille, jolloin kehitysympäristöön voidaan määrittää ulkopuolisia kehittäjiä tai

testaajia varten erilliset käyttöoikeudet heidän pääsemättä käsiksi organisaation tuotantoympäristön tietoihin. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Samoin ulkopuolisten toimittajien tuottamia palveluita, raportteja ja tallenteita tulee tarkkailla ja katselmoida säännöllisesti. Täytyy myös varmistua siitä, että ulkopuolinen toimittaja toimii sopimukseen sisällytettyjen turvamekanismien ja määritysten mukaisesti. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Standardi edellyttää tarkkailemaan säännöllisesti resurssien käyttöä ja laatimaan ennusteita tulevista kapasiteettivaatimuksista. Tällä voidaan varmistaa riittävä suorituskyky ja resurssit palvelemaan organisaation tarpeita järjestelmien toiminnan tämän vuoksi häiriintymättä. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Organisaation on laadittava hyväksyntäkriteerit järjestelmien päivityksiä sekä uusien järjestelmien käyttöönottoa varten. Oleellista tässä on kunnollisen testaussuunnitelman laatiminen sekä sitoutuminen riittäviin testauksiin ennen järjestelmien käyttöönottoa. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Haittaohjelmien ja virusten torjuntaa varten on myös turvamekanismit, mitkä velvoittavat organisaatiota huolehtimaan riittävistä havaitsemis- ja estotoimista sekä käyttäjien ohjeistuksista. Käytännössä oikeanlaiset virusturva- ja haittaohjelmien torjuntasovellukset sekä opastus turvalliseen ohjelmistojen käyttöön ovat tämän turvamekanismin mukaista toimintaa. Myös varmuuskopiointi on suunniteltava huolellisesti ja sovittava sen toiminnan säännöllisestä testaamisesta. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Verkon hallittavuus ja valvottavuus on myös tärkeä osa tietoturvaa. Verkkoa tulee valvoa uhkien tunnistamiseksi, jotta voidaan taata organisaation tietojen pysyminen oikeissa käsissä. Myös omien verkkopalvelujen turvallisuusominaisuudet ja hallintavaatimukset kuuluu yksilöidä ja kirjata mahdollisiin verkkopalvelusopimuksiin, olivat ne ulkoistettuja tai organisaation sisäisiä palveluita. Käytännössä tämä tarkoittaa hallintaominaisuuksien ja käytettävien yhteysmuotojen ja protokollien kirjaamista, jotta ollaan perillä järjestelmien ominaisuuksista sekä niiden

käytettävyyteen ja turvallisuuteen vaikuttavista riskeistä. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Siirrettävien tietovälineiden, kuten muistitikkujen ja optisten levyjen käyttöön tulee laatia toimivat menettelytavat. Näiden välineiden käyttö muodostaa aina riskin, sillä niiden avulla voidaan tuoda organisaation järjestelmiin tai viedä järjestelmistä materiaalia suojaamattomassa muodossa hyvinkin yksinkertaisesti. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Tietovälineiden käytöstä poistoa varten kuuluu laatia menettelytavat, minkä avulla varmistetaan tietojen säilyminen organisaation sisällä. Nämä menettelytavat kirjataan tietoturvallisuuspolitiikkaan tai sen soveltamisohjeisiin. Kaikkien järjestelmien dokumentaatiot tulee suojata luvattomalta käytöltä. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Tietojen vaihtoa varten tulee ottaa käyttöön tiedonvaihtoperiaatteet, menettelyohjeet ja turvamekanismit. Organisaatioiden tulee laatia keskinäiset sopimukset tiedon ja ohjelmien vaihdosta. Sekä tiedon fyysistä että sähköistä kuljetusta varten on oltava riittävät suojaukset tietojen väärinkäyttöä tai turmeltumista varten. Tämä koskee myös verkkoasiointia sekä viestiliikennettä, tietojen ja viestien epätäydellinen lähetys, kopiointi, muuttaminen tai toisto on pystyttävä estämään. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Tietojärjestelmien tapahtumalokien käyttöä varten on laadittava suunnitelma, minkä perusteella lokeja valvotaan käyttäjien toiminnan, tietoturvaloukkausten ja niiden yritysten kannalta. Lokit tulee koota ja niitä tulee säilyttää sovittu aika, jotta esimerkiksi tapahtunut tietoturvaloukkaus voidaan tutkia. Häiriöt tulee kirjata, analysoida ja ryhtyä asianmukaisiin toimenpiteisiin. Lokitiedot on lisäksi suojattava luvattomalta pääsyltä ja tietojen muuttamiselta. Myös pääkäyttäjien ja operaattorien tekemät toiminnot tulee kirjata. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Kaikkien organisaatiossa olevien järjestelmien ja tietokoneiden kellot tulee synkronoida sovitun tarkan ajanlähteen kanssa. (ISO/IEC 27001 -tietoturvallisuusstandardi)

4.5 Pääsyoikeuksien valvonta

Pääsyoikeuksia varten tulee laatia pääsynvalvontaperiaatteet, jota dokumentoidaan ja katselmoidaan sovituin aikavälein. Käyttöoikeuksien avaamisiin, muuttamisiin ja poistoihin tulee olla menettelyohjeet. Pääkäyttäjäoikeuksien myöntämisten suhteen täytyy olla erittäin kriittinen, ja mikäli oikeudet myönnetään, tulee niiden käyttöä valvoa. Lisäksi kaikkia käyttöoikeuksia tulee säännöllisesti tarkistaa ja korjata aina vallitsevan tarpeen mukaisiksi. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Verkkopalvelujen käytön periaatteisiin kuuluu, että käyttäjillä on pääsyoikeudet ainoastaan tarvitsemiinsa palveluihin, ja jokaiseen palveluun nämä oikeudet myönnetään erikseen. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Laitteiden ja käyttäjien tunnistamiseen täytyy olla menetelmät, joilla pyritään estämään ulkopuolisten tekijöiden aiheuttamia riskejä. Etätyöpisteissä verkkoyhteyksien tulisi olla tarkoituksenmukaisia, eli sieltä sallittaisiin pääsy ainoastaan kyseisestä pisteestä tehtävien työtehtävien hoitoon tarvittaviin sovelluksiin ja palveluihin. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Sisäänkirjausmenettelyn avulla valvotaan käyttöjärjestelmään pääsyä, ja jokaisella käyttäjällä tulee olla käytössään henkilökohtainen käyttäjätunnus, mikä on vain käyttäjän henkilökohtaista käyttöä varten. Salasanoja varten tulee olla hallintajärjestelmä, millä varmistutaan salasanojen riittävästä turvallisuudesta ja laadusta. Järjestelmien turvamekanismit ohittavia sovellusten tulee valvoa tarkasti. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Käyttämättömien istuntojen tulee sulkeutua, kun ne ovat olleet passiivisina riittävän pitkään. Samoin suuren riskin sovelluksissa tulee rajoittaa yhteysaikaa, sikäli kun ne eivät oleellisesti häiritse järjestelmien käyttöä. Etätyössä tulee määrittää toimintaperiaatteet, joiden avulla suojaudutaan matkakäytön ja etäyhteyksien aiheuttamilta riskeiltä. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Järjestelmien perus- ja pääkäyttäjien pääsyä tietoihin tai sovellusten toimintoihin tulee rajoittaa määriteltyjen pääsynvalvontaperiaatteiden mukaisesti. Arkaluonteisille sovelluksille täytyy järjestää eristetty ympäristö, esimerkiksi ulkoverkosta eristetty lähiverkko. (ISO/IEC 27001 -tietoturvallisuusstandardi)

4.6 Tietojärjestelmien hankinta, kehitys ja ylläpito

Organisaatiolla on oltava selvillä liiketoimintaprosessit ja tarkka liiketoimintavaatimusten määrittely uuden tai olemassa olevan järjestelmän kehittämistä varten. Järjestelmää suunniteltaessa täytyy erityisesti huomioida syötettävien tietojen kelvollisuus oikeellisuuden ja asianmukaisuuden varmistamiseksi. Järjestelmään tulee ohjelmointivirheiden aiheuttamien vääristymien tai toimimattomuuksien minimoimiseksi kehittää tietojen oikeellisuustarkistukset. Samoin tulostetun tiedon oikeellisuudesta tulee huolehtia. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Tietojen salaamiseen on myös hyvä olla käytössä menetelmiä, joilla minimoidaan mahdollisuudet hyödyntää vääriin käsiin joutunutta tietoa. Tällöin myös salakirjoitusavaimilla tulee olla erikseen määritelty hallintamenettely. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Suojauksien olemassa oleviin järjestelmiin on oltava kunnossa. Organisaatiolla tulee olla menettelytavat, joilla valvotaan ohjelmistojen asentamista tuotannossa oleviin järjestelmiin, samoin kuin valvontatyökalut testiympäristöjen käyttöä varten. Ohjelmistojen ja järjestelmien lähdekoodeihin ei pitäisi olla pääsyä kuin erikseen määritetyillä käyttäjillä. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Tietojärjestelmien, käyttöjärjestelmien ja sovellusohjelmistojen päivitys ja muut muutokset ovat välttämätön osa organisaatioiden toimintaa ja kehitystä. Näiden toimien on kuitenkin oltava valvontamenettelyn alaisia, ja niiden aiheuttamat haitat ja mahdolliset tietovuotoriskit on minimoitava. Organisaation on harkittava, mitkä muutokset ovat liiketoiminnan kannalta oleellisia ja valvottava myös ulkoistettua ohjelmistokehitystä. Ajantasainen tieto tietojärjestelmien haavoittuvuuksista on tärkeää ja sen avulla voidaan arvioida järjestelmien käytöstä aiheutuvia riskejä. (ISO/IEC 27001 -tietoturvallisuusstandardi)

4.7 Tietoturvahäiriöiden ja liiketoiminnan jatkuvuuden hallinta

Kaikesta suunnittelusta ja ohjeistuksesta huolimatta aina on mahdollisuudet tahallisiin tai tahattomiin tietoturvahäiriöihin. Näiden raportoinnista tulee olla ohjeistus, kenelle ilmoitetaan ja miten, ja minkälaisiin toimiin tilanteessa ryhdytään. Organisaatiossa kaikilla käyttäjillä on velvollisuus raportoida mahdollisista ongelmista tai järjestelmien toimintavirheistä. Organisaatiolla on oltava määriteltynä menettelytavat häiriöihin reagoimiseksi asianmukaisella tavalla ja tehokkaasti. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Menettelytapoja kaivataan myös häiriöiden laadun, määrän ja niiden aiheuttamien kustannusten mittaamiseen ja seuraamiseen. Jos häiriö kohdistuu johonkin henkilöön tai organisaatioon, ja odotettavissa on oikeustoimia, on todistusaineiston kerääminen ja säilyttäminen hoidettava kyseisen lainkäyttöalueen todistusaineistoa koskevien sääntöjen mukaisesti. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Liiketoiminnan jatkuvuuden hallinnalla tavoitellaan mahdollisuuksia taata liiketoiminnan jatkuminen ja suojata prosesseja tietojärjestelmien häiriöiden tai katkosten vaikutuksilta. Tätä varten organisaation tulee kehittää tietoturvallinen jatkuvuussuunnitelma, minkä avulla toimintaa saadaan ylläpidettyä vaaditulla tasolla tietyn aikaa ja tiedot saadaan palautettua ja käyttövalmiiksi häiriön jälkeen. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Nämä suunnitelmat muuttuvat tietojärjestelmien tai käyttöympäristöjen muuttuessa. Myös testaamiseen täytyy kiinnittää riittävästi huomiota, millä on tarkoitus välttää odottamattomien ongelmien syntyminen häiriötilanteessa. (ISO/IEC 27001 -tietoturvallisuusstandardi)

4.8 Vaatimustenmukaisuus

Organisaatiolla on oltava menettelytavat, millä varmistetaan tietoturvallisuuden hallintajärjestelmän kaikkien sopimusten, sääntöjen ja ajantasaisen lainsäädännön mukaisuus. Näiden mukaan tulee varmistaa myös tietosuoja, yksityisyys ja väärinkäytön ehkäisy. Esimiesten vastuulla on vastuualueidensa turvamenettelyjen virheetön suorittaminen ja tietoturvallisuuspolitiikan ja -standardin vaatimusten mukainen noudattaminen. (ISO/IEC 27001 -tietoturvallisuusstandardi)

Tietoturvallisuusstandardin mukainen tietoturvallisuuden hallintajärjestelmä
Tietoturvallisuusstandardin lähtökohtana on organisaation tarpeisiin luotu tietoturvallisuuden hallintajärjestelmä. Valtiovarainministeriön Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI antaa ohjeessaan Tietoturvallisuuden hallintajärjestelmän arviointisuositus hyvää pohjaa oikeanlaiselle hallintajärjestelmälle. (Tietoturvallisuuden hallintajärjestelmän arviointisuositus)

VAHTI-ohjeet peräävät toimivan johdon vastuuta organisaation tietoturvallisuuden organisoimisesta. Johdon tulee olla tietoinen organisaation tietoturvallisuuden tasosta ja siihen kohdistuvista riskeistä. Johdolla tulee myös olla käytössään vertailevaa tietoa suhteessa toisiin saman alan, kokoluokan tai tietoteknisen infrastruktuurin omaaviin organisaatioihin. (Tietoturvallisuuden hallintajärjestelmän arviointisuositus)

Tietoturvallisuuden hallintajärjestelmä käsittää VAHTI-ohjeiden mukaan seuraavia osia:

- tietoturvallisuuspolitiikka ja sen soveltamisohjeet
- tietoturvallisuusstrategia

- riskianalyysi
- tietoturvallisuussuunnitelma ja -ohjeet
- jatkuvuus- ja toipumissuunnitelma
- tietojenkäsittelyn poikkeusolojen valmiussuunnitelma
- tietoturvallisuuden tulosohjaus
- tietoturvallisuuden toteutustapa, organisaatio ja vastuut
- vuosisuunnitelmat ja budjetit
- raportointi

(Tietoturvallisuuden hallintajärjestelmän arviointisuositus)

ISO/IEC 27000 -sarja kokonaisuudessaan

ISO/IEC 27000 on vaatimussarja, joka sisältää seuraavat osat:

- 27000 Principles and Vocabulary
- 27001 ISMS, vaatimusstandardi, tietoturvallisuuden hallintajärjestelmän pohja
- 27002 -menetelmäohje, korvaa aikaisemman 17799:2005 -menetelmäohjeen
- 27003 Implementation Guidance
- 27004 Measurement
- 27005 Risk Management

ISO/IEC 27001 on julkaistu vuonna 2005, ISO/IEC 27002 vuonna 2007. Sarjan muut osat ovat vielä työn alla, eikä aikataulua ole ilmoitettu. (ISO 27001 -koulutuksen luentomateriaali)

5 TIETOTURVALLISUUDEN SERTIFIOINTI

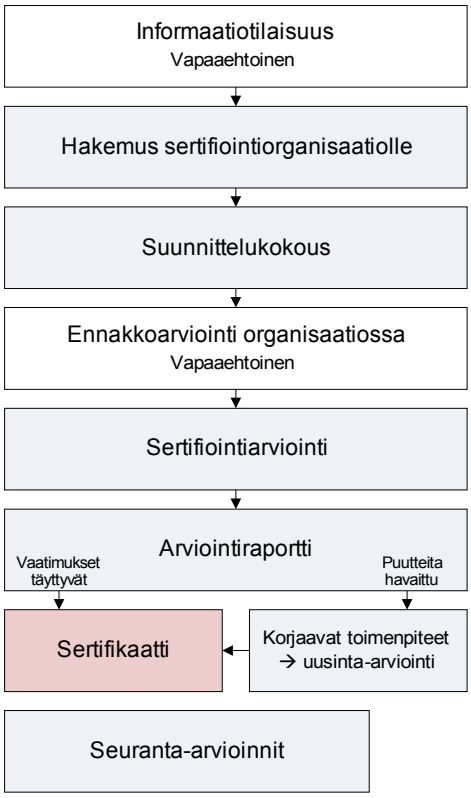
5.1 Sertifioinnin taustaa

Tietoturvallisuuden sertifiointi on osoituksena johdon sitoutumisesta ja organisaation pyrkimyksestä parempaan tietoturvallisuuteen ja laatuun. Sertifioinnilla tavoitellaan imagollista ja myös taloudellista hyötyä, sillä sertifikaatti on näkyvä asiakirja ja sitä voidaan pitää näkyvillä esimerkiksi markkinointimateriaaleissa, www-sivuilla ja sähköpostien allekirjoituksissa. Tämä ISO/IEC 27001 -tietoturvallisuusstandardi on kansainvälisesti tunnustettu ja arvokas kilpailuetu nopeasti kehittyvällä alalla ja muuttuvassa liiketoimintaympäristössä. (ISO 27001 -koulutuksen luentomateriaali)

Tietoturvallisuusstandardi lähtee toimivasta tietoturvallisuuden hallintajärjestelmästä. Sen käyttö edellä mainittujen hyötyjen lisäksi edesauttaa organisaatiota saavuttamaan toiminnan tehostamisen ja tuntemuksen kautta saavuttamaan kustannusetuja. Järjestelmä perustuu oikeaoppiseen ja hallittuun tietojärjestelmien käyttöön ja ylläpitoon, mikä yksinkertaistaa niiden hallintaa ja pienentää riskejä ongelmien syntyyn sekä nopeuttaa niistä aiheutuneiden seurausten korjaamista. (ISO 27001 -koulutuksen luentomateriaali)

5.2 Sertifiointiprosessi

Kaikkien hallintajärjestelmien sertifiointiprosessi on samanlainen. Kuvio 4 näyttää prosessin vaiheet vapaaehtoisesta informaatiotilaisuudesta sertifiointiin ja seuranta-arviointeihin.



Kuvio 4: Sertifiointiprosessi (ISO 27001 -koulutuksen luentomateriaali)

Hakemus

Sertifiointiprosessi alkaa varsinaisesti organisaation jätettyä sertifiointihakemuksen sertifiointia suorittavalle organisaatiolle. Hakemuksessa tulee näkyä hakemuksen kohteena oleva toiminta, eli mille järjestelmälle organisaatio hakee sertifikaattia. Lisäksi hakijan tulee toimittaa sertifiointiorganisaatiolle liiketoiminnastaan seuraavia tietoja:

- Organisaatio; osoitteet, yhteystiedot
- Prosessit
- Mahdolliset rajaukset
- Liikevaihto
- Toimintaa säätelevät määräykset, standardit ja lait
- Toiminnan erityispiirteet
- Aikaisemmat sertifioinnit
- Toivottu sertifiointiajankohta

(ISO 27001 -koulutuksen luentomateriaali)

Suunnittelukokous

Sertifiointiprosessin toinen vaihe on suunnittelukokous, missä käydään läpi tietoturvajärjestelmän tai laatujärjestelmän dokumentaatio, prosessit, johdonkatselmusmenettelyt ja niiden pöytäkirjat, sisäisten auditointien menettelyt ja niiden raportointi, sertifiointiarvioinnin ohjelma, riskienarvioinnin menettely ja tulokset sekä soveltamissuunnitelma. Näiden tietojen perusteella voidaan suorittaa vapaaehtoinen ennakkoarviointi, minkä perusteella saadaan kuva, kannattaako vielä varsinaista sertifiointiarviointia suorittaa. (ISO 27001 -koulutuksen luentomateriaali)

Sertifiointiarviointi

Sertifioinnin arviointivaiheessa arvioidaan, toimivatko järjestelmät esitettyjen dokumenttien mukaisesti. Arvioinnin tavoitteena on sekä standardin vaatimusten että oman liiketoiminnan asettamien lisävaatimusten täyttymisen toteaminen. Työ suoritetaan ottamalla pistokokeita ja etsimällä niiden avulla mahdollisia poikkeamia. (ISO 27001 -koulutuksen luentomateriaali)

Jos sertifiointiarvioinnissa ei havaita poikkeamia, sertifiointiorganisaatio voi suositella sertifikaatin myöntämistä. Poikkeamatilanteissa sertifiointiprosessi jatkuu antamalla lisäaikaa korjaaviin toimenpiteisiin. Yleisin aika poikkeamien korjaamiseksi on kolme kuukautta. Tämän jälkeen suoritetaan sertifiointiarviointi uudelleen. (ISO 27001 -koulutuksen luentomateriaali)

Arvioinneissa arvioidaan organisaation tietoisuutta ja toimintamalleja seuraavissa asioissa:

- Tietoisuus tuotteeseen tai palveluun liittyvistä asiakas- ja viranomaisvaatimuksista.
- Kyky tuottaa johdonmukaisesti nämä vaatimukset täyttäviä tuotteita tai palveluita.
- Prosessimainen toimintamalli.
- Painottuminen ongelmien välttämiseen, ei ainoastaan korjaamiseen.
- Järjestelmän tehokkuuden jatkuvan parantamisen toimiminen asetettujen tavoitteiden mukaisesti.

- Tietoturvallisuuden hallintajärjestelmän kattavuus ja tehokkuus.
- Riskienarviointi.
- Soveltamissuunnitelma, eli miten käyttöönotetuilla turvamekanismeilla hallitaan tietoturvariskejä.

(ISO 27001 -koulutuksen luentomateriaali)

Arviointiraportti

Arviointiraporttiin kirjataan mahdolliset sertifiointiarvioinnissa esille tulleet poikkeamat sekä yleisiä kehitysehdotuksia ja ratkaisuja. Poikkeamat luokitellaan seuraavasti:

- Vakava: Järjestelmä ei ole valmis. Toiminnoista löytyy useita esimerkkejä, joissa ei noudateta ISO/IEC 27001 -tietoturvallisuusstandardin vaatimuksia. Tämä edellyttää uusinta-arviointia.
- Lievä: Järjestelmästä löytyy pieniä ja satunnaisia poikkeamia ISO/IEC 27001 -tietoturvallisuusstandardin vaatimuksista tai ohjeistosta. Lievät poikkeamat eivät laatunsa vuoksi edellytä uusinta-arviointia.

(ISO 27001 -koulutuksen luentomateriaali)

Sertifiointipäätös

Sertifikaatti myönnetään, jos arvioinnissa ei ole tullut ilmi vakavia puutteita, tai kaikki arviointiraportissa havaitut poikkeamat on korjattu. Sertifikaatti sitoo organisaation jatkuvan parantamisen politiikkaan. ISO/IEC 27001 -tietoturvallisuusstandardin noudattamista tullaan seuraamaan kerran tai kaksi kertaa vuodessa ulkoisilla auditoinnella. Organisaatio sitoutuu suorittamaan myös sisäisiä auditointeja, missä omaehtoisesti varmistetaan tietoturvallisuuden hallintajärjestelmän toimivuus ja tietoturvallisuusstandardin noudattaminen. (ISO 27001 -koulutuksen luentomateriaali)

6 KOHDEYRITYKSEN KUVAUS

6.1 Autovahinkokeskus Oy

Autovahinkokeskus Oy (AVK) on auto- ja liikennevakuutustoimintaa harjoittavien vakuutusyhtiöiden omistama yritys, jonka tehtävänä on lunastettujen ajoneuvojen realisointi ja korjauskelvottomista ajoneuvoista purettujen varaosien myynti. AVK realisoi vuosittain n. 22 500 ajoneuvoa.

AVK toimii kahdessa toimipisteessä, Espoossa ja Pirkkalassa. Omaa henkilökuntaa on noin 50 henkilöä. Lisäksi AVK:lla on yhteistyökumppaneita, kuljetusliikkeitä ja välivarastoja ympäri Suomen, jotka hoitavat kuljetuksia kolaripaikoilta välivarastoille ja runkokuljetuksia välivarastoilta AVK:n toimipisteisiin. Muutamat välivarastot hoitavat myös ajoneuvojen realisointia omista toimipisteistään, jolloin niitä ei tarvitse kuljettaa Espooseen tai Pirkkalaan.

Yrityksen molemmissa toimipisteissä toimii ajoneuvo- ja varaosamyynnin asiakaspalvelupisteet, ajoneuvojen vastaanotto ja esikäsittely sekä purkamo. Lähes jokainen henkilökuntaan kuuluva käyttää työssään tietotekniikkaa, ja näin henkilöstön tietotekninen osaaminen ja tietoturvallisuus ovat keskeisiä asioita päivittäisessä työssä.

6.2 AVK:n tietojärjestelmät ja niiden käyttöoikeudet

AVK:lla on käytössään yleisten toimistosovellusten lisäksi lukuisia omaan liiketoimintaan räätälöityjä järjestelmiä, kuten taloushallinto-ohjelmisto, operatiivinen tietojärjestelmä, ekstranet, intranet ja www-sivusto.

Operatiivinen tietojärjestelmä – Tessu

AVK:n keskeisin päivittäinen työkalu on Tessu-tietojärjestelmä. Järjestelmää käytetään ajoneuvojen ja varaosien myyntiin, tietojen ylläpitoon ja laskutukseen. Järjestelmä seuraa ajoneuvon kulkua ja kirjattuja tapahtumia koko realisointiprosessin ajan.

Tessu pitää sisällään kaikki ajoneuvon tekniset tiedot, myyntilupatiedot, hinnoitteluhistorian, asiakkaiden lähettämät tarjoukset, vakuutusyhtiöiden määrittelemät myyntiehdot ja ajoneuvon logistiikkaa koskevat tiedot. Tessu huolehtii myös kaikesta asiakastietojen, varaosien, ja myyntiä koskevien tietojen ylläpidosta.

Tessu lähettää ja vastaanottaa tietoja reaaliaikaisesti ja eräajoina muista tietojärjestelmistä. Näitä järjestelmiä ovat mm. AVK:n omat tietojärjestelmät sekä vakuutusyhtiöiden tietojärjestelmät.

Tessu-tietojärjestelmän yhteyteen on toteutettu myös samaa tietokantaa käyttäviä apuohjelmia ja raportointityökaluja, joiden tehtävänä on poimia tietokannasta liiketoiminnan kannalta kurantteja tietoa ja tuottaa niistä raportointimateriaalia organisaation johdon käyttöön.

Ekstranet

Ekstranet on AVK:n yhteistyökumppaneita varten luotu järjestelmä, jonka kautta vahinkotarkastajat laativat sähköisesti kuljetustilauksia kuljetusliikkeille, jotka hyväksyvät ja kirjaavat ajoneuvojen tapahtumat järjestelmään. Järjestelmä automatisoi ajoneuvon saapumiseen liittyvää logistista prosessia, sillä koko prosessi hallinnoidaan tämän tietojärjestelmän avulla.

WWW-sivusto

AVK:n WWW-sivut pitävät sisällään yrityksen esittelyn sekä ajoneuvo- ja varaosamyynnin osat. Alla on lyhyesti lueteltuna ominaisuuksien pääpiirteitä. WWW-sivuilla on AVK:n toiminnan esittely sekä myynnissä olevat ajoneuvot ja varaosat. Rekisteröityneet käyttäjät voivat sopia myös sähköisistä tarjouksista. Sivuilla on

myös muita palveluita, kuten ajoneuvopäivystäjä, mitä käyttäen asiakas saa ilmoituksen hakuehtojensa mukaisen ajoneuvon saapumisesta myyntiin.

Intranet

Intranet on AVK:n sisäiseen käyttöön kehitetty tietojärjestelmä, jonka suunnittelu ja toteutus pohjautuu oman henkilöstön tiedonhaun ja tiedottamisen tarpeisiin. Järjestelmän käyttäjiä ovat ainoastaan AVK:n oma henkilökunta, ja järjestelmän ylläpidosta ja kehittämisestä huolehtii tällä hetkellä AVK:n hallinto. Järjestelmä ei ole yhteydessä muihin AVK:n tietojärjestelmiin, vaan toimii itsenäisenä tiedonhakukanavana.

Taloushallinnon järjestelmät

Taloushallintoa varten on oma ohjelmisto, joka toimii kirjanpidon ja reskontran työkaluna. Ohjelmisto ei ole yhteydessä muihin tietojärjestelmiin, vaan toimii itsenäisenä järjestelmänä.

Tietojärjestelmien käyttöoikeudet

AVK:n henkilökunnalla sekä sidosryhmien edustajilla ja asiakkailla on henkilökohtaiset käyttäjätunnukset tarvitsemiinsa järjestelmiin. Järjestelmiin ei ole olemassa ns. yleistunnuksia, mitä käyttämällä pääsisi anonyyminä käsiksi järjestelmien tietoihin. Käyttäjätunnusten luominen ja muuttaminen tapahtuu keskitetysti järjestelmiä ylläpitävän henkilön kautta. Käyttäjän oikeudet eri tietoihin määritellään tunnuksia perustettaessa ja niitä voidaan tarvittaessa muuttaa tarpeen mukaan.

6.3 AVK:n sertifiointitavoitteiden taustaa

AVK on aloittanut toimintansa vuonna 1966 omistamiensa vakuutusyhtiöiden toimesta ja alansa ainoana toimijana. Ajan kuluessa vakuutusyhtiöiden toiminta ja omistajasuhteet ovat muuttuneet merkittävästi, ja yhtiöiden omat sekä AVK:ta koskevat vaatimukset ovat kasvaneet kohti kansainvälisiä laatuvaatimuksia. Tällä hetkellä käytössä oleva ISO 14001 -standardin mukainen ympäristöjärjestelmä on otettu käyttöön ja sertifioitu vakuutusyhtiöiden vaatimuksesta. (Keränen 2009)

Laatuvaatimukset kasvavat edelleen ja alalle on ollut tulossa uusia toimijoita, kuten alun perin suomalainen Lars Krogius Oy ja ruotsalainen Yallotrade AB. Näiden yritysten tarkoituksena oli kilpailla realisointiyhteistyöstä vakuutusyhtiöiden kanssa. Molemmat yritykset ovat tällä hetkellä luopuneet tästä hankkeesta, mutta liiketoimintaympäristö elää silti jatkuvasti. (Keränen 2009)

Vakuutusyhtiöiden jatkuva kansainvälistyminen ja liiketoiminta-alueiden kasvaminen vaikuttaa myös selkeästi ajoneuvojen realisointia koskevaan päätöksentekoon. Kotimaisuus ei ole merkittävä kilpailuvaltti, jos jokin ulkomainen toimija voi kansainvälisesti osoittaa olevansa tehokkaampi ja laadukkaampi toimija.

Vakuutusyhtiöiden liiketoiminta, kuten muukin kaupallinen liiketoiminta, edellyttää korkeaa tietoturvallisuutta ja asianmukaista suhtautumista tietoturvallisuuteen. Lunastettujen ajoneuvojen ja niiden käsittelyyn liittyvät tiedot ovat luottamuksellisia. Tietoturvaloukkaukset ovat merkittävä riski, ja oletettavasti niiden riskien vähentäminen tulee olemaan yksi suurimpia yhteistyön edellyttämiä vaatimuksia.

On luultavasti ajan kysymys, milloin vakuutusyhtiöt alkavat edellyttää yhteistyökumppaneiltaan liiketoimintaansa liittyvien standardien noudattamista. Yritysten kansainvälistyessä ja ulkomaisten toimijoiden tullessa kotimaahamme toimivat ja valvotut laatujärjestelmät ovat merkittävä kilpailuetu ja tulevaisuudessa myös yhteistyön vaatimus.

7 TUTKIMUKSEN TOTEUTUS JA TUTKIMUSTULOKSET

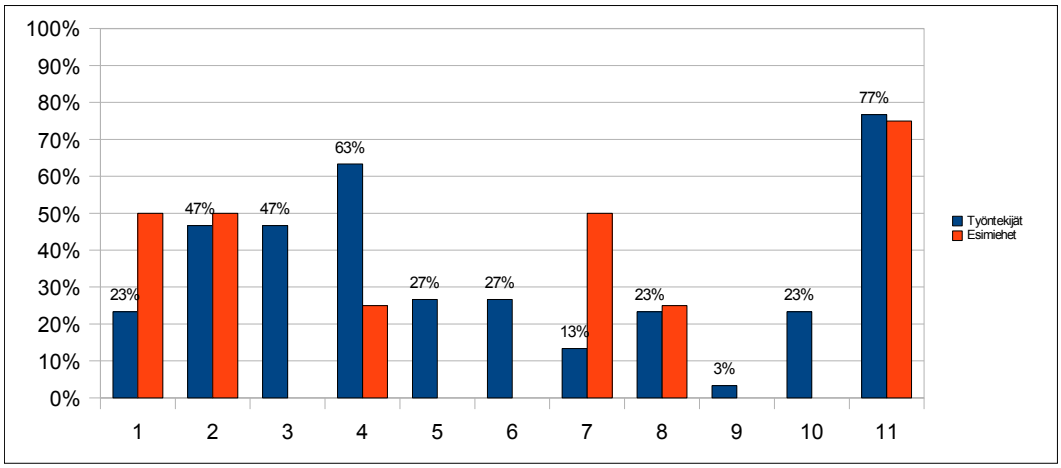
7.1 Henkilöstön suhtautuminen tietoturvaan

Henkilöstön asenteita ja tietoturvan tuntemusta selvitettiin strukturoidulla kyselylomakkeella (Liite 1). Lomake on osa Valtion teknillisen tutkimuskeskuksen (VTT) pk-yritysten riskienhallinnan työvälinesarjaa. Lomakkeella selvitettiin, miten henkilöstöä on ohjeistettu tietojärjestelmien ja laitteiden turvalliseen käyttöön ja miten tietojärjestelmiä ylläpidetään ja valvotaan. Kyselyyn osallistui yhteensä 34 henkilöä, joista neljä oli esimiehiä.

Esimiehet ja työntekijät vastasivat käyttäen samaa lomaketta esimiesten vastatessa kaikkiin kysymyksiin ja työntekijöiden vastatessa kohtiin 1 ja 5. Vastaukset käsiteltiin anonyymeinä, työntekijät ja esimiehet arvioitiin kuitenkin erikseen.

Henkilöstön tietoisuus tietoriskeistä

Kuviossa 5 kuvataan työntekijöiden ja esimiesten myönteiset vastaukset liitteessä 1 olevan kysymyslomakkeen ensimmäiseen kysymyssarjaan.



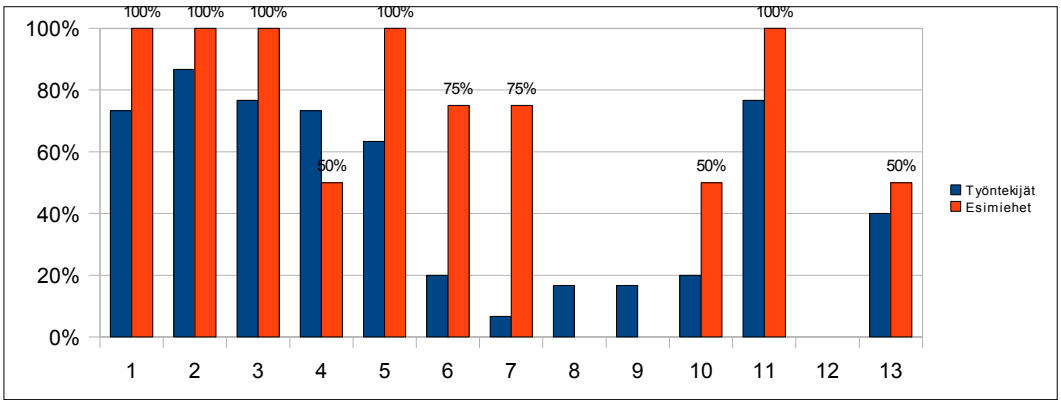
Kuvio 5: Henkilöstön tietoisuus tietoriskeistä.

Kysymys	Työntekijät	Esimiehet
1. Onko henkilöstölle koulutettu nykyaikaisen liiketoiminnan ja tuotekehityksen luottamuksellisuuteen ja tietosuojaan liittyviä yleispiirteitä?	23,00%	50%
2. Tunteeko henkilöstö yrityksen vastuut tietojen luottamuksellisuuden ja muun tietoturvallisuuden suhteen?	47%	50%
3. Onko kaikille selvää, millaisten tietojen suojaaminen on tärkeää?	47%	0%
4. Onko kaikille selvää, mitä yrityksen toiminnasta saa kertoa ulkopuolisille?	63%	25%
5. Onko yritykselle määritelty tietoturvaperiaatteet ja laadittu niiden toteuttamiseksi ohjeet?	27%	0%
6. Kattavatko ohjeet sähköisten tietojärjestelmien lisäksi suullisen viestinnän ja paperidokumenttien käsittelyn ja jakelun?	27%	0%
7. Onko henkilöstö koulutettu tunnistamaan tietoriskejä ja noudattamaan yrityksen turvakäytäntöjä?	13%	50%
8. Onko olemassa menettely tietoturva-asioiden käsittelyä varten?	23%	25%
9. Onko jokainen työntekijä allekirjoittanut tietojen käyttösäännöt?	3%	0%
10. Ovatko tietojen luokitteluohjeet ja käytännöt osa arkipäivän toimintaa?	23%	0%
11. Tietääkö henkilöstö, minne ilmoittaa havaitsemistaan tietoturvarikkeistä tai käytäntöjen puutteista?	77%	75%

Taulukko 3: Henkilöstön tietoisuus tietoriskeistä.

Tutkimuksessa tulee ilmi, että tietojenkäsittelyyn ja tietoturvaan kaivataan ohjeistusta ja koulutusta. Samoin tietoisuus siitä, mihin häiriötilanteissa raportoidaan, on puutteellista. Työntekijöiden ja esimiesten välillä ei ole suuria käsityseroja henkilöstön tietoturvatietoisuudesta.

Tietojärjestelmien ja tietokoneiden käyttö



Kuvio 6: Tietojärjestelmien ja tietokoneiden käyttö

Kysymys	Työntekijät	Esimiehet
Onko henkilöstöllä riittävä perusosaaminen järjestelmien käyttöön?	73%	100%
Saavatko työntekijät häiriö- ja virhetilenteissa apua ja neuvontaa?	87%	100%
Käyttääkö jokainen työntekijä työssään vain omaa käyttäjätunnustaan?	77%	100%
Onko varmistettu turvallisen salasanan muodostaminen?	73%	50%
Onko estetty mahdollisuus muilta työntekijöiltä lukea tai muuttaa käyttäjän tietoja käyttäjän huomaamatta?	63%	100%
Onko varmuuskopioiden ottamiseen ja palauttamiseen olemassa toimintaohjeet?	20%	75%
Valvotaanko varmuuskopioiden ottamista?	7%	75%
Onko Internetin käyttö ohjeistettu?	17%	0%
Onko sähköpostin käyttö ohjeistettu?	17%	0%
Onko virustentorjuntamenettelyt ohjeistettu työ- sekä kotikoneiden osalta?	20%	50%
Ovatko virusohjelmien ja muiden vastaavien päivitykset automatisoitu?	77%	100%
Salakirjoitetaanko kannettavilla laitteilla (tietokoneet, kämmentietokoneet yms.) olevat luottamukselliset tiedot?	0%	0%
Onko käyttäjiä kielletty asentamasta yrityksen verkkoon tai työasemiin ulkopuolisia ohjelmistoja tai laitteita?	40%	50%

Taulukko 4: Tietojärjestelmien ja tietokoneiden käyttö.

Vaikka lähes jokainen henkilö käyttää päivittäisissä työssään tietojärjestelmiä ja tietokoneita, on niiden käytön ohjeistuksessa puutteita. Myös käyttöohjeita ja koulutuksia tarvitaan laitteiden ja ohjelmistojen käyttöä varten.

Työsuhdeasiat ja henkilöstön toimintatavat

Liitteessä 1 olevan kyselylomakkeen kohtiin 2-4 pyydettiin esimiehiltä vastauksia. Kohdat käsittelevät työsuhteen aloittamista ja päättämistä sekä henkilöstön tietoturvallisia toimintatapoja. Vastaukset olivat hyvin yksimielisiä.

Tutkimuksessa tuli esille, että tietoturva-asioita ei tuoda riittävästi esille uuden henkilön aloittaessa. Tietoturvapolitiikkaa, tietojärjestelmien käyttöön ja tietojen käsittelyyn liittyvää ohjeistusta ei aina sisällytetä perehdytykseen. Sen sijaan työsuhteen päättymiseen liittyvät seikat, kuten tietojärjestelmien käyttöoikeuksien

poistaminen ja työvälineiden palauttaminen on oikein organisoitua. Myös siitä pidetään huolta, että mahdollinen irtisanomistilanne on lainmukainen ja perusteltu.

7.2 ISO/IEC 27001 -tietoturvallisuusstandardin vaatimukset

Liitteessä 2 olevassa taulukossa on kuvattu ISO/IEC 27001 -tietoturvallisuusstandardin valvontatavoitteet ja niiden toteutuminen AVK:lla. Toteutumisen arviointiin on käytetty AVK:lla käytettävissä olevaa tietoa sekä haastatteluja (Puro & Ranttila 2009). Taulukossa on merkitty osittain tai kokonaan toteutumattomat valvontatavoitteet termein ”tulee toteuttaa” tai ”tulee laatia.”

Tutkimuksessa käytiin läpi kaikki ISO/IEC 27001 -tietoturvallisuusstandardin 133 valvotatavoitetta ja vertailitiin niiden toteutumista AVK:lla. Tutkimuksessa kävi ilmi, että tietojärjestelmien ja laitteiden tietoturvallisuus on hyvää tasoa, mutta haastattelututkimuksen tulosten tavoin puutteita löytyi henkilöstön osaamisesta, käyttötottumuksista sekä dokumentoinnista.

Tietojärjestelmien ongelmakohtia olivat mm. käyttäjien roolitukset, yksittäistapauksissa heikot salasanat, siirrettävien tietovälineiden suojaukset sekä kannettavien tietokoneiden salaukset ja suojaukset. Palvelinten ja tietoliikenneyhteyksien suojaukset oli hoidettu hyvin ja niiden toimintaa valvottiin säännöllisesti ISO/IEC 27001 -tietoturvallisuusstandardin edellyttämällä tavalla. Myös tietojärjestelmien kehittäminen organisoitiin oikein.

Henkilöstön osaamisen puutteet tulivat esille molemmissa tutkimuksissa. Ongelmia tuottavat pääasiassa epävarma tietotekniikan käyttö ja siihen liittyvät riskit, kuten liian heikot salasanasuojaukset, väärät suojausasetukset ja yleisesti tieto siitä, millaisten tietojen suojaaminen on tärkeää. Tutkimuksissa tuli esille selkeä koulutus- ja perehdytystarve sekä tietotekniikkaan että tietoturvallisuuteen. Peruskäyttäjän päivittäisiin työvälineisiin kuuluvat operatiivinen tietojärjestelmä, toimistosovellukset sekä muutamat apuohjelmat.

Dokumentointi ja toiminnan suunnittelua tulee kehittää. Liiketoiminnan prosesseja ei vielä ole kuvattu kattavasti eikä riskianalyysiä tai toipumissuunnitelmaa ole tehty. Myöskään menettelytapoja laite- tai ohjelmistohankintoja varten ei vielä ole. Tietoturvapolitiikka ei ole kokonaisuudessaan ajan tasalla, eikä se ole kaikkien saatavilla. Sitä vastoin liiketoiminnan vaatimukset sekä yhteistyö viranomaisten ja erityisintressiryhmien kanssa toimii oikein.

Tätä opinnäytetyötä tehdessä Suomessa ei ole vielä montaa tietoturvallisuutta sertifioinutta organisaatiota. AVK:lla on hyvä tilaisuus osoittaa olevansa tässä asiassa laadukas yhteistyökumppani ja toimivansa jatkuvan kehittämisen periaatteiden mukaisesti. Standardien mukaisten järjestelmien luominen ja ylläpito lähtee aina organisaation liiketoiminnan tarpeista, joten organisaation koko tai toimiala ei ole ratkaisevaa sertifioinnin kannalta.

AVK:lla on hyvät edellytykset luoda toimiva tietoturvallisuuden hallintajärjestelmä. Organisaatio on matala ja liiketoiminta-alueet on hyvin vastuutettuja, mikä nopeuttaa merkittävästi järjestelmän käyttöönottoa ja siihen liittyvää henkilöstön perehdytystä.

8 YHTEENVETO

Tietoturvallisuus on osa jokaisen organisaation liiketoimintaa ja riskienhallintaa. Liiketoiminnan jatkuvuus ja laadukas toiminta edellyttää asiallista huolehtimista tietoturvallisuudesta. Se vaikuttaa yrityksen imagoon ja joissakin tilanteissa osoitus tietoturva-asioiden oikeasta hoitamisesta voi olla edellytyksenä sopimuksen ja liikekumppanuuden syntymiselle. Liiketoiminnan laadusta riippuen tietoturvallisuuden tasoon voi olla myös lakeihin ja muihin sopimuksiin nojaavia vaatimuksia.

Tietoturvallisuudesta huolehtiminen vaatii aina panostusta, mutta oikein organisoituna se on kallisarvoinen voimavara ja kilpailuetu. Vastuu tietoturvallisuudesta huolehtimisesta on organisaation johdolla, mutta jokainen organisaation jäsen vaikuttaa siihen omalla toiminnallaan.

Tietoturvallisuuden oleellinen osa on liiketoiminnan prosessien tunteminen ja riskien tiedostaminen. Riskejä ei voi poistaa kokonaan, mutta niiden todennäköisyys ja vaikutukset on käsiteltävä huolellisesti sekä laadittava suunnitelmat niiden torjumiseksi ja vahinkojen minimoimiseksi. Tietoriskit ovat muiden riskien tavoin mukana kaikissa liiketoiminnan prosesseissa.

Autovahinkokeskus Oy:n tavoitteena on luoda toimiva tietoturvallisuuden hallintajärjestelmä käyttäen pohjana ISO/IEC 27001 -tietoturvallisuusstandardin vaatimuksia. Standardi on yhteensopiva muiden hallintajärjestelmien kanssa ja soveltuu mille tahansa toimialalle sekä minkäkokoiseen organisaatioon tahansa. Kun tietoturvallisuus on standardin edellyttämällä tasolla, on AVK:lla mahdollisuus hakea tietoturvasertifikaattia.

Opinnäytetyö selvitti AVK:n tietoturvallisuuden nykytilaa tietojärjestelmien sekä henkilöstön tietoturvatietoisuuden näkökulmasta. Tutkimuksen mukaan tietojärjestelmien turvallisuus on tietoturvallisuuden kannalta hyvää tasoa, teknisissä ratkaisuissa korjattavia asioita tuli vain jonkin verran esille. Näiden korjaaminen edellyttää paitsi laitteistojen ja ohjelmistojen päivittämistä ja ominaisuuksien käyttöönottoa, myös yhteityötä tietoliikenneverkkoa ylläpitävän yhteistyökumppanin kanssa. Heidän suhtautumisensa Autovahinkokeskuksen tietoturvallisuuden kehittämiseen oli haastattelun (Ranttila 2009) mukaan myönteistä, ja moniin teknisiin kysymyksiin oli olemassa suoran käden ratkaisu.

Dokumentoinnissa ja tietojärjestelmien valvonnassa on myös parannettavaa. ISO/IEC 27001 -tietoturvallisuusstandardi edellyttää paljon tietoturvallisuuteen vaikuttavien asioiden suunnittelua, kirjaamista ja dokumentointia toimenpiteiden toteuttamisen ohella. Kun nämä on tehty, tulee toimenpiteitä ja niiden dokumentaatioita katselmoida suunnitelluin väliajoin. Liiketoiminnan prosessit on kuvattava, tietoturvapolitiikka on päivitettävä ajan tasalle ja saatava koko henkilöstön käyttöön. Lisäksi on laadittava liiketoimintaprosesseihin perustuvat riskianalyysit sekä toipumissuunnitelma.

Henkilöstön tietoturvallisuuden osaamisessa oli paljon kehitettävää. Suurin osa haastatelluista ei ollut saanut tietojärjestelmien käyttökoulutusta eikä perehdytystä tietoturvallisuudesta. Myös yleinen tietoisuus siitä, mitkä ovat organisaatiossa suojattavia asioita, oli puutteellista. Tällaiset asiat voivat vaikeuttaa päivittäisten työtehtävien hoitamista ja voivat aiheuttaa todellisia tietoturvariskejä. Näitä ei teknisin menetelmin pysty helposti poistamaan, koska tietojärjestelmien heikko kohta on aina kaikista suojaustoimista huolimatta käyttäjä. Väärin toimiessaan käyttäjä voi aiheuttaa korjaamatonta vahinkoa.

Näihin asioihin voidaan kuitenkin myönteisesti vaikuttaa järjestämällä koulutusta tietotekniikan ja tietojärjestelmien käyttöön ja perehdyttämällä tietovälineiden turvallisiin käyttötapoihin.

Tutkimuksen aikana tuli esille selkeä tahto tietoturvallisuuteen vaikuttavien asioiden kehittämiseksi. Sekä työntekijät että johto ovat tietoisia kehitystarpeista, ja käyttäjät vaikuttivat suhtautuvan järjestettäviin koulutuksiin ja perehdytyksiin myönteisesti ja varauksettomasti.

AVK:lla on näiden tutkimusten pohjalta hyvät edellytykset luoda ISO/IEC 27001 -tietoturvallisuusstandardin mukainen tietoturvallisuuden hallintajärjestelmä ja aloittaa mahdollinen tietoturvallisuuden sertifiointiprosessi. Kehityksen myötä paitsi tietoliikenteen ja tietojärjestelmien tietoturvallisuus paranee, myös työympäristö muuttuu tietoturvallisemmaksi sekä henkilöstön tietoisuus suojausta vaativista asioista paranee.

LÄHTEET

Painetut lähteet

Inspecta Sertifointi Oy. 2008. Tietoturvallisuusstandardi ISO 27001 -kolutus. Luentomateriaali.

Kajava, J. 2001. Tietoturvan merkitys IT-sidonnaisissa liiketoimintaprosesseissa. Esitys.

Kerko, P. 2001. Turvallisuusjohtaminen. Jyväskylä: PS-Kustannus

Sulosaari, A. 2004. Tietoturva-ammattilaisen osaamistarvekartoitus. Diplomityö

Suomen standardisoimisliitto SFS. 2008. ISO/IEC 27001 -tietoturvallisuusstandardi liitteineen

Valtiovarainministeriö. 2003. Tietoturvallisuuden hallintajärjestelmän arviointisuositus. Helsinki: Edita Prima Oy

Sähköiset lähteet

Autovahinkokeskus Oy. 2009. Autovahinkokeskus. Autovahinkokeskus Oy [viitattu 3.4.2009]. Saatavissa http://www.avk.fi.

CERT-FI. 2009. CERT-FI – CERT-toiminta. Viestintävirasto [viitattu 19.3.2009]. Saatavissa http://www.cert.fi/palvelut/toiminta.html.

Haastattelut

Keränen, O. 2009. Tutkija. Autovahinkokeskus Oy. Haastattelu 19.3.2009.

Puro, K. 2009. Hallintopäällikkö. Autovahinkokeskus Oy. Haastattelu 3.4.2009.

Ranttila, M. 2009. Plus Verkot Oy. Haastattelu 26.-28.3.2009

LIITTEET

LIITE 1 VTT: Pk-yritysten riskienhallinnan työvälinesarja – Henkilöstön tietoisuus ja toimintatavat -kyselylomake

LIITE 2 ISO/IEC 27001 -tietoturvallisuusstandardin valvontatavoitteet ja niiden vaatimusten toteutuminen

LIITE 1.

Henkilöstön tietoisuus ja toimintatavat

Tarkistuslista arkipäivän tietojenkäsittelytapojen riskien tunnistamiseksi.

Yritys:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa yrityksen toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

Henkilöstön tietoisuus tietoriskeistä

	Kyllä	Ei	Ei koske meitä
Onko henkilöstölle koulutettu nykyaikaisen liiketoiminnan ja tuotekehityksen luottamuksellisuuteen ja tietosuojaan liittyviä yleispiirteitä?	☐	☐	☐
Tunteeko henkilöstö yrityksen vastuut tietojen luottamuksellisuuden ja muun tietoturvallisuuden suhteen?	☐	☐	☐
Onko kaikille selvää, millaisten tietojen suojaaminen on tärkeää?	☐	☐	☐
Onko kaikille selvää, mitä yrityksen toiminnasta saa kertoa ulkopuolisille?	☐	☐	☐
Onko yritykselle määritelty tietoturvaperiaatteet ja laadittu niiden toteuttamiseksi ohjeet?	☐	☐	☐
Kattavatko ohjeet sähköisten tietojärjestelmien lisäksi suullisen viestinnän ja paperidokumenttien käsittelyn ja jakelun?	☐	☐	☐
Onko henkilöstö koulutettu tunnistamaan tietoriskejä ja noudattamaan yrityksen turvakäytäntöjä?	☐	☐	☐
Onko olemassa menettely tietoturva-asioiden käsittelyä varten?	☐	☐	☐
Onko jokainen työntekijä allekirjoittanut tietojen käyttösäännöt?	☐	☐	☐
Ovatko tietojen luokitteluohjeet ja käytännöt osa arkipäivän toimintaa?	☐	☐	☐
Tietääkö henkilöstö, minne ilmoittaa havaitsemistaan tietoturvarikkeistä tai käytäntöjen puutteista?	☐	☐	☐

Uudet työntekijät

	Kyllä	Ei	Ei koske meitä
Tarkistetaanko uusien työntekijöiden taustat ennen työsuhteen alkamista?	☐	☐	☐
Ovatko tietoturva-asiat mukana uusien työntekijöiden perehdyttämisessä?	☐	☐	☐
Selvitetäänkö myös uusille ja väliaikaisille työntekijöille yrityksen tietoturvapolitiikan ja vaitiolositoumuksen merkitys?	☐	☐	☐
Allekirjoittavatko työntekijät erillisen sitoumuksen tietojen ja järjestelmien käytöstä sekä tietojen palauttamisesta työsuhteen jälkeen?	☐	☐	☐

ESR Työsuojelurahasto

Työsuhteen päättyminen

	Kyllä	Ei	Ei koske meitä
Onko suunniteltu toimenpiteet, joilla varmistetaan tietoturvallisuus työsuhteiden päättyessä?	☐	☐	☐
Onko henkilön irtisanoutumistilanteessa esimiehellä tieto kaikista henkilön käyttäjätunnuksista ja käyttöoikeuksista, joiden voimassaolo tulee poistaa?	☐	☐	☐
Huolehditaanko, että kaikki työntekijän käytössä olleet työ-, tallennusvälineet sekä yritystä koskevat asiakirjat palautetaan yritykselle?	☐	☐	☐
Onko varauduttu työntekijöiden riitaisaan irtisanoutumiseen tai irtisanomiseen?	☐	☐	☐
Onko irtisanomistilanteissa varmistettu, että irtisanomisperuste on lainmukainen ja dokumentein perusteltavissa?	☐	☐	☐

Henkilöstön toimintatavat

	Kyllä	Ei	Ei koske meitä
Käsittelevätkö työntekijät työhönsä liittyviä, luottamuksellisia tietoja tarkoituksenmukaisesti?	☐	☐	☐
Ovatko yrityksen keskeiset tiedot suojattu mm. rajaamalla niiden saatavuus ja määrittelemällä niiden käyttöoikeudet?	☐	☐	☐
Onko minimoitu mahdollisuus myydä tai luovuttaa yritykselle keskeisiä tietoja ja dokumentteja?	☐	☐	☐
Ovatko yrityksen sisäiset valvontajärjestelmät asianmukaiset (työnvalvonta, tilojen valvonta, tietojen käytön ja tietojärjestelmien valvonta)?	☐	☐	☐
Onko työntekijöiden omien töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)?	☐	☐	☐
Onko luottamuksellisten tietojen säilyttämiseen riittävästi lukittuja tiloja?	☐	☐	☐
Hoidetaanko jätepaperin keräys ja käsittely hallitusti?	☐	☐	☐
Ovatko puhelinkäyttäytymisohjeet olemassa?	☐	☐	☐
Onko toiminta tulipalon varalle ohjeistettu ja harjoiteltu?	☐	☐	☐
Onko varahenkilöjärjestelyistä huolehdittu?	☐	☐	☐

Tietojärjestelmien ja tietokoneiden käyttö

	Kyllä	Ei	Ei koske meitä
Onko henkilöstöllä riittävä perusosaaminen järjestelmien käyttöön?	☐	☐	☐
Saavatko työntekijät häiriö- ja virhetilenteissa apua ja neuvontaa?	☐	☐	☐
Käyttääkö jokainen työntekijä työssään vain omaa käyttäjätunnustaan?	☐	☐	☐
Onko varmistettu turvallisen salasanan muodostaminen?	☐	☐	☐
Onko estetty mahdollisuus muilta työntekijöiltä lukea tai muuttaa käyttäjän tietoja käyttäjän huomaamatta?	☐	☐	☐
Onko varmuuskopioiden ottamiseen ja palauttamiseen olemassa toimintaohjeet?	☐	☐	☐
Valvotaanko varmuuskopioiden ottamista?	☐	☐	☐
Onko Internetin käyttö ohjeistettu?	☐	☐	☐
Onko sähköpostin käyttö ohjeistettu?	☐	☐	☐
Onko virustentorjuntamenettelyt ohjeistettu työ- sekä kotikoneiden osalta?	☐	☐	☐
Ovatko virusohjelmien ja muiden vastaavien päivitykset automatisoitu?	☐	☐	☐
Salakirjoitetaanko kannettavilla laitteilla (tietokoneet, kämmentietokoneet yms.) olevat luottamukselliset tiedot?	☐	☐	☐
Onko käyttäjiä kielletty asentamasta yrityksen verkkoon tai työasemiin ulkopuolisia ohjelmistoja tai laitteita?	☐	☐	☐

Laatijat: Tuija Kyrölä, Tietoturvakoulutus Oy, Matti Vuori, VTT Automaatio, Johannes Halmevuo. Copyright © 2004 VTT. Työvälinesarjan ovat pääosin rahoittaneet Euroopan sosiaalirahasto ja sosiaali- ja terveysministeriön työsuojeluosasto sekä Työsuojelurahasto. Versio 2.1. 17.9.2004. Tiedosto: kor-tie-henkilosto.doc

LIITE 2

VALVONTATAVOITTEET	TOTEUTUMINEN
Turvallisuuspolitiikka	
Tietoturvapolitiikka	
Tietoturvapolitiikan määrittelyasiakirja	Tietoturvapolitiikkaa varten tulee laatia johdon hyväksymä määrittelyasiakirja. Se tulee julkaista ja tiedottaa kaikille työntekijöille sekä järjestelmätoimittajille.
Tietoturvapolitiikan katselmointi	Tietoturvapolitiikan katselmointia varten tulee suunnitella aikataulu.
Tietoturvallisuuden organisoiminen	
Sisäinen organisaatio	
Johdon sitoutuminen tietoturvallisuuteen	Johto on näkyvästi sitoutunut tietoturvallisuuden kehittämiseen suunnittelemalla mm. tietotekniikan käyttökoulutuksia. Tietoturvallisuuden tarpeet huomioidaan myös tietojärjestelmien kehitystyössä.
Tietoturvallisuuden koordinointi	Tietoturvallisuuden edistäminen on kohdistettu tietojärjestelmistä vastaavalle henkilölle sekä verkkoa hallinnoivalle yhteistyökumppanille.
Tietoturvallisuutta koskevien vastuiden jako	Tietoturvavastuut tulee määritellä.
Tietojenkäsittelypalveluita koskeva hyväksyntäprosessi	Uusien tietojenkäsittelypalvelujen käyttöönottoa varten on laadittava menettelytapa.
Salassapitositoumus	Salassapitositoumukset on sisällytettynä työsopimukseen sekä muihin yhteistyösopimuksiin. Sopimuksia säilytetään turvallisessa paikassa. Säännöllinen katselmointi tulee suunnitella.
Yhteydet viranomaisiin	AVK:lla on toimiva yhteistyö liiketoimintaan liittyvien viranomaisten kanssa.
Yhteydet erityisintressiryhmiin	Koulutuksia ja perehdytyksiä järjestetään tarpeen mukaan.
Tietoturvallisuuden riippumaton arviointi	Auditointi suunnitellaan mahdollisen sertifiointiprosessin yhteydessä.
Ulkopuoliset tahot	
Ulkopuolisiin tahoihin liittyvien riskien tunnistaminen	Ulkopuolisten tahojen aiheuttamat organisaation tietoihin kohdistuvat riskit tulee luetteloida ja laatia turvamekanismit riskien pienentämiseksi.
Turvallisuudesta huolehtiminen asiakassuhteissa	Asiakkaat pääsevät käsiksi ainoastaan organisaation julkiseen tietoon www-sivuilla ja ekstranetissä.
Turvallisuudesta huolehtiminen kolmansien osapuolten sopimuksissa	Palvelujen ja järjestelmien toimittajien kanssa laaditaan aina sopimukset, missä mainitaan tietojärjestelmien käytön ehdot.

Suojattavien kohteiden hallinta	
Vastuu suojattavista kohteista	
Suojattavien kohteiden luetteloiminen	Suojattavat kohteet tulee luetteloida.
Suojattavien kohteiden omistajuus	Kaikille tiedoille ja tiedonkäsittelypalveluihin liittyville kohteille tulee nimetä omistaja.
Suojattavien kohteiden hyväksyttävä käyttö	Suojattavien kohteiden käyttöä varten tulee luoda säännöt.
Tiedon luokitus	
Luokitusohjeita	Tiedot tulee luokitella niiden arvon, lakisääteisten vaatimusten, arkaluonteisuuden sekä kriittisyyden perusteella.
Tiedon merkitseminen ja käsittely	Luokitteluperusteet tulee ottaa käyttöön ja sen perusteella laatia tiedon merkitsemistä ja käsittelyä koskeva ohjeistus.
Henkilöstöturvallisuus	
Ennen työsuhteen alkua	
Roolit ja vastuut	Jokainen organisaation työntekijä sekä ulkopuoliset käyttäjät tulee dokumentoida ja heille tulee määrittää yksilöllinen rooli tietojärjestelmien käyttäjinä.
Valinta	Jokaisen uuden käyttäjän tausta tulisi tarkistaa asiaan liittyviä lakeja, määräyksiä ja eettisiä normeja noudattaen. Tarkistuksessa tulee ottaa huomioon liiketoiminnalliset vaatimukset sekä käsiteltävien tietojen kriittisyys.
Työsopimuksen ehdot	Työsopimuksien ehtojen tulee sisältää henkilöiden sekä organisaation vastuut tietoturvallisuudesta. Nämä pitää sisällyttää työsopimuksiin.
Työsuhteen aikana	
Johdon vastuu	Johdon tulee edellyttää, että työntekijät sekä ulkopuoliset tietojärjestelmien käyttäjät noudattavat turvallisuutta organisaatioon luotujen periaatteiden ja menettelytapojen mukaisesti.
Tietoturvatietoisuus, -koulutus ja -harjoittelu	Tietoturvatietoisuutta tulee parantaa koulutuksen ja perehdyttämisen avulla.
Sanktiomenettelyt	Turvasäännösten rikkomusta varten tulee luoda sanktiomenettelyt.
Työsuhteen päättäminen tai muuttaminen	
Päättämisvastuut	Yrityksen johto päättää työsuhteiden muuttamisesta tai päättämisestä.
Suojattavien kohteiden palauttaminen	Esimiehet valvovat suojattavien kohteiden, kuten puhelimien, kannettavien tietokoneiden ja avainten, palautusta

Käyttöoikeuksien poistaminen	Kaikkien käyttäjien käyttöoikeudet tietojärjestelmiin tulee poistaa käyttäjän työ- tai sopimussuhteen päättyessä. Henkilön toimenkuvan muuttuessa myös käyttöoikeudet tietojärjestelmiin tulee tarkastaa.
Fyysinen turvallisuus ja ympäristön turvallisuus	
Turva-alueet	
Fyysinen turva-alue	Tietoja sisältävät laitteet ja muut tietovälineet on sijoitettu lukittuihin tiloihin, joihin on pääsy ainoastaan henkilökunnan avaimilla. Työaikana asiakaspalvelupisteet ovat aina miehitettyinä ovien ollessa lukitsemattomina.
Kulunvalvonta	Jokaisella on käytössään henkilökohtainen avain.
Toimistojen, tilojen ja laitteistojen suojaus	Tiloihin pääsee ainoastaan henkilökohtaisilla avaimilla ja työajan ulkopuolella käytössä on kameravalvonta ja liiketunnistimet.
Suojaus ulkoisia ja ympäristön uhkia vastaan	Tiloissa liikkuminen on rajoitettua ja valvottua.
Turva-alueilla työskentely	Parannettavaa.
Julkinen pääsy, toimitukset ja kuormausalueet	Yleisillä paikoilla liikkuminen on valvottua ja niistä ei ole vapaata kulkuyhteyttä turva-alueille.
Laiteturvallisuus	
Laitteiden sijoitus ja suojaus	Palvelimet, kytkimet ja reitittimet on sijoitettu lukittuihin ja valvottuihin tiloihin.
Peruspalvelut	Palvelinten, kytkinten ja reitittimien toiminta on varmistettu UPS-laitteilla.
Kaapeloinnin turvallisuus	Tietoliikennekaapelit on sijoitettu seinien sisään ja listoihin, kytkennät ovat lukituissa ristikytkentäkaapeissa.
Laitteiden huolto	Verkkoa hallinnoiva yhteistyökumppani valvoo verkon ja palvelinten toimintaa jatkuvasti, lisäksi ohjelmistopäivitykset tehdään säännöllisin väliajoin.
Toimitilojen ulkopuolelle vietyjen laitteiden turvallisuus	Toimitilojen ulkopuolella käytetään enimmäkseen kannettavia tietokoneita, missä on mahdollisuus kiintolevyjen salakirjoitukseen. Myös muut tietovälineet voidaan suojata teknisin salausmekanismein.
Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen	Työasemien ja muiden laitteiden muistit tyhjennetään joko ohjelmallisesti tai fyysisesti tuhoamalla ennen laitteen käytöstäpoistamista.
Suojattavien kohteiden siirtäminen pois työpaikalta	Laitteita, tietoaineistoja tai ohjelmia ei pääsääntöisesti kuljeteta työpaikan ulkopuolelle.

Tietoliikenteen ja käyttötoimintojen hallinta	
Menettelyohjeet ja velvollisuudet	
Kirjalliset menettelyohjeet	Kirjallisia menettelyohjeita ei vielä ole.
Muutosten hallinta	Kehityspiirteet tuotetaan testattaviksi kehitysympäristöön, testataan testaussuunnitelman mukaisesti ja siirretään tuotantoon.
Tehtävien eriyttäminen	Tietojärjestelmissä on määritettyinä käyttäjätasot, minkä mukaan käyttäjillä on pääsy oman työtehtävänsä mukaisiin tietoihin.
Kehitettävän, testattavana ja tuotannossa olevien palveluiden erottaminen	Kehitys- ja testausympäristöt ovat sijoitettu eri palvelimille.
Ulkopuolisten palvelujen toimittamisen hallinta	
Palvelujen toimittaminen	Käytössä ovat toimittajakohtaiset sopimukset sekä alan yleiset sopimusehdot.
Ulkopuolisten palvelujen tarkkailu ja katselmointi	Ulkopuolisia palveluita seurataan raportteja ja laskuerittelyjä käyttäen. Sisäisiä tai ulkoisia auditointeja ei tällä hetkellä suoriteta.
Ulkopuolisten palvelujen muutosten hallinta	Muutostilanteissa prosessien kriittisyys sekä liiketoiminnan häiriintymisen riskit otetaan tarkasti huomioon.
Järjestelmän suunnittelu ja hyväksyntä	
Kapasiteetin hallinta	Kapasiteetin käyttöä tarkkaillaan jatkuvasti. Kapasiteetin rajoitukset tulisi ottaa käyttöön sekä laatia ennusteita kapasiteetin riittävyydestä.
Järjestelmän hyväksyntä	Uusien järjestelmien käyttöönotto toteutetaan vasta toiminnallisuuksien testaamisen jälkeen. Testauksia varten laaditaan testaussuunnitelmat sekä nimetään testauksien vastuuhenkilöt.
Suojaus haittaohjelmia ja liikkuvia ohjelmia vastaan	
Turvamekanismit haittaohjelmien torjunnassa	Virusten- ja haittaohjelmien torjuntaa varten on kaikkiin työasemiin sekä palvelimiin asennettu ohjelmistot. Työaseman palauttaminen ongelmatilanteessa on nopeaa. Ohjeet haittaohjelmien tunnistamiseen ja torjuntaan tulee laatia.
Turvamekanismit liikkuvien ohjelmien torjunnassa	Liikkuvien ohjelmien käyttö on estetty.
Varmuuskopiointi	
Tietojen varmuuskopiointi	Palvelimet varmuuskopioidaan suunnitelman mukaan. Palautusten testaus tulee suunnitella ja toteuttaa.

Verkon turvallisuuden hallinta	
Verkon turvamekanismit	Verkkoa ylläpitävä yhteistyökumppani valvoo verkkoa jatkuvasti. Tietojen suojaamiseksi käytetään aina mahdollisuuksien mukaan suojattuja yhteyksiä ja palomuurit sallivat ainoastaan tunnetut ja luotetut yhteydet.
Verkkopalvelujen turvaaminen	Verkkoa ylläpitävä yhteistyökumppani valvoo verkkopalvelujen ja tietojärjestelmien toimivuutta jatkuvasti.
Tietovälineiden käsittely	
Siirrettävien tietovälineiden hallinta	Muistitikkujen ja optisten levyjen suojaamiseen tulee laatia menettelytavat.
Tietovälineiden poistaminen käytöstä	Käytöstä poistuvat tietovälineet tuhotaan ennen niiden kierrätystä.
Tietojen käsittelyohjeet	Tietojen käsittelyä ja tallennusta koskevat ohjeet tulee laatia.
Järjestelmän dokumentoinnin turvaaminen	Järjestelmän dokumentointi on laadittu ja sitä säilytetään suojatussa paikassa palvelimella.
Tiedon vaihto	
Tiedonvaihtoperiaatteet ja -menettelytavat	Osa tiedonvaihtoperiaatteista on dokumentoitu (mm. vakuutusyhtiöiden tiedonsiirrot).
Tiedonvaihtosopimukset	Tietoa vaihtavien tahojen kanssa on laadittu yhteistyösopimukset. Sopimuksia tulee tarkentaa mm. teknisten määritysten osalta.
Fyysiset tietovälineet kuljetuksen aikana	Kannettavien tietokoneiden kiintolevyt sekä mukana kuljetettavat muistitikut voidaan suojata salauksilla. Tämä ei ole tällä hetkellä vielä käytössä kaikkien henkilöiden työvälineissä.
Sähköinen viestintä	Osa järjestelmistä toimii käyttäen suojattuja yhteyksiä, osaan joudutaan laatimaan parannuksia.
Liiketoiminnan tietojärjestelmät	Tietojärjestelmäratkaisut pyritään toteuttamaan parhaalla mahdollisella käytettävissä olevalla asiantuntemuksella tietoturvallisuuden kannalta.
Verkkoasiointipalvelut	
Verkkoasiointi	Tietojärjestelmissä jokainen käyttäjä toimii henkilökohtaisella käyttäjätunnuksellaan.
Verkon kautta välitetyt tapahtumat	Tietojärjestelmissä on käytössä henkilökohtaiset käyttäjätunnukset. Osa tietojärjestelmistä käyttää vielä suojaamattomia yhteyksiä.
Julkinen informaatio	WWW-sivut ja ekstranet ovat ainoat AVK:n julkisessa verkossa olevat järjestelmät. Niiden valvontaan on tarkat tilastointityökalut ja niitä seurataan päivittäin.

Tarkkailu	
Tapahtumalokit	Verkon tapahtumalokeja ei tällä hetkellä säilötä pysyvästi. Niiden säilöminen tulee ottaa käyttöön ja tarvittaessa valvontaa tulee laajentaa.
Järjestelmän käytön tarkkailu	Verkkoa ylläpitävä yhteistyökumppani valvoo aktiivisesti tietoliikennettä valvontatyökalujen avulla sekä seuraa lokitiedostoja.
Lokitietojen suojaus	Lokitiedot tallennetaan kansioihin jotka ovat ainoastaan järjestelmän pääkäyttäjien saatavilla.
Pääkäyttäjä- ja operaattorilokit	Verkkoa ylläpitävä yhteistyökumppani dokumentoi suoritetut työt ja ne on eritelty laskutuksessa.
Häiriöiden kirjaus	Häiriöt tulee kirjata erikseen. Tällä hetkellä ne paljastuvat lokitietojen perusteella.
Kellojen synkronointi	Kaikkien työasemien kellot synkronoidaan automaattisesti toimialueen ohjauskoneen kanssa, mikä synkronoi aikatietonsa internetin aikapalvelimen kanssa.
Pääsyoikeuksien valvonta	
Liiketoiminnan asettamat vaatimukset pääsynvalvonnalle	
Pääsynvalvonnan toimintaperiaatteet	Pääsynvalvontaperiaatteet tulee laatia liiketoiminta- ja turvallisuusvaatimusten perusteella.
Käyttöoikeuksien hallinta	
Käyttäjien rekisteröinti	Käyttäjien rekisteröintiä sekä tunnusten poistamista varten tulee laatia menettelyohjeet.
Pääkäyttäjän oikeuksien hallinta	Pääkäyttäjän oikeudet palvelimiin sekä tietojärjestelmiin on ainoastaan verkkoa ylläpitävällä yhteistyökumppanilla sekä organisaatiossa sitä työkseen tarvitsevilla henkilöillä. Järjestelmien käyttöä valvotaan lokitiedostoilla.
Käyttäjän salasanojen hallinta	Käyttäjätunnukset tietojärjestelmiin myönnetään tarpeen mukaan.
Käyttöoikeuksien uudelleenarviointi	Käyttöoikeudet tulee arvioida säännöllisin väliajoin.
Käyttäjän velvollisuudet	
Salasanan käyttö	Windows-verkossa vaaditaan turvallinen salasana, jotkut tietojärjestelmät hyväksyvät heikkolaatuisemmat salasanat. Käyttäjiä on ohjeistettu valitsemaan turvalliset salasanat.
Valvomattomat käyttäjien laitteet	Työasemat sekä palvelimet lukittuvat automaattisesti tietyn ajan käyttämättömyyden jälkeen.
Puhtaan pöydän ja puhtaan näytön politiikka	Henkilöitä on ohjeistettava.

Verkkoon pääsyn valvonta	
Verkkopalvelujen käytön periaatteet	Jokaiselle henkilölle on myönnetty käyttöoikeudet ainoastaan tarvitsemiinsa tietojärjestelmiin ja sovelluksiin.
Ulkopuolisia yhteyksiä käyttävien henkilöiden todentaminen	Ulkoverkosta pääsee organisaation verkkoon ainoastaan suojatun VPN-yhteyden avulla. Jokaisella etäyhteyksiä käyttävällä henkilöllä on käytössään henkilökohtainen käyttäjätunnus.
Laitteiden tunnistus verkossa	Laitteiden tunnistus ei tällä hetkellä ole käytössä. Kytkimissä on valmiudet tämän toiminnon käyttöönottoon, jolloin jokaiselta verkkoon pyrkivältä laitteelta vaaditaan tunnistus ennen IP-osoitteen myöntämistä.
Etähuoltoyhteyksien suojaus	Etähuoltoyhteyksissä on käytössä ainoastaan suojatut yhteydet.
Verkkojen looginen jaottelu	Oman organisaation sekä muiden toimijoiden, kuten vartiointiliikkeen käytössä olevat laitteet, on erotettu kytkimissä käyttäen VLAN-portteja. Näin ulkopuoliset laitteet eivät pääse kirjautumaan organisaation toimialueeseen eivätkä pääse käsiksi sisäverkossa toimiviin tietojärjestelmiin.
Verkkoyhteyden valvonta	Ulkoverkon käyttöä valvotaan palomuurin avulla organisaation verkossa, vieraissa verkoissa työasemien virusturva- ja palomuuriohjelmisto on määritetty korkeaan suojaustasoon.
Verkon reitityksen valvonta	Verkon toimintaa valvova yhteistyökumppani valvoo verkon toimintaa ja siihen kohdistuvia sisäisiä sekä ulkoisia tietomurtoyrityksiä sekä sovellusten aiheuttamia häiriöitä.
Käyttöjärjestelmään pääsyn valvonta	
Turvalliset sisäänkirjausmenettelyt	Jokaiseen työasemaan sekä tietojärjestelmään kirjaudutaan käyttämällä henkilökohtaisia käyttäjätunnuksia.
Käyttäjän tunnistaminen ja todentaminen	Verkossa oleviin työasemiin kirjautumiseen sekä jokaiseen tietojärjestelmään kirjaudutaan käyttämällä henkilökohtaisia käyttäjätunnuksia.
Salasanojen hallintajärjestelmä	Windows-verkon järjestelmäkäytäntöihin on asetettu salasanojen pituus- ja turvavaatimukset, lisäksi eri sovelluksissa on sovelluskohtaiset salasanojen käsittelyt. Muutamat sovellukset sallivat turvattomien salasanojen käytön eivätkä vaadi ajoittaista salasanan vaihtamista.
Järjestelmän apuohjelmien käyttö	Järjestelmän ja sovellusten turvamekanismit ohittavien sovellusten käyttöoikeus on ainoastaan järjestelmäasiantuntijalla sekä verkkoa hallinnoivalla yhteistyökumppanilla. Näiden sovellusten käyttöä valvotaan lokitiedostoilla.

Istunnon aikakatkaisu	Selaimen kautta ajettavissa sovelluksissa istunto katkeaa aina muutaman minuutin käyttämättömyyden jälkeen. Työasemat menevät lukkoon 15 minuutin toimettomuuden jälkeen.
Yhteysajan rajoittaminen	Suuren riskin sovelluksissa yhteysaikaa tulee rajoittaa. Tämä toimii kaikissa selaimen kautta ajettavissa tietojärjestelmissä.
Sovellukseen ja tietoon pääsyn valvonta	
Tietojen käytön rajoittaminen	Kukin käyttäjä pääsee käsiksi vain tarvitsemiinsa tietoihin. Ainoastaan Tessu tarvitsee tarkemman käyttäjätilien määrityksen.
Arkaluonteisen sovelluksen eristäminen	Eristettyä tietokoneympäristöä vaativaa sovellusta ei ole käytössä.
Tietokoneen matkakäyttö ja etätyö	
Tietokoneen matkakäyttö ja tietoliikenne	Vieraassa tietoliikenneverkossa käytetään suojattua VPN-yhteyttä AVK:n verkkoon pääsyä varten. Vieraassa verkossa ollessaan työaseman virustentorjunta- ja palomuuriohjelma käyttää korkeaa suojaustasoa. Myös jokaisen kannettavan työaseman kiintolevy voidaan salata.
Etätyö	Etätyötä varten käytetään suojattua VPN-yhteyttä. Tiedostot tulee tallentaa palvelimen verkkolevyille eikä työaseman kiintolevylle.
Tietojärjestelmien hankinta, kehitys ja ylläpito	
Tietojärjestelmien turvallisuusvaatimukset	
Turvallisuusvaatimusten analyysi ja määrittely	Suuria tietojärjestelmävaihdoksia tai mittavia muutostöitä ei ole tehty viime aikoina, mutta kehityspiirteissä otetaan tietoturvallisuus huomioon.
Virheetön tietojenkäsittely sovelluksissa	
Syöttötietojen oikeellisuuden tarkistus	Sovelluksissa on käytössä tekniset mekanismit tietojen oikean muodon ja oikeellisuuden valvontaan. Muutamia puutteita on tunnistettu ja ne on luetteloitu päivityslistaan.
Sisäisen käsittelyn valvonta	Tietojärjestelmissä tulee olla mekanismit tietojen oikeellisuuden varmistamista varten. Nämä on rakennettu käytettäviin tietojärjestelmiin ja sovelluksiin.
Viestien eheys	Viestien aitouden ja eheyden varmistamiseksi voidaan ottaa käyttöön esimerkiksi digitaalinen allekirjoitustekniikka. Käyttöönoton ongelmana on vastaanottajan teknisten valmiuksien puuttuminen allekirjoitusten käsittelyä varten.
Tulostustietojen oikeellisuuden tarkistus	Jokainen käyttäjä tarkastaa tietojärjestelmissä käsittelemiensä tietojen oikeellisuuden.

Salakirjoitusmekanismit	
Salakirjoitusmekanismien käytön periaatteet	Arkaluontoisen tiedon käyttöön voidaan soveltaa esimerkiksi PGP-salausta. Tällä hetkellä se ei ole käytössä.
Salausavaintenhallinta	AVK:lla ei ole käytössä salaustekniikoita.
Järjestelmätiedostojen turvallisuus	
Tuotannossa olevan ohjelmiston valvonta	Tuotannossa oleviin ohjelmistoihin tehdään muutokset testausten jälkeen sovitun aikataulun mukaan.
Järjestelmän testiaineiston suojaus	Tietojärjestelmien muutosten testauksiin laaditaan testaussuunnitelma, minkä mukaan nimetyt henkilöt testaavat muuttuneet ominaisuudet ja raportoivat siitä suunnitelman mukaan.
Ohjelmien lähdekoodiin pääsyn valvonta	Lähdekoodiin on pääsy ainoastaan ohjelmiston kehittäjällä.
Kehitys- ja tukiprosessien turvallisuus	
Muutosten valvontamenettelyt	Tietojärjestelmien muutoksia tilattaessa sovitaan tapauskohtaisesti muutosten toimeenpanon valvonnasta.
Käyttöjärjestelmän muutosten jälkeinen sovellusten tekninen tarkastus	Käyttöjärjestelmät vaihdetaan hallitusti ja sovellusten toimivuus testataan ennen vaihtoa.
Ohjelmistopakettien muutoksia koskevat rajoitukset	Ohjelmistopaketteihin tehdään muutoksia tarpeen vaatiessa ja muutokset testataan aina ennen käyttöönottoa.
Tietovuodot	Tietovuotojen syntyä ehkäistään ohjeistamalla ja kouluttamalla käyttäjiä.
Ulkoistettu ohjelmistokehitys	Organisaation tulee valvoa ulkoistettua ohjelmistokehitystä. Ennen tietojärjestelmän muutosten siirtämistä tuotantoon muutokset testataan ja niistä raportoidaan laaditun testaussuunnitelman mukaan.
Teknisten haavoittuvuuksien hallinta	
Teknisten haavoittuvuuksien valvonta	Verkkoa hallinnoiva yhteistyökumppani hoitaa tietojärjestelmien valvontaa ylläpitosopimuksen mukaan.
Tietoturvahäiriöiden hallinta	
Tietoturvatapahtumista ja -heikkouksista raportoiminen	
Tietoturvatapahtumien raportointi	Tietoturvatapahtumista tulee raportoida. Verkkoa hallinnoiva yhteistyökumppani valvoo säännöllisesti AVK:n verkkoliikennettä sopimuksen mukaan ja raportoinnista on sovittu.

Turvallisuuden heikkouksista raportoiminen	Kaikkien käyttäjien tulee kiinnittää huomiota järjestelmissä ja palveluissa mahdollisesti esille tuleviin suojauksen heikkouksiin. Tämä vaatii ohjeistamista ja kouluttamista.
Tietoturvahäiriöiden ja parannuskohteiden hallinta	
Vastuut ja menettelytavat	Tietoturvahäiriöistä aiheutuvaa riskiä on pienennetty ulkoistamalla tietoliikenteen valvonta verkkoa hallinnoivalle yhteistyökumppanille.
Tietoturvahäiriöistä oppiminen	Verkkoa hallinnoiva yhteistyökumppani seuraa aktiivisesti tietoturvaloukkauksia sekä niiden yrityksiä.
Todisteiden kokoaminen	Mahdollisia rikosoikeudellisia toimenpiteitä vaativien todisteiden (mm. lokitiedostot) kokoaminen ja säilyttäminen hoidetaan automaattisesti.
Liiketoiminnan jatkuvuuden hallinta	
Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia	
Tietoturvallisuuden sisällyttäminen liiketoiminnan jatkuvuuden hallintaprosessiin	Liiketoimintaprosessit on kuvattava ja laadittava liiketoimintalähtöinen riskianalyysi.
Liiketoiminnan jatkuvuus ja riskien arviointi	Liiketoimintaprosessit on kuvattava, laadittava liiketoimintalähtöinen riskianalyysi sekä laadittava toipumissuunnitelma (Disaster Recovery Plan, DRP)
Tietoturvallisuuden sisältävien jatkuvuussuunnitelmien kehittäminen ja toteuttaminen	AVK:n tulee laatia DRP, mihin sisällytetään testausmenetelmät ja määräajoin suoritettavat testaukset.
Liiketoiminnan jatkuvuussuunnitelman puitteet	AVK:n tulee laatia DRP sekä kuvata liiketoiminnan prosessit.
Liiketoiminnan jatkuvuussuunnitelman testaus, ylläpito ja uudelleenarviointi	Toipumissuunnitelmaan sisällytettävät testausmenetelmät ja aikataulut.
Vaatimustenmukaisuus	
Lakisääteisten vaatimusten noudattaminen	
Sovellettavan lainsäädännön tunnistaminen	Tietojärjestelmät toteutetaan alan osaavien yhteistyökumppanien kanssa. Tietojärjestelmien dokumentoinnissa on vielä kehitettävää.
Aineettomat oikeudet	Aineettomien oikeuksien hallintaan tulee olla käytössä menettelytavat. Lisenssit ovat ulkopuolisen yhteistyökumppanin kanssa hankitut ja ovat ajan tasalla.
Organisaation tallenteiden suojaus	Arkistoitavat tallenteet on sijoitettu lukittuihin ja valvottuihin tiloihin. Tallenteiden suojausta kehitetään jatkuvasti.
Tietosuoja ja henkilöiden yksityisyys	Tietosuoja tulee varmistaa lakien, määräysten sekä sopimusten edellyttämällä tavalla. Tämä toteutuu.

Tietojenkäsittelypalvelujen väärinkäytön estäminen	Tämän toteuttamiseen on käytössä tekniset menetelmät, kuten palomuuri, verkkoliikenteen valvontatyökalut sekä rajoitetut käyttöoikeudet.
Salakirjoitusmekanismeja koskevat säädökset	Näitä tulee käyttää sopimusten, lakien ja määräysten niin velvoittaessa. Tämä toteutuu.
Turvallisuuspolitiikan ja -standardien noudattaminen ja tekninen vaatimustenmukaisuus	
Turvallisuuspolitiikan ja standardien noudattaminen	Esimiesten tulee varmistaa vastuualueidensa turvamenettelyt. Tämä sisältyy tietoturvapolitiikkaan, joka on vielä työn alla.
Teknisen kelpoisuuden tarkastus	Kun tietoturvallisuuden hallintajärjestelmä on käytössä, menetelmien ja välineiden tekninen vaatimustaso on tarkastettava säännöllisin väliajoin.
Tietojärjestelmän tarkastusnäkökohtia	
Tietojärjestelmän tarkastusmekanismit	Auditointityökaluja ei vielä ole olemassa.
Tietojärjestelmän tarkastusvälineiden suojaus	Näitä tullaan säilyttämään suojatuissa verkkohakemistoissa kuten ympäristöjärjestelmän auditointivälineitäkin.

Taulukko: ISO/IEC 27001 -tietoturvallisuusstandardin valvontatavoitteet ja niiden toteutuminen