

Ilmari Luoma

# Tietoturvallisuusauditointi ISO27000-viitekehyksessä

Julkinen osa

Opinnäytetyö

Kevät 2015

SeAMK Tekniikka

Tietotekniikan koulutusohjelma

SEINÄJOEN AMMATTIKORKEAKOULU

## Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoverkkotekniikka

Tekijä: Ilmari Luoma

Työn nimi: Tietoturvaluusauditointi ISO27000-viitekehyksessä

Ohjaaja: Alpo Anttonen

Vuosi: 2015

Sivumäärä: 50

Liitteiden lukumäärä:2

---

Tiedon olemassaolo eri olomuodoissa muodostaa vaikeasti hallittavan uhkakentän, jonka käsittelyyn kansainvälisesti hyväksytty ISO 27000 -standardi on hyvä väline.

Työn tarkoitus on perehtyä ISO/IEC 27000 -standardisarjaan, soveltaa standardin vaatimuksia laatimalla tietoturvaluuden auditointiaineisto ja -menetelmä, sekä toteuttaa tietoturvaluusauditointi käytännössä.

Työssä esitellään tietoturvaluuden kytkeytyminen yritysturvaluuteen, tietoturvaluuden osa-alueittainen rakentuminen ISO-standardien mukaisesti, sekä viisi-tasoinen auditointimalli jokaisen osa-alueen tehokkaaseen kartoittamiseen.

Laadittu auditointiaineisto luo rakenteen auditoinnille, helpottaa auditointityötä sekä mahdollistaa helpon ja tehokkaan dokumentoinnin auditoinnin aikana.

Auditoinnin tarkoituksena on kartoittaa toimeksiantajan tietoturvaluuden nykytila, sekä laatia tietoturvaluusraportti, jota käytetään pohjana toimeksiantajan tietoturvaluuden kehitysprojektissa. Auditointi rakentuu haastatteluista, sekä käytännön katselmuksesta toimeksiantajan toimintaympäristössä.

Avainsanat: tietoturvaluus, auditointi, turvaluusjohtaminen, ISO 27000, ISO 27001, ISO 27002

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

## **Thesis abstract**

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Networking Technology

Author: Ilmari Luoma

Title of thesis: Information security audit in ISO 27000 framework

Supervisor: Alpo Anttonen

Year: 2015

Number of pages: 50

Number of appendices: 2

---

Information in different forms generates a challenging threat-field. ISO 27000 is a framework designed to manage information risks comprehensively. The objective of this thesis was threefold: introducing ISO 27000 series of standards, applying the requirements of the standards to the design material and processes needed to perform an information security audit in ISO 27000 framework, and actually performing the mentioned information security audit.

The thesis demonstrates the connection between corporate security and information security as well as the diverse areas of information security within the ISO 27000 framework. The thesis also introduces a five-level audit method, designed for a thorough and efficient information security audit.

The created audit material gave structure for the audit, simplifies the process, and provided a method for easy documentation. The purpose of the audit was to map the current information security level of the client, and to draft an information security level report which was used as the baseline for an information security development plan. The audit consisted of a series of interviews and inspections on the premises.

Keywords: Information security, audit, security management, ISO 27000, ISO 27001, ISO 27002

## SISÄLTÖ

Opinnäytetyön tiivistelmä.....	2
Thesis abstract.....	3
SISÄLTÖ.....	4
Kuva-, kuvio- ja taulukkoluettelo.....	6
Käytetyt termit ja lyhenteet.....	7
1 JOHDANTO.....	9
1.1 Työn tausta.....	9
1.2 Työn tavoite.....	9
1.3 Työn rakenne.....	9
2 TIETOTURVALLISUUS.....	11
2.1 Tietoturvallisuuden perusteet.....	12
2.2 Saatavuus.....	12
2.3 Luottamuksellisuus.....	13
2.4 Eheys.....	13
2.4.1 Fyysinen olomuoto.....	13
2.4.2 Looginen olomuoto.....	14
2.4.3 Immateriaalinen olomuoto.....	14
2.5 Kiistämättömyys.....	15
2.6 Tunnistus.....	16
2.7 Todennus.....	16
3 TIETOTURVALLISUUDEN KÄSITTELY.....	17
3.1 Tietoturvallisuus osana yritysturvallisuutta.....	17
3.2 Tietoturvallisuuden osa-alueiden määrittely.....	18
3.2.1 Hallinnollinen tietoturva.....	20
3.2.2 Fyysinen tietoturvallisuus.....	21
3.2.3 Laitteistoturvallisuus.....	23
3.2.4 Ohjelmistoturvallisuus.....	25
3.2.5 Tietoaineiston turvallisuus.....	27
3.2.6 Tietoliikenneturvallisuus.....	28
3.2.7 Henkilöstöturvallisuus.....	30

3.2.8 Käyttöturvallisuus.....	32
4 HYBRIDIMALLI .....	34
5 KÄYTÄNNÖN TOTEUTUS.....	46
5.1 Objekttiivinen tarkastelu .....	46
5.2 Subjekttiivinen tarkastelu .....	47
LÄHTEET .....	49
LIITTEET .....	50

## Kuva-, kuvio- ja taulukkoluetelo

Kuvio 1. PDCA-vuosikello .....	21
Kuvio 2. Suppea luokittelumerkintä.....	28
Kuvio 3. Hybridimalli .....	35
Kuvio 4. Direktiotaso .....	37
Kuvio 5. Fyysinen taso.....	38
Kuvio 6. Looginen taso .....	40
Kuvio 7. Immateriaalitaso.....	42
Kuvio 8. Sidosryhmätaso .....	44
Kuvio 9. Opinnäytetyön toteutuskaavio.....	47

## Käytetyt termit ja lyhenteet

<b>Direktio (oikeus)</b>	Työnantajan työsopimuslainmukainen oikeus osoittaa työntekijöille työtä ja työskentelytapa.
<b>Force majeure</b>	Sopimusoikeudessa määritelty ylivoimainen ennakoimaton este, joka (yleensä) on vastuuvapautusperuste.
<b>Fyysinen tieto</b>	Tietoaineisto, joka on olemassa fyysisessä olomuodossa, esimerkiksi paperiasiakirjat.
<b>Immateriaalinen tieto</b>	Tietoaineisto, joka on olemassa ihmisten ajatuksissa.
<b>ISO</b>	Kansainvälinen standardoimisjärjestö (International Organization for Standardization).
<b>ISO 27000:2009</b>	Standardi, joka määrittelee tietoturvallisuuden hallintajärjestelmän yleiskatsauksen.
<b>ISO 27001:2009</b>	Standardi, joka määrittelee tietoturvallisuuden hallintajärjestelmänvaatimukset.
<b>ISO 27002:2005</b>	Standardi, joka määrittelee tietoturvallisuuden hallintakeinojen toteutusohjeet.
<b>Kaasusammutuslaitteisto</b>	Palonsammutusjärjestelmä, joka toimii syrjäyttämällä palamisen kannalta tarpeellisen hapen esimerkiksi argonkaasulla.
<b>Kognitio (toiminnot)</b>	Ihmisen kyky vastaanottaa, käsitellä, tallettaa sekä soveltaa tietoa.
<b>Korruptoitua</b>	Tiedon muuntuminen halutusta muodosta joko osittain tai täydellisesti käyttökelvottomaksi.
<b>Looginen tieto</b>	Tieto, joka sijaitsee missä tahansa tietovälineessä, johon on pääsy minkä tahansa tietoverkon välityksellä.

<b>Optinen media</b>	Tiedon tallennusväline, jonka toimintaperiaate perustuu tiedon lukemiseen ja kirjoittamiseen laser-säteen avulla (esimerkiksi Blu-ray-levy)
<b>Salassapitosopimus</b>	rajoittaa työntekijän mahdollisuuksia jakaa yritystä koskevaa tietoa kolmannelle osapuolelle työsuhteen aikana sekä työsuhteen päättymisen jälkeen.
<b>Tietoturvahäiriö</b>	Tilanne, joka on aiheuttanut tietoturvallisuuden vaarantumisen.
<b>Tietoturvatapahtuma</b>	Tilanne, joka on aiheuttanut mahdollisuuden tietoturvallisuuden vaarantumiseen.



# 1 JOHDANTO

## 1.1 Työn tausta

Tieto on yrityksen vaikeimmin määriteltävä ja rahallisesti hankalin arvoitettava voimavara. Tietoa on nykyään olemassa sekä fyysisenä aineistona paperilla, teknisenä aineistona kiintolevyillä sekä abstraktina (hiljaisena) tietona työntekijöiden päässä. Tietoturvallisuuden hallinta tähtää tilanteeseen, jossa yritys hallitsee tiedon elinkaarta tiedon hankinnasta tiedon tuhoamiseen ja minimoi tiedosta tai tiedolle aiheutuvat negatiiviset vaikutukset.

Tietoturvallisuuden hallinnan tarkoitus on muuttaa yrityksen toimintakulttuuri reaktiivisesta toimintamallista proaktiiviseen toimintamalliin. Reaktiivisessa toimintamallissa ulkopuolinen tapahtuma laukaisee toimenpiteet, toisin kuin proaktiivisessa, jossa toimenpiteet ovat jo valmiina ennen tapahtumaa.

## 1.2 Työn tavoite

Työn tavoitteena on laatia tietoturvallisuusauditointiaineisto ISO-27000-viitekehyksessä, jonka avulla suoritetaan tietoturvallisuuden perustason kartoitus alueella toimivassa yrityksessä, sekä suunnitellaan jatkotoimenpiteet tietoturvallisuuden kehittämiseksi.

## 1.3 Työn rakenne

Luvussa 2 käsitellään tietoturvallisuuden peruseriaatteet ISO 27000 -standardin määritelmien mukaisesti ja esitellään tiedon käsittely fyysisenä, loogisena ja immateriaalisena mediana.

Luvussa 3 käsitellään tietoturvallisuuden kytkeytymistä yritysturvallisuuden kautta yrityksen riskienhallintaan, kerrotaan tietoturvallisuuden johtamisen peruseriaatteet, esitellään tietoturvallisuuden osa-alueiden sisältö sekä esitellään tietoturvallisuuden auditointimalli.

Työn käytännön toteutus käsitellään luvussa 4 objektiivisesta ja subjektiivisesta näkökulmasta. Objektiivinen näkökulma käsittelee, miten opinnäytetyön käytännön osuuden tekeminen eteni yleisellä tasolla. Subjektiivisessa tarkastelussa esitellään opinnäytetyön edistymiseen liittyvät henkilökohtaiset havainnot.

## 2 TIETOTURVALLISUUS

Tietoturvallisuus käsitteenä sisältää joukon toimenpiteitä, joilla minimoidaan tiedon tuhoutumisen tai korruptoitumisen, häiriöitymisen ja väärinkäytöksen riski. Tietoturvallisuus konseptina on moniulotteinen kokonaisuus, jota on käsiteltävä perinteisen kolmiulotteisen fyysisen ympäristön lisäksi kolmessa lisäulottuvuudessa: loogisessa ulottuvuudessa, immateriaalisessa ulottuvuudessa sekä ajallisessa ulottuvuudessa. (ISO 27000 2009, 15.)

Loogisella ulottuvuudella tarkoitetaan tiedon olemassaoloa paikallis- ja laajaverkkoihin kytketyissä järjestelmissä sekä paikallisesti käytettävissä muistimedioissa. Looginen tieto on altis perinteisille fyysisille riskeille sekä kyberriskeille. (ISO 27000 2009, 23.)

Immateriaalisella ulottuvuudella tarkoitetaan tietoa, joka ei ole olemassa fyysisessä eikä loogisessa muodossa, vaan osana henkilön kognitiivisia toimintoja. Ihmisen muisti on muistimedianan altis korruptoitumiselle, eikä ihmistä voida pakottaa unohtamaan oppimaansa. Immateriaalisen tiedon hallinnassa suuri merkitys onkin yrityksen toiminnan kannalta vääränlaisen immateriaalitiedon kertyminen. (ISO 27000 2009, 23.)

Konkretisoimaan tietoturvallisuuden laaja-alaista toimintakenttää alla on esitetty erilaisia tilanteita, jotka kuuluvat tietoturvallisuuden piiriin.

1. Tiedon tuhoutuminen tai korruptoituminen
  - a. Käyttäjän virheellinen toiminta
  - b. Ulkoisen toimijan toimenpiteet
  - c. Paikallinen onnettomuus
  - d. Force majeure
2. Tiedon häiriöityminen
  - a. Tiedon suunnittelematon muuttaminen

- b. Tiedon lievä korruptoituminen
- c. Fyysisen tietoliikenteen häirintä
- d. Teknisen tietoliikenteen häirintä
- e. Ulkoisen toimijan aiheuttama tiedon tarkoituksellinen muuttaminen

### 3. Tiedon väärinkäyttö

- a. Salaisen tiedon paljastuminen
- b. Muun kuin salaisen tiedon luvaton käyttö
- c. Tiedon luvaton kopioiminen. (ISO 27000 2009, 15.)

## 2.1 Tietoturvallisuuden perusteet

Hyvälle tietoturvallisuudelle on määritelty kolme määrittävää periaatetta ja kolme tukevaa periaatetta. Määrittävät periaatteet ovat tiedon saatavuus, tiedon luottamuksellisuus ja tiedon eheys. Tukevat periaatteet ovat kiistämättömyys, tunnistaminen ja todentaminen. (ISO 27000 2009, 13–17.)

## 2.2 Saatavuus

Saatavuusvaatimus käsitteenä tarkoittaa, että henkilön aseman tai tehtävän suorittamiseksi tarpeellisen tiedon on oltava saatavilla oikea-aikaisesti. Tietoturvallisuustoimenpiteillä (prosesseilla) on turvattava tiedon oikea-aikaisuusvaatimus kriittisyyskiireellisyysluokituksen mukaisesti. Tiedon ollessa kriittistä tiedonsaannin tulee olla viivytyksetöntä. Tiedon ollessa ei-kriittistä tiedonsaantiaika voi olla voi pitkä. (ISO 27002 2013, 123.)

Käytännön tasolla saatavuus ilmentää palvelutasoa (toimintataso). Toimintavarmat järjestelmät pitävät palvelutason korkealla, jolloin toimintaa haittaavia tapahtumia ei ole. Häiriösietoiset järjestelmät mahdollistavat palvelutason portaitaisen laskun häiriön pitkittyessä (tietoturvahäiriö). (ISO 27002 2013, 123.)

Tietoturvahäiriön lievempänä muotona voidaan pitää ”tietoturvatapahtumaa”, jossa häiriötä ei aiheudu, mutta puitteet ovat olemassa. Puhekielinen vertailukelpoinen käsite voisi olla ”läheltä piti”-tilanne. (ISO 27000 2009, 15.)

Teollisuuslaitetekniikassa saatavuudesta käytetään usein nimitystä käytettävyys, jolloin viitataan eritoten laitteen tai järjestelmän toimintavarmuuteen. (ISO 27000 2009, 13.)

### **2.3 Luottamuksellisuus**

Luottamuksellisuusvaatimuksenmukainen tietoturvallisuusluokiteltu (myöhemmin luokiteltu) tieto on ainoastaan tiedon luokituksen mukaisten henkilöiden saatavilla ja käytettävissä. Tiedon ja työntekijöiden luokittelun myötä myös käsittelytilat, käsittelylaitteet ja tiedon siirtotavat on luokiteltava, jotta voidaan saavuttaa riittävä luokittelukokonaisuus. (ISO 27000 2009, 13.)

### **2.4 Eheys**

Eheysvaatimuksen täytyessä ollaan tilanteessa, jossa tiedon luominen, muuttaminen ja tuhoaminen ovat hallittuja toimenpiteitä, eikä tietoa voida muuttaa tai tuhota ilman dokumentoitua kirjausketjua. Tiedon eheyden takaamiseksi on luotava toimiva tiedon muutoksenhallintajärjestelmä, jossa on huomioitava tiedon olemassaolon kolme olomuotoa: fyysinen, looginen ja immateriaalinen. (ISO 27000 2009, 15.)

#### **2.4.1 Fyysinen olomuoto**

On laadittava menettelyt paperiasiakirjojen, mikrofilmien, piirustusten ja kuvien väärinkäytösten, suunnittelemattoman tuhoutumisen ja muuntelun ehkäisemiseksi, havaitsemiseksi ja torjumiseksi. Pelkästään fyysisessä olomuodossa oleva tieto on altis erityisesti ympäristön aiheuttamille riskeille, sillä fyysisessä olomuodossa oleva tieto on tuhottavissa usein jo pelkästään kosteudella. (ISO 27002 2013, 77.)

### 2.4.2 Looginen olomuoto

Loogisessa muodossa oleva tieto on muistivälineillä, kiintolevyillä, verkkolevyillä tai pilvipalveluissa, jolloin on usein olemassa kolme keinoa päästä tietoon käsiksi:

1. Fyysinen tietoväline voi olla fyysisen uhan kohteena. Fyysinen uhka voi olla joko laiterikosta, käyttäjästä, ympäristöstä tai ulkopuolisesta toimijasta johdettu tiedon osittainen tai täydellinen korruptoituminen, luvaton kopioituminen tai paljastuminen.
2. Fyysinen tietoväline voi olla paikallisen yhteyden kautta käsiteltävissä, jolloin tieto voidaan osittain tai täydellisesti korruptoida, luvattomasti kopioida tai paljastaa joko käyttäjän toimien tai kolmannen osapuolen toimesta.
3. Loogiseen tietovälineeseen voidaan avata yhteys ulkoisesta lähteestä, jolloin voidaan kolmannen osapuolen toimesta luvattomasti kopioida, korruptoida tai paljastaa tietoa. (ISO 27002 2013, 73.)

### 2.4.3 Immateriaalinen olomuoto

Immateriaalisessa olomuodossa oleva tieto ei ole olemassa fyysisesti saatavilla olevana medianana eikä loogisessa tallennusvälineessä, vaan osana ihmisen kognitiivisia toimintoja, minkä vuoksi kyseisen tiedon eheyden takaaminen vaatii tukitoimia fyysisten ja loogisten tietovälineiden muodossa. Immateriaalinen tieto on kuudenlaisten uhkien kohteena:

1. Immateriaalisen tiedon korruptoitumisaste on luontaisesti korkea, mikäli tietoa ei käytetä, jolloin tietoa on päivitettävä toistuvasti.
2. Työntekijän poistuessa työnantajan palveluksesta poistuu yrityksestä työntekijän työvuosiin eksponentiaalisesti verrannollinen määrä hiljaista tietoa (oppimiskäyräperiaate: työtehtävän työaika lyhenee 20 % työntekokertojen kaksinkertaistuessa).

3. Työntekijän kognitiiviseen toimintaan vaikuttava terveydentilan heikkeneminen aiheuttaa tiedon äkillisen ja hallitsemattoman osittaisen tai täydellisen korruptoitumisen.
4. Reflektoiminen on osa työntekijän kasvuprosessia. Mikäli reflektointi kohdennetaan oikein, se on työntekijän osaamista kasvattava toimi, mutta sopivan reflektointiympäristön puuttuessa, työntekijä paljastaa luokiteltua tietoa luokittelun ulkopuoliselle taholle, kuitenkin ilman pahansuopaa aietta.
5. Sosiaalinen manipulointi on tiedonhankintatapa, jossa työntekijää manipuloidaan paljastamaan luokiteltua tietoa kolmannelle osapuolelle tai antamaan käyttöoikeus luokiteltuun tietoon.
6. Tarkoituksellinen väärinkäyttö. Työntekijä käyttää työnantajansa palveluksessa saamiaan kriittisiä tietoja joko kolmannen osapuolen tai itsensä eduksi. (ISO 27002 2013, 28–32, 35–37.)

## 2.5 Kiistämättömyys

Kiistämättömyys tarkoittaa yksiselitteistä vastuuta tiedon luomisesta, olemassa olevan tiedon muuttamisesta tai tiedon tuhoamisesta. Kiistämättömyys edellyttää olosuhteita, joissa jokainen tietoon liittyvä muutostoimenpide on yksiselitteisesti kohdennettavissa muutoksen tekijään, jolloin voidaan luoda juridisesti pätevä olosuhde, jossa toimenpiteen suorittaja ei voi kiistää jälkikäteen toimiaan. (ISO 27000 2009, 17.)

Kiistämättömyyden toteuttaminen vaatii vahvan tunnistamisen ja todentamisen toteuttamista, jotta voidaan sulkea pois todennäköisyydellisesti ja tilastollisesti järkevällä todennäköisyydellä kolmannen osapuolen toiminta tietoaaineiston muutostilanteessa (ISO 27000 2009, 17).

## 2.6 Tunnistus

Tunnistus tarkoittaa, että tietojärjestelmän käyttäjän käyttäjätunnus on yksilöitävissä. Esimerkiksi yrityksen tietojärjestelmän käyttäjätunnus a000123 on rekisteröity henkilölle ”Matti Meikäläinen”. (ISO 27000 2009, 18.)

## 2.7 Todennus

Todennuksessa edellä mainitun tunnistuksen jälkeen varmistetaan luotettavasti, että käyttäjätunnukseen liitetty henkilö on tosiasiallisesti tunnuksen käyttäjä. Esimerkiksi aiemmin mainitulla Matti Meikäläiselle rekisteröidyllä käyttäjätunnuksella a000123 järjestelmään kirjautunut henkilö todella on Matti Meikäläinen.

Tunnistus ja todennus on tavanomaisimmin tietojärjestelmissä käytetty toimenpide, mutta tunnistus ja todennus voidaan ulottaa myös fyysiseen tietoaaineistoon, jolloin tunnistus vaatii joko yksilöivän tunnisteiden (esimerkiksi henkilökortin) ja salasanan tunnisteen käyttöä tai manuaalista valvotun kirjausprosessin käyttöä (ISO 27000 2009, 13).

Sivuhuomiona mainittakoon, että myös immateriaalitietoon pääsemistä voidaan rajoittaa esitetyin keinoin, mutta immateriaalitietoon pääsyn rajoittamiseen liittyvä tunnustus tulee kysymykseen lähinnä viranomaistoiminnassa (ISO 27000 2009, 13).



### 3 TIETOTURVALLISUUDEN KÄSITTELY

Tietoturvallisuuden käsittelymalleja on lukuisia: Suomessa käytetyt mallit ovat Elinkeinoelämän Keskusliiton yritysturvallisuusmäärittely, puolustusministeriön laatima kansallinen turvallisuusauditointikriteeristö (KATAKRI), valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmän ohjeisto (VAHTI), sekä ISO 27000 -standardisarja.

#### 3.1 Tietoturvallisuus osana yritysturvallisuutta

Tietoturvallisuutta ei voi käsitellä erillään muista turvallisuuden osa-alueista, sillä tietoturvallisuus käsittelee koko yritysturvallisuuden kenttää. Siksi onkin käsitettävä yritysturvallisuuden kokonaisuus, ennen kuin voidaan keskittyä itse tietoturvallisuuteen. Yritysturvallisuuden kokonaisuuden esittelyyn yksinkertaisin malli on elinkeinoelämän keskusliiton yritysturvallisuuden määrittely.

Elinkeinoelämän keskusliitto on määritellyt yritysturvallisuuden kokonaisuuden jakamalla yritysturvallisuuden kymmeneen osa-alueeseen seuraavasti:

1. Tuotannon ja toiminnan turvallisuus
  - a. Käsittelee tuotantolaitteiden turvallisuutta
2. Työturvallisuus
  - a. Käsittelee työntekijöiden työturvallisuutta
3. Ympäristöturvallisuus
  - a. Käsittelee ympäristöturvallisuutta
4. Pelastustoiminta
  - a. Käsittelee palo- ja pelastustoimintaan liittyviä valmiuksia
5. Valmiussuunnittelu
  - a. Käsittelee väestönsuojelullisia keinoja sekä kriittisten toimintojen koventamistoimia
6. Tietoturvallisuus
  - a. Käsittelee tiedon turvallisuutta
7. Henkilöturvallisuus
  - a. Käsittelee henkilöstön turvallisuutta
8. Kiinteistö- ja toimitilaturvallisuus

- a. Käsittelee kiinteistön ja toimitilojen turvallisuutta
- 9. Ulkomaantoimintojen turvallisuus
  - a. Käsittelee ulkomailla tapahtuvan liiketoiminnan ja henkilöstön turvallisuutta
- 10. Rikosturvallisuus
  - a. Käsittelee yrityksen toimia rikosriskeihin varautumiseksi (Yritysturvallisuus [viitattu 15.4.2015].)

Yritysturvallisuuden täydellinen hallitseminen vaatii siis yritysturvallisuuden monipuolista katselmointia. On myös todettavissa erilaisten osa-alueiden riskinhallintakeinojen aiheuttavan yritysturvallisuuden kannalta positiivisia vaikutuksia myös muille, kuin hallintakeinolle määritellylle sektorille. Esimerkiksi työntekijän allekirjoittama salassapitosopimus on osa tietoturvallisuutta, mutta on samalla myös osa yrityksen varautumista rikoksiin. (Yritysturvallisuus [viitattu 15.4.2015].)

Huomattavalle määrälle osa-alueista on olemassa olevia lainsäädäntötasolla säädettyjä määräyksiä, erilaisten valvontaviranomaisten vaatimuksia sekä kansallisia tai kansainvälisiä standardeja. Standardisoinnista mainittakoon tuotannon ja toiminnan turvallisuutta sekä kiinteistö- ja toimitilaturvallisuutta sivuava ISO 9000 -standardisarja, ympäristöturvallisuutta käsittelevä ISO 14000 -standardisarja sekä tietoturvallisuutta käsittelevä ISO 27000 -standardisarja.

### **3.2 Tietoturvallisuuden osa-alueiden määrittely**

Kokonaisuuden hallitsemisen helpottamiseksi tietoturvallisuuden osa-alue on segmentoitu kahdeksaan osa-alueeseen:

- 1. Hallinnollinen tietoturvallisuus
  - a. Tietoturvallisuuden pohja on yrityksen toimintastrategia sekä yrityksen sisällä tapahtuvat selkeät aikataulutukset, sekä vastuutukset.
- 2. Fyysinen tietoturvallisuus

- a. Käsittelee toimitilojen ja laitteiden fyysistä suojaamista toimitiloissa sekä toimitilojen ulkopuolella. Fyysisen tietoturvan osalla määritellään varautumistoimenpiteet laitteiden tapaturmasta, onnettomuudesta, varkaudesta tai vandalismista aiheutuvia fyysisiä riskejä.
3. Laitteistoturvallisuus
  - a. Laitteistoturvallisuudessa varmistutaan hankinta-, käyttö- ja käytöstä poistamisketjun tietoturvallisesta toteutuksesta, kuten myös huolto- ja ylläpitoketjun hallitsemisesta.
4. Ohjelmistoturvallisuus
  - a. Ohjelmistoturvallisuudessa käsitellään lisenssien hallintaa, ohjelmistojen asennus- ja käyttöpolitiikkaa, sekä varmuuskopiointia ja päivityksien hallintaa.
5. Tietoaineiston turvallisuus
  - a. Tiedon luokittelu tietoturvaluokituksen mukaan ja toimenpiteet salassa pidettävän tiedon salassa pitämiseksi.
6. Tietoliikenneturvallisuus
  - a. Tietoa siirretään tietoliikenneverkoissa paikallisesti sekä laajaverkoista, josta johtuen tietoverkkojen ja tietoliikennelaitteiden, palomuurien sekä tunkeutumisen havaitsemis- ja estojärjestelmien hallinta on keskeisessä roolissa loogisella tasolla tapahtuvaa tietoturvaa.
7. Henkilöstöturvallisuus
  - a. Immateriaalisen tiedon hallinta alkaa rekrytointiprosessissa, jatkuu työsuhteen kestäessä ja päättyy irtisanomisprosessiin. Henkilöstöturvallisuus käsittää myös henkilöstön järjestelmällisen koulutuksen ja tietoturvauhista informoimisen.
8. Käyttöturvallisuus
  - a. Käyttöturvallisuuden alla käsitellään pääsynhallintatoimet sekä fyysisellä, loogisella, että immateriaalitasolla. Usein myös salasana-käytännöt sisällytetään käyttöturvallisuuteen. (ISO 27002 2013, 8–10, 14–16.)

Yrityksen liiketoiminnan luonteesta ja laajuudesta riippuen osioiden kriittisyysaste ja osioiden painotukset saattavat vaihdella. Tietoturvallisuuden monipuolinen käsittely

vaikuttaa myönteisesti yritysturvallisuuden rikosturvallisuutta, pelastustoimintaa, valmiussuunnittelua, ympäristöturvallisuutta, henkilöturvallisuutta, kiinteistö- ja toimitilaturvallisuutta sekä toiminnan ja tuotannon turvallisuutta käsitteleviin sektoreihin.

Tietoturvallisuuden tehokas toteuttaminen edellyttää perustasoisten murtosuojausmenettelyjen, kulunvalvonnan, todistusaineiston keräämisen turvaamisen, palontorjunnan, kriisistä palautumisen, jätteiden käsittelyn, kierrätyksen, henkilötietojen hallinnan ja teollisuuslaitteiden ylläpidon suunnittelua ja turvallista toteutusta. Hallintakeinoina edellä luetellut liittyvät olennaisesti aiemmin mainittuihin muihin yritysturvallisuuden osa-alueisiin. (ISO 27002 2013, 8–10.)

### **3.2.1 Hallinnollinen tietoturva**

Tietoturvallisuus ei ole tila, vaan prosessi. Tietoturvallisuus vaatii yrityksen johdolta sitoutumista ja strategista suunnittelua, tarvittavien resurssien ja vastuiden allokoimista sekä asianmukaisten toimintamallien ja suunnitelmien luomista. Tietoturvallisuus edellyttää erillisen tietoturvaohjelman laadintaa, jolla tietoturvallisuuden tavoitteet jalkautetaan yrityksen joka tasolle. (ISO 27002 2013, 15–17.)

Monissa yrityksissä toimitaan reaktiivisella mallilla, jossa toimitaan vasta ulkopuolisen toimijan aloitteen jälkeen. Tietoturvallisuuden kehittäminen vaatii jatkuvaa riskien ja uhkakuvien kartoittamista ja niihin reagoimista. Tietoturvallisuuden hallinta tähtää proaktiiviseen malliin, jossa tilanteeseen on reagoitu ennen uhkakuvan realisointia, jolloin aloite on yrityksellä. (ISO 27002 2013, 8–10.)

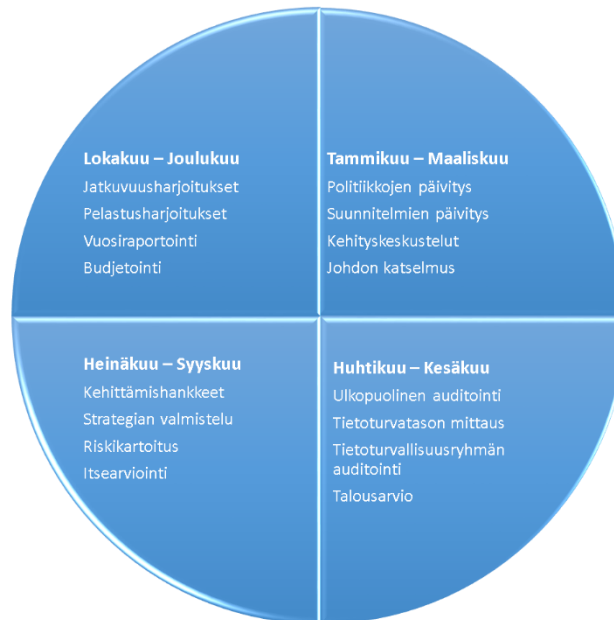
Tietoturvallisuuden prosessina voidaan käyttää esimerkiksi PDCA-mallia (Kuvio 1 PDCA-vuosikello), joka koostuu neljästä vaiheesta:

Plan = Suunnitteluvaihe, jossa laaditaan suunnitelma tietoturvallisuuden kehittämiseksi.

Do = Toteutusvaihe, jossa ryhdytään toteuttamaan suunniteltuja tavoitteita.

Check = Tarkistusvaihe, jossa verrataan toteutunutta tavoitteisiin.

Act/Adjust = Mukautumisvaihe, jossa ohjataan toimintaa oikeaan suuntaan.  
(ISO 27000 2009, 24)



Kuvio 1. PDCA-vuosikello

Mikäli yrityksessä on käytössä laatu järjestelmä (ISO 9001) tai vastaava järjestelmä, voidaan tietoturvallisuuden hallinta sisällyttää olemassa oleviin kehitysprosesseihin.  
(ISO 27001 2009, 8-10, 22.)

### 3.2.2 Fyysinen tietoturvallisuus

Tietoaineiston ollessa fyysisessä tai fyysiselle medialle talletetussa olomuodossa, tieto voi fyysisesti tuhoutua, sitä voidaan muunnella tai se voidaan varastaa fyysisessä ympäristössä. Konkreettisesti fyysinen tieto on myös helposti muunnettavissa immateriaaliseksi tai loogiseksi tiedoksi. Tästä syystä tietoon pääsyä tulee rajoittaa fyysisesti. (ISO 27002 2013, 77.)

Tiedon fyysiset tilat tulee luokitella tiedon luokittelua vastaavalle tietoturvasolle, jotta estetään asiattomien pääsy tietoon, jolloin tiloissa tapahtuvaa liikkumista tulee

myös valvoa (kulunvalvonta) ja luvaton tunkeutuminen estää. Tunkeutumisen estäminen toteutetaan useimmiten vahvistamalla tilan murtosuojausta. (ISO 27002 2013 77.)

Tunkeutumisen estämisen jatkeena tulee huomioida myös fyysisen kosketuksen, veden, tulen, auringonvalon, sähkön, sähkömagnetismin sekä mikrobien pääsy tilaan, tarkoituksella tai vahingossa. (ISO 27002 2013, 81.)

- Fyysinen kosketus altistaa kaiken tietoaineiston rikkoutumiselle. Paperi voi revetä, optinen levy voi naarmuuntua, kiintolevy voi pudota ja ihon rasvat tuhoavat valokuva- ja mikrofilmimateriaalia. (ISO 27002 2013, 77, 83.)
- Vesi tuhoaa paperiasiakirjat, sekä sähköiset tallennusmediat, mutta ei vaikuta optiseen tallennusmediaan. (ISO 27002 2013, 77, 83.)
- Liian suuri ilmankosteus edistää mikrosienten kasvua paperissa (home) sekä nopeuttaa elektronisissa komponenteissa metallien hapettumista. Näistä syistä arkistoja ei tulisi sijoittaa kellarikerrokseen eikä sprinklerijärjestelmää tai perinteisiä jauhesammuttimia tulisi käyttää paperiarkistoja tai sähköisiä tallennusmedioita sisältävissä tiloissa, vaan on käytettävä esimerkiksi kaasusammutuslaitteistoa ja hiilidioksidisammuttimia. (Kaasusammutinlaitteistot 2015, 11.)
- Tuli tuhoaa käytännössä jokaisen muistimedian, jolloin kriittinen tieto tulisi sijoittaa palosuojakaappiin. Tässä tulisi huomioida, että palosuojakaappi ei ole kassakaappi eikä kassakaappi ole välttämättä palosuojakaappi. (ISO 27002 2013, 77, 83, 92.)
- Valon ultravioletti- ja infrapunasäteily tuhoaa paperiasiakirjat, valokuvat, mikrofilmin sekä optiset muistimediat, jolloin joko luonnonvalon pääsy tilaan on estettävä tai suodatettava. (ISO 27002 2013, 77, 83.)
- Jännite- tai virtapiikit tuhoavat tai korruptoivat sähköistä muistiaineistoa sekä saattavat aiheuttaa tulipalon laiterikon seurauksena. (ISO 27002 2013, 51, 81.)
- Sähkömagneettinen kenttä tuhoaa sähköistä tietoaineistoa. Mahdollisia lähteitä ovat esimerkiksi kaiuttimet (magneettilliset), radioaallot ja metallinpaljastimet. (ISO 27002 2013, 51, 81.)

Näiden seikkojen vuoksi on laadittava selkeät ohjeistukset, miten luokitelluissa tiloissa työskennellään, jotta vältytään tiedon tahattomalta korruptoitumiselta, muuntumiselta, tuhoutumiselta tai luvattomalta käytöltä.

Fyysinen turvallisuus käsittää myös tiedonsiirto- ja sähkökaapeloinnin suojaamisen luvattomalta liittymiseltä, tarkkailulta sekä häirinnältä. Esimerkiksi arkiston tai palvelintilan sähkönsyöttö tulisi suojata siten, ettei järjestelmän tiedonsiirtoa tai sähkönsaantia voida häiritä luvattomasti. Palvelimet on sammutettava hallitusti sähkökatkutilanteessa, mikä vaatii varavoimajärjestelmän tai akuston käyttöä. (ISO 27002 2013, 85.)

Tilojen kulunvalvonnassa käytettävät erilaiset sähköiset lukot toimivat toisistaan poikkeavilla tavoilla sähkökatkoksen aikana. Esimerkiksi sähkömagneettilukko avautuu sähkökatkoksesta, missä taas sähkömoottorilukko ei. Tiedonsiirtokaapelointiin pääsy mahdollistaa tiedonsiirron kaappaamisen, seuraamisen ja väärentämisen, esimerkiksi kulkuoikeuden väärennysmielessä tai palvelimen tapauksessa kriittisten tietojen urkinnan, tietoliikenneverkon häirinnän tai palvelimen saastuttamisen. (ISO 27002 2013, 76–82.)

### **3.2.3 Laitteistoturvallisuus**

Laitteistoturvallisuus on selkeintä käsitellä laitteiston elinkaaren hallinnan kautta:

Valmistusvaiheessa laitteet rakennetaan ensin tehtaalla komponenteista, joihin osaan on ajettu firmware- ohjelmisto (käskykanta). Seuraavaksi laitteeseen asennetaan käytettävät ohjelmistot ja tehdään asetussäätelyt. Valmistusvaiheen elinkaaren hallinnassa on huomioitava laitteistovalmistajan luotettavuus komponentti- tai firmware-riskien vähentämiseksi. Komponenttiriskejä ovat esimerkiksi komponenttien harvinaisuus (hintaa, toimitusvaikeudet) ja laatu (käyttöikä). Firmware-riskit voivat ilmetä huonona yhteensopivuutena tai komponenttien virheellisestä suorittamisesta aiheutuvina virheellisinä toimintoina, jotka voivat aiheuttaa tietoturvahäiriön tai tietyissä olosuhteissa mahdollistaa luvattoman pääsyn järjestelmään. (ISO 27002 2013, 149.)

Myyntivaiheessa jälleenmyyjä saattaa asentaa laitteeseen omia apuohjelmiaan, jotka voivat olla lopullisen käyttötarkoituksen näkökulmasta tarpeettomia tai tietoturvan kannalta riskialttiita. Myyjän kanssa onkin dokumentoitava, mitä komponentteja käytetään, mitä laitteeseen asennetaan, millaiset selvitykset asennuksista on toimitettava, miten itse laitteen toimitus järjestetään ja miten vastuut ja takuut jakautuvat. Näillä toimilla ehkäistään luvattomien apuohjelmien pääsyä järjestelmään. (ISO 27002 2013, 144–148.)

Käyttöönottovaiheessa laitteeseen asennetaan toimintaympäristössä tarvittavat ohjelmistot, asennetaan firmware- ja ohjelmistopäivitykset, asetetaan järjestelmäasetukset ja tarkistetaan järjestelmät aiemmin mainittujen apuohjelmien varalta. Kun laitteen asianmukainen toimivuus on varmistettu, liitetään laite huolto-, ylläpito- ja kierrätysohjelmaan. (ISO 27002 2013, 87, 148.)

Käyttövaiheessa laitteeseen asennetaan järjestelmällisesti ohjelmisto- ja firmware-päivitykset ja komponenteille tehdään ylläpitohuolto ylläpito-ohjelman mukaisesti. Ohjelmassa tulisi huomioida tarvittaessa myös varalaitteiden ja varaosien saataavuus. Mikäli huoltopalvelu on ulkoistettu, on oltava dokumentoituna huollon suorittaja, toimenpiteiden kirjaus sekä vastuut ja työn takuu. Käyttövaiheessa tulee kiinnittää huomiota myös laitteiston suojaamiseen ympäristön ja käyttäjän toimilta. Esimerkiksi tietokoneen keskusyksikön tulisi sijaita vähintään 10 cm lattiatason yläpuolella pölyn tarpeettoman kertymisen ja vesivahingon varalta. Lisäksi on huomioitava nesteiden kaatumisen mahdollisuus työpöydältä. Reitittimet, kytkimet, IDS/IPS-järjestelmät, palomuurit ja palvelimet on pidettävä tarkasti valvotussa tilassa staattisissa olosuhteissa. (ISO 27002 2013, 77, 92–94.)

Poisto- ja kierrätysvaiheessa laitteesta poistetaan kaikki luokiteltu tieto. Matalan luokituksen tiedossa riittävä toimenpide on kiintolevyn tyhjennys esimerkiksi Gutmann-metodilla (tieto ylikirjoitetaan lukuisia kertoja satunnaisella tiedolla), mutta korkean luokituksen tiedossa muistivälineen fyysinen tuhoaminen on ainoa tapa varmistua, ettei tietoa voida palauttaa. Muut laitteiston komponentit voidaan kierrättää yrityksen kierrätyspolitiikan mukaisesti. (ISO 27002 2013, 11, 49, 75, 121,171.)

Erityishuomiota on annettava laitteille, joita käytetään yrityksen tilojen ulkopuolella. Näille laitteille on laadittava selkeä käyttö-, säilytys-, kuljetus-, varkaudenesto- ja



etähallintapolitiikka ja niihin liittyvä ohjeistus. Laitteiden käyttö poikkeaa muista laitteista siten, että laitteeseen on pääsy myös ulkopuolisilla henkilöillä eikä käyttöympäristöä voi kontrolloida samalla tavalla kuin yrityksen sisällä. Laitteeseen tulisi merkitä selkeästi käyttörajoitukset esimerkiksi tekstillä: ”Ainoastaan työntekijän X käyttöön”. (ISO 27002 2013, 22–26.)

Tällaiset laitteet on suojattava fyysisen rikkoutumisen varalta suojakotelolla ja tarvittaessa iskusuojakalvolla. Lisäksi laite on suojattava katoamisen ja varkauden varalta fyysisillä lukitusmenettelyillä (esim. Kensington-lukitus) ja etäkäyttömahdollisuudella. Etäkäytön tulisi mahdollistaa laitteen lukitseminen, tietojen kopioiminen ja poistaminen, sekä laitteen jäljitys. Useimmat varkaudenestojärjestelmät mahdollistavat myös viestin lähettämisen laitteen löytäjälle/luvattomalle käyttäjälle. (ISO 27002 2013, 82, 88, 90, 92.)

### **3.2.4 Ohjelmistoturvallisuus**

Yrityksen tietojärjestelmät käyttävät lukuisia ohjelmistoja, joiden ylläpidon on oltava järjestelmällistä. Käytettävät ohjelmat tuleekin luetteloida ja lisenssien voimassaolo sykliä selvittää. Ohjelmistojen ja lisenssien luetteloinnin jälkeen tunnetaan ne ohjelmistot ja lisenssit, joiden käyttö on toiminnan kannalta välttämätöntä jolloin tarpeettomat ohjelmistot ja lisenssit voidaan poistaa käytöstä ja tarpeettomien ohjelmistojen asentaminen voidaan estää. (ISO 27002 2013, 141, 169–171.)

Ohjelmistoihin on usein eritasoisia käyttäjätunnuksia, jolloin käyttäjälle ja ylläpitäjille tulisi rajata pienimmät mahdolliset oikeudet ohjelmistoon tarpeettomien ja luvattomien muutosten estämiseksi. Ohjelmistoille tulee laatia ylläpitosuunnitelma, jonka perusteella ohjelmistojen ohjelmistopäivitykset asennetaan, ja ongelmatilanteiden varalle on kohdennettu riittävästi henkilöresursseja. Mikäli tukipalvelut on ulkoistettu, tulee sopimuksella yksilöidä selkeästi, mihin käyttötarkoituksiin ylläpito-oikeuksia käytetään. Ulkopuolisten ylläpitäjien oikeudet on siis rajattava mahdollisimman suppeiksi. (ISO 27002 2013, 127, 135.)

Ohjelmistot tulee valita siten, että ne tukevat tietoturvasuoritusajattelua. Esimerkiksi asiakirjahallintajärjestelmän tulee kirjata, kuka on käyttänyt mitäkään asiakirjaa, mitä

asiakirjalle on tehty ja koska asiakirjaa on käytetty. Nämä toimenpiteet eivät kuitenkaan ole toimivia, vaikka ohjelmisto sen mahdollistaisikin, mikäli tunnistus ja todennustoimenpiteet ovat puutteellisia. (ISO 27002 2013, 95.)

Ohjelmistoturvallisuuden osana on myös viruksilta ja haittaohjelmilta suojautuminen. Suojautuminen tapahtuu ylläpidetyillä viruksentorjuntaohjelmilla ja haittaohjelmien poisto-ohjelmilla, mutta myös varmuuskopiointilla on yhä suurempi merkitys ransomware- ja cryptoware-haittaohjelmien yleistyttyä. (ISO 27002 2013, 99.)

Ransomware on haittaohjelma (malware), joka lukitsee saastuneen koneen ja esittää lunnasvaatimuksen koneen lukituksen avaamiseksi. Useimmat ransomware-haittaohjelmat on poistettavissa lunnaita maksamatta. Mikäli käyttäjä maksaa lunnaat, luonnollisestikaan koneen lukkiutumisen poistuminen ei ole varmaa. (Ransomware [viitattu 15.4.2015].)

Cryptoware tekee saman mitä ransomware, mutta sen lisäksi cryptoware nimensä mukaisesti kryptaa (salakirjoittaa) tiedostot. (Ransomware [viitattu 15.4.2015]).

Esimerkki: Cryptoware iskee kuukauden 25. päivä ja varmuuskopiointi tehdään kuukauden 1. ja 15. päivä. Varmuuskopioimatonta tietoa on siis 10 päivän ajalta. Vaihtoehdot ovat seuraavat:

1. Palautetaan 15. päivän varmuuskopiosta tiedot, menetetään 10 päivän tiedot (hyväksytään tietojen menetys).
2. Joihinkin cryptoware-haittaohjelmiin on olemassa valmiit purkuohjelmat.
3. Jos valmista purkuohjelmaa ei ole, niin salausmenetelmän selvittäminen on mahdollista, mikäli yhdestä saastuneesta tiedostosta on olemassa muuttumaton varmuuskopio. Näiden perusteella voidaan ratkaista yksinkertaiset kryptausmenetelmät. (Ransomware [viitattu 15.4.2015].)

Edellä mainitun esimerkin mukaisesti cryptowaren salauksen purkaminen ei ole välttämättä mahdollista, jolloin tiedosta menetetään se, mikä on varmuuskopioimatta cryptowaren iskuhetkellä. Tästä syystä yrityksissä tulisi paneutua varmuuskopiointiin ja tunkeutumisen havaitsemis- ja estojärjestelmiin, sillä nämä ovat ainoat keinot estää koneen ja työpaikan verkon saastuminen.

Olennaista on myös menettelyiden huolellinen dokumentoiminen. Ohjelmistojen asennuksista, päivityksistä, käytöstä poistamisesta, käyttöoikeuksista ja ylläpitotoimista on pidettävä ajantasaista lokia. (ISO 27002 2013, 98–104.)

### 3.2.5 Tietoaineiston turvallisuus

Yrityksessä on abstrakti massa tietoa, jonka luokittelu eri laisiin kategorioihin on lähtökohta tiedon turvaamiselle. Tietoa on fyysisessä, loogisessa ja immateriaalisessa muodossa, mistä johtuen erityyppisten tietoaineistojen luokittelujen on oltava yhdenmukaiset. Tiedon, tiedon käsittelijän, käsittelytilan, käsittelylaitteen, tietoliikenneväylän, tiedon reflektointiympäristön sekä tiedon tuhoamismetodin on oltava luokiteltu yhdenmukaiselle tasolle. Mikäli tietoa lähetetään yrityksestä ulos, on selvitettävä, mikä tietoturvasuustaso vastaanottavassa yrityksessä vastaa lähettävän yrityksen tietoturvasuustaso.

Työssä käytetään neliportaista luokittelua: julkinen, luottamuksellinen, salainen ja erittäin salainen.

1. Erittäin salainen tieto (Ytterst hemlig, top secret) on tieto, joka paljastuessaan aiheuttaa katastrofaalista vahinkoa yritykselle, esimerkiksi asiakasrekisteri, laskutusrekisteri, tai prototyypin tuotekehitystiedot.
2. Salainen tieto (Hemlig, secret) on tieto, joka paljastuessaan aiheuttaa merkittävää vahinkoa yrityksen liiketoiminnalle. Esimerkiksi kilpailutustarjous. Arkaluonteiset henkilötiedot kuuluvat vähintään tähän kategoriaan.
3. Luottamuksellinen (Konfidentiell, confidential) tieto on tietoa, jonka paljastumisesta aiheutuu vähäinen haitta liiketoiminnalle. Luottamuksellista tietoa on esimerkiksi asiakkaan kanssa solmittu sopimus.
4. Julkinen tieto on tietoa, joka ei aiheuta haittaa yrityksen toiminnalle paljastuessaan. Julkista tietoa ovat esimerkiksi markkinointimateriaali, aukioloajat ja yrityksen osoitetiedot. (ISO 27002 2013, 45.)

Tiedon luokittelun jälkeen tieto on merkittävä luokitustaan vastaavasti. Julkisen tiedon merkitseminen on yleensä tarpeetonta ja työlästä, siksi ainoastaan luottamukselliset, salaiset ja erittäin salaiset tiedot merkitään. Merkintä voidaan tehdä joko

suppealla merkintäkaavalla (malli seuraavalla sivulla) tai laajalla merkintäkaavalla (Liite 1: Tietoturvallisuusluokittelun asiakirjan kansilehti). Merkinnöissä voidaan käyttää myös värejä tai muita visuaalisia merkkejä erottamaan ne toisistaan. Useimmissa tapauksissa karkea luokittelu on riittävä, mutta tietyissä tilanteissa lisätarkenteet ovat tarpeen, sillä pelkkä tasoluokittelu ei rajaa käyttöoikeutta riittävästi, varsinkin suuremmissa yrityksissä. Liitteessä 1 on esitelty esimerkki asiakirjan luokittelusta. (ISO 27002 2013, 43, 45, 47, 49.)

Esimerkki: Olkoon yrityksessä 5 osastoa. Osastojen yhteiseltä kahvipöydältä löytyy asiakirja, joka on merkitty: ”Luottamuksellinen”. Paikalla on jokaisen osaston esimies, jolla on oikeus käsitellä oman osastonsa luottamuksellista tietoa. 80 % todennäköisyydellä henkilö, jolla ei ole oikeutta käsitellä kyseistä tietoa, käsittelee tietoa avaamalla asiakirjan selvittääkseen kenelle asiakirja on osoitettu.

Yllä mainittu ongelma on ratkaistavissa lisäämällä luokitteluun merkintä ”Osasto X”, missä X on tietoa käsittelevä osasto (Kuvio 2 Suppea luokittelumerkintä).



Kuvio 2. Suppea luokittelumerkintä

### 3.2.6 Tietoliikenneturvallisuus

Tietoliikenne käsittää kaiken datan, mitä lähetetään sisäisissä sekä laajaverkoissa. Tietoliikenteen turvallisuus on taattava sekä fyysisessä että loogisessa ympäristössä. Fyysisellä tasolla tietoliikenteen turvaaminen tarkoittaa reitittimien, kytkimien sekä kaapeloinnin suunnittelua siten, että minimoidaan luvattoman käytön ja tahattoman vahingoittumisen riski. Käytännön tasolla tarkoittaa sitä, että reitittimet ja kytkimet on koteloitava siten, ettei luvattomilla henkilöillä ole niihin pääsyä. Kaapelointi ja tietoliikennesiirteiden sijoittelu on toteutettava siten, että luvaton kytkeytyminen estetään. Käyttäjien laitteistoista on myös estettävä ulkoisten verkkosovittimien käyttö tietoturvallisuuden kiertämisen estämiseksi. (ISO 27002 2013, 85.)

Verkon fyysinen rakenne on myös olennainen osa tietoturvallisuutta. Kriittisiä järjestelmiä varten tulisi rakentaa oma fyysinen verkko, johon ei ole pääsyä ulkopuolelta. Tällöin voidaan merkittävästi vaikeuttaa ulkopuolisia tunkeutumisyrityksiä kriittisiin järjestelmiin. Eri osastot tulisi myös jakaa eri verkkoihin virtuaalilähiverkoin tai fyysisin lähiverkoin. (ISO 27002 2013, 85, 119.)

Kun fyysisellä tasolla on saatu luotua selkeät reitit tietoliikenteelle, voidaan käsitellä loogisia ratkaisuja säätelemään liikennettä mainituilla reiteillä. Loogisella tasolla tietoturvallisuuden kulmakivet ovat palomuurit ja tunkeutumisen havaitsemis- ja estojärjestelmät (jatkossa IDS/IPS). Palomuurille annetaan sääntöjä, joiden perusteella palomuuuri päästää liikennettä sisään ja ulos, mutta palomuuuri ei käsittele kovinkaan tarkasti, mitä liikennettä palomuurin läpi kulkee. Palomuuuri on suunniteltu havaitsemaan tunkeutumisia lähes ainoastaan sisäverkon ulkopuolelta. IDS/IPS-järjestelmät tarkkailevat sisäistä verkkoliikennettä ja havaitsevat epäilyttävän liikenteen (havaitsemisjärjestelmä) ja estävät epäilyttävän liikenteen (estojärjestelmä). (ISO 27002 2013, 105.)

Osana tietoliikenneturvallisuutta ovat palvelunestohyökkäysten (DoS, DDoS) havaitsemis- ja torjuntajärjestelmät. Palvelunestohyökkäyksen tarkoitus on lamaanuttaa esimerkiksi internetsivupalvelin ylikuormittamalla palvelin suurella määrällä verkkoliikennettä. Mikäli samalla palvelimella sijaitsevat myös muut verkkopalvelut, samalla kertaa kaatuvat myös muut verkkopalvelut. Tämän vuoksi palvelimet, joilla käsitellään ulkoisia toimintoja, kuten internetsivuja tai sähköpostia, tulisi eriyttää yrityksen kriittisistä palvelimista. (ISO 27002 2013, 123.)

Eriyistä haastetta muodostuu tilanteessa, jossa joudutaan lähettämään arkaluonteista tietoa internetin kautta. Tällöin tulisi luoda suojattu ja salattu yhteys. Tähän suositellaan käytettäväksi VPN-tunnelointia tai muuta vastaavaa menettelyä. (ISO 27002 2013, 55.)

Tietoliikenneturvallisuuden, kuten muidenkin tietoturvallisuuden osa-alueiden painotus on kuitenkin henkilöstön tietoturvallisuustietoudessa. Mikäli työntekijä käyttää väärin hänelle sallittuja ohjelmia tai on varomaton internetin käyttäjä, saattaa käyttäjä aiheuttaa tai merkittävästi helpottaa tietoturvahäiriön tapahtumista loogisista ja

fyysisistä suojauskeinoista huolimatta. Tämän vuoksi onkin laadittava tarkat ohjeistukset langattomien verkkojen ja internetin käytöstä. (ISO 27002 2013, 33, 47, 55.)

Kaikista tietoliikennejärjestelmistä tulisi pitää ajantasaista dokumentaatiota ja kaikki tietoliikennelaitteisiin ja kaapelointiin tapahtuvat muutokset tulee hyväksyttävä ja toteuttaa eri henkilöiden toimesta, jotta vältetään tietoturvallisuuden vaarantavilta virheiltiltä ja tarkoitukselliselta muuntelulta. (ISO 27002 2013, 114, 121, 125).

### **3.2.7 Henkilöstöturvallisuus**

Tietoturvallisuuden näkökulmasta ihminen on immateriaalitietovarasto, jonka luontainen palomuuuri toimii työpaikalla hyvin, työajan ulkopuolella välttävästi ja työsuhteen jälkeen olemattomasti. Tämän vuoksi tietoturvallisuuselementteihin on kiinnitettävä huomiota jo ennen työsuhteen alkua. Henkilöstöturvallisuutta käsitellään tässä työssä kolmijakoisena kokonaisuutena: rekrytointivaihe, työvaihe ja irtisanomisvaihe.

Rekrytointivaiheessa (työpaikkailmoitusta tehtäessä) tulee hakijalle ilmoittaa, mikäli henkilöstä tullaan pyytämään soveltuvuusarvio poliisilta, mikäli henkilöstä tullaan tekemään turvallisuusselvitys tai mikäli henkilöltä edellytetään erityistä osaamista tietoturvallisuuteen liittyen. Työhaastatteluvaiheessa on varmistettava henkilön pätevyys varmistamalla oppilaitos- ja työtodistuksien aitous sekä tulisi tarkistaa suositelijoiden tosiasiallinen asema (lainsäädännön rajoissa). Työhönottovaiheessa henkilön on hyväksyttävä salassapitosopimus, tietoaineiston, käyttöoikeuksien ja tietojärjestelmien käyttöehdot sekä mahdollinen soveltuvuuslausunto- tai turvallisuusselvitysmenettely. (ISO 27002 2013, 29–31.)

Työvaiheen alussa henkilölle on perehdytettävä muodollisella perehdytysmenettelyllä tietojärjestelmien käytön, tietoaineiston käsittelyn ja tiedon luokittelun periaatteet. Henkilö pitää myös ohjeistaa kurinpitomenettelyyn, joka seuraa annetun ohjeiston noudattamatta jättämisestä. Immateriaalisen tiedon korruptoitumisasteen ollessa luontaisesti korkea tulisi harvoin tarvittavaa tietoa kerrata säännöllisesti, sekä järjestää tukiaineistoa joko fyysisessä tai loogisessa muodossa saataville. Henkilön

tietoturvallisuusluokittelu on tarkasteltava uudelleen, mikäli henkilön rooli muuttuu työsuhteen aikana. (ISO 27002 2013, 31, 33, 35, 37, 57.)

Nykyisin tietoturvallisuuteen kuuluu myös henkilöstön suojeleminen ulkoisia uhkia vastaan. Olivat uhat yksinkertaisia vainoamistapauksia tai tunteenpurkauksia, työnantajan tulisi tarkastella, mitä henkilötietoja työntekijöistä luovutetaan ulos. Asiakaspalvelutehtävässä työskentelevän henkilön nimikyltistä ilmenevä etunimi ja sukunimi antavat mahdollisuuden verkkovainoamiselle, mikäli henkilö on rekisteröitynyt johonkin yhteisöpalveluun. Yhdistämällä nimitieto yrityksen parkkipaikalla sijaitsevaan autoon voidaan selvittää työntekijän kotiosoite ja puhelinnumero. Tätä kutsutaan kumulatiiviseksi (kasautuvaksi tai kertyväksi) tiedoksi, jossa kokoelmasta matalle luokiteltua tietoa tuleekin yhtä tai useampaa luokkaa korkeampaa tietoa. (ISO 27002 2013, 33, 35.)

Esimerkki: Tiikerikidnappaus, jossa ensin selvitetään yrityksen maksuliikennettä käsittelevät työntekijät. Seuraavaksi kidnapataan työntekijän läheinen kiristystarkoituksessa. Sitten pakotetaan työntekijä siirtämään yrityksen tililtä lunnasrahat voimakkaan uhka- ja aikapaineen alla. Tiikerikidnappaus-nimitys tulee rikokseen liittyvän seurannan ja ”vaanimisen” elementistä. (PSNI [viitattu 15.4.2015].)

Tähän työnantajan tulisi varautua suojaamalla kriittisten henkilöiden tiedot tietojenluovutuskielloin (Väestörekisterikeskus, Trafi yms.), kouluttamalla sekä teknisesti estämällä varojen siirtäminen ilman hyväksymisketjun käsittelemää tositetta. (ISO 27002 2013, 33, 35.)

Irtisanomisvaiheessa työnantajalla on Suomen rikoslain 30 luvun 5 § mukaisesti kahden vuoden ajan suoja immateriaalioikeuksilleen. Tätä oikeutta voidaan sopusoikeudellisesti jatkaa myös pidempään, mikäli henkilö on hyväksynyt salassapitosopimuksen. (Rikoslaki 1889, 30 luku 5 §.)

Immateriaalioikeuksissa rikosoikeudellisesta näkökulmasta tarkasteltuna on työnantajan kannalta ongelmallista se, että työnantajan on kyettävä näyttämään toteen aiheutunut vahinko. Tämä on monissa tapauksissa erittäin hankalaa, sillä luvattomasti hankitun tiedon omistamista on vaikea toteennäyttää. Salassapitosopimukseen on kirjattava sopimussakko, jonka perusteella voidaan määrätä vahingonkor-

vaus toteennäyttämättä aiheutunutta vahinkoa, sillä nyt sopimuksen rikkominen riittää. Sopimussakon summan ollessa kohtuuttoman suuri, henkilö voi riitauttaa sopimuksen ja saattaa sopimussakon lopullisen suuruuden käräjäoikeuden ratkaistavaksi. (ISO 27002 2013, 39.)

### **3.2.8 Käyttöturvallisuus**

Käyttöturvallisuus käsittää kaikki toimet erityisesti tietojenkäsittelyn suojaamiseksi. Käyttöturvallisuuden perustana toimivat hyvin ylläpidetyt toimintaohjeet. Toimintaohjeet on löydettävä sekä tietojärjestelmien ylläpidosta että järjestelmiä käyttäviltä. Myös tietojärjestelmissä tapahtuviin muutoksiin on käytettävä erillistä hallintajärjestelyä, jossa muutoksen esittäjä ja toteuttaja ovat kaksi eri henkilöä. Tällä estetään muutoksesta aiheutuvat tietoturvatapahtumat ja tietoturvahäiriöt. (ISO 27002 2013, 95.)

Käyttöturvallisuuden kannalta olennaista on kartoittaa ja priorisoida käytettävien palvelujen sekä ohjelmistojen resurssien nykyinen ja tulevaisuuden käyttö. Esimerkkinä mainittakoon, että loppukäyttäjälaitteiden ja verkkolaitteiden käyttöikä on noin viisi vuotta, missä taas tietoliikennekaapeloinnin käyttöikä on vähintään 10 vuotta. Toisena esimerkkinä mainittakoon palveluiden priorisointi. Toiminnanohjausjärjestelmän verkkoliikenteen prioriteetin tulee olla korkeampi kuin YouTube-videon toistamisen. (ISO 27002 2013, 85, 117.)

Käyttöturvallisuus käsittää myös viruksilta ja haittaohjelmilta suojautumisen erityisesti loppukäyttäjälaitteessa. Tällä rajauksella estetään päällekkäisyydet tietoliikenteen turvallisuuden osa-alueen kanssa (verkkolaitteiden suojaaminen). Loppukäyttäjän käyttöoikeuksien rajaaminen tietojärjestelmissä sekä päätelaitteissa estää tehokkaasti haittaohjelmien, virusten ja muiden ei-toivottujen ohjelmien asentumisen järjestelmään. (ISO 27002 2013, 99.)

Käyttöturvallisuudessa käsitellään myös tietojärjestelmien käytön ja ylläpidon seuranta rakentamalla suojattua tapahtumalokikantaa. Lokikannan avulla voidaan havaita tunkeutumisy yrityksiä, onnistuneita tunkeutumisia, asiatonta käyttöä ja aiheet-



tomia muutoksia järjestelmässä. Mikäli on syytä epäillä rikosta, niin tehokas lokitiedostonjen muodostaminen mahdollistaa tehokkaat forensiset (tekninen rikostutkinta) toimenpiteet. (ISO 27002 2013, 105.)

Salasanaturvallisuudella pyritään suojaamaan salasanat arvaamiselta, murtamiselta, kaappaamiselta ja väärentämiseltä. Käyttäjän tulisi laatia riittävän monimutkainen salasana, jonka murtamisessa kuluu riittävän kauan aikaa. Ongelmaksi muodostuu ihmisen muistin ja tietokoneen muistin rakenne-ero. Tietokone kykenee käsittelemään suurella tehokkuudella erilaisia tietotyyppisiä, kuten kokonaislukuja, kirjaimia ja erikoismerkkejä (ihmiseen verrattuna). Ihmisen muistin rakenteesta johtuen ihmisen on vaikea muistaa epäjohdonmukaisia merkkijonoja. (ISO 27002 2013, 61, 63, 65.)

Yleisesti käytetty ohje on, että salasanan tulisi olla vähintään 10 merkkiä pitkä isoista aakkosista, pienistä aakkosista, numeroista ja erikoismerkeistä koostuva merkkijohdistelmä, jolla luodaan suuri merkkientropia (satunnaisuus). Ihmisen kyky muistaa abstrakti merkkijono on heikko, mikä johtaa tukitoimien käyttöön, kuten salasanojen kirjoittamiseen muistilapulle, jolloin salasana on olemassa immateriaalissa muodossa, fyysisenä paperilla sekä loogisena palvelimella.

Olkoon salasana 'sA0pl€okE', jolloin entropia on  $255^8=1,8*10^{19}$ . (Tietokoneen ASCII-merkistössä on 255 merkkiä ja salasana on 8 merkkiä pitkä.)

Olkoon salasana 'Häähää! Murrahan tämä!', jolloin entropia on  $255^{22}=6,2*10^{52}$

Jälkimmäisen salasanan murtoaika on  $4,9*10^{33}$  kertaisesti suurempi ja huomattavasti helpommin muistettava. ( $4,9*10^{33} = 4\ 900\ 000\ 000\ 000\ 000\ 000\ 000\ 000\ 000$ ).

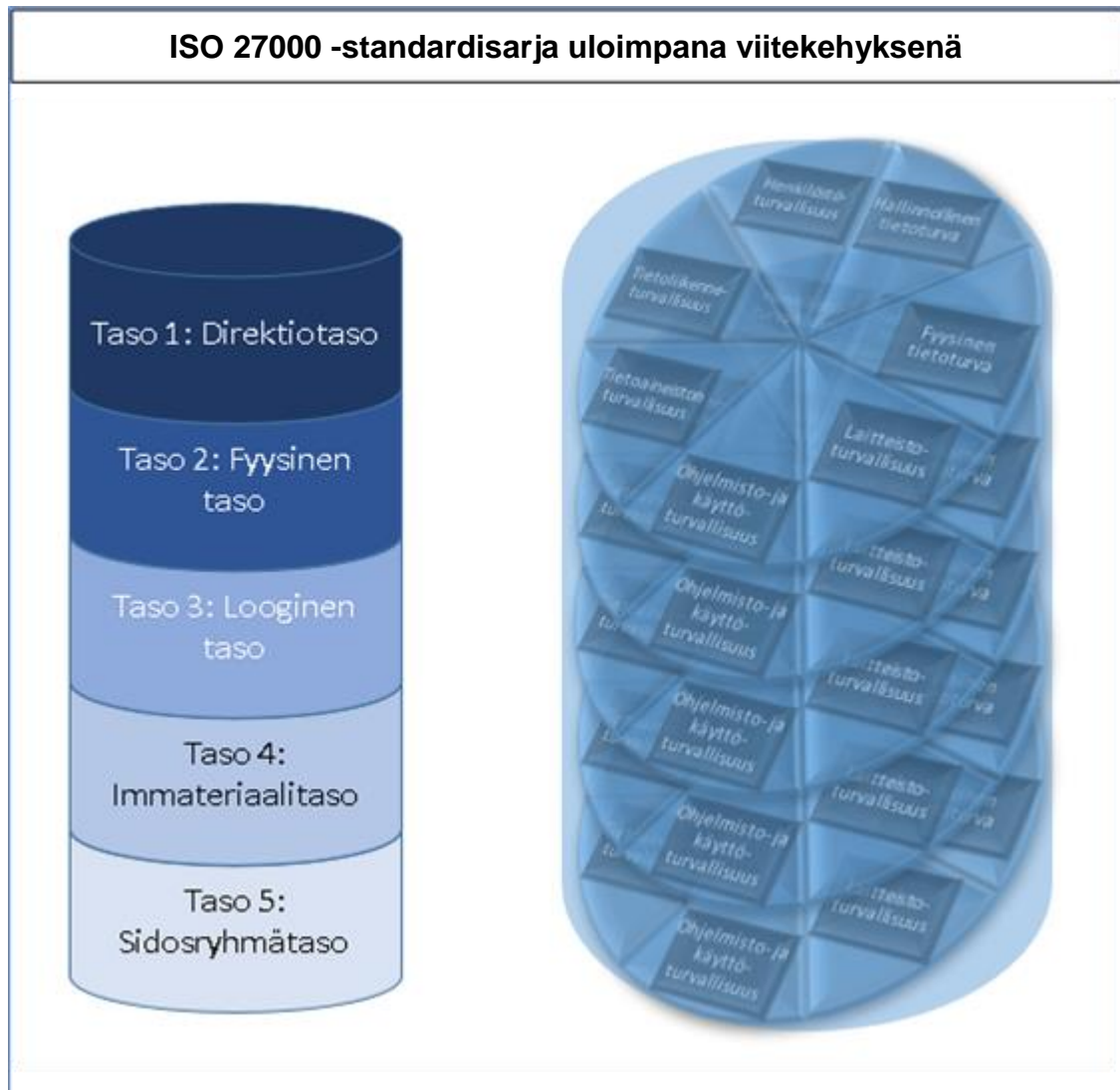
Salasanan selvittäminen on mahdollista myös muilla keinoin. Salasana voidaan selvittää tietyissä olosuhteissa tietoliikenneverkkoa salakuuntelemalla, palvelimen salasanatietokanta murtamalla tai käyttäjän oman yli katsomalla. Tästä syystä salasanojen lähetys ja talletus palvelimille tulisi tapahtua kryptattuna. (ISO 27002 2013, 61, 63, 65.)

## 4 HYBRIDIMALLI

Tietoturvallisuuden laajan ja moniulotteisen luonteen vuoksi tarkoituksenmukaisin tapa käsitellä tietoturvallisuutta ISO 27000 -viitekehyksessä on tehdä se viidestä eri perspektiivistä, joita nimitetään tasoiksi ja tarkastelumallia hybridimalliksi:

1. Direktiotasolla katselmoidaan työnantajan lainsäädännöllisten velvollisuuksien sekä työnoitusvelvoitteiden mukaisesti tietoturvallisuutta.
2. Fyysisellä tasolla tarkastellaan fyysisen tiedon elinkaarta tiedon luomisesta tuhoamiseen sekä loogista tietoa, joka on olemassa fyysisessä olomuodossa.
3. Loogisella tasolla tarkastellaan loogisessa muodossa olevan tiedon elinkaarta tiedon luomisesta tuhoamiseen.
4. Immateriaalitasolla tarkastellaan immateriaalisessa muodossa olevaa tietoa, eli työntekijää informaatioäilynä.
5. Sidosryhmätasolla tarkastellaan yrityksen ja sidosryhmien välistä tiedonsiirtoa sekä tiedon elinkaaren hallintaa.

Jokainen taso on kuvattu konseptin selitetekstillä ja lyhyellä kuvauksella. Mallin toteuttamiseksi on laadittu 200 sivuinen auditointiaineisto, joka käsittää n. 1300 tarkasteltavaa kohtaa.



Kuvio 3. Hybridimalli

Tietoturvallisuus jakautuu auditointiaineistossa 1300 tarkastelukohtaan, joita ei eritellä tässä. Jokaista tasoa käsitellään esimerkein. Tärkein huomio auditointimallissa on, että ensin käsitellään jokin tietty tietoturvallisuuden osio, sen jälkeen käsitellään mainituista 1300 kohdasta ne, jotka liittyvät kyseisen osion direktiotasoon, sitten ne, jotka liittyvät kyseisen osion fyysiseen tasoon ja niin edelleen (kuvio 3, Hybridimalli).

Kun kaikki viisi tasoa on käsitelty, käsitellään seuraava osio direktiotasolla, sitten fyysisellä tasolla jne. Lopuksi kerätään kaikki direktiotason auditointitulokset yhteen ja muodostetaan niistä kokonaisuus. Seuraavaksi kerätään fyysisen tason aineisto ja laaditaan niistä kokonaisuus jne. Visuaalisesti ajateltuna, viisikerroksinen kakku leikataan kahdeksaan palaan.

Jokaisen tason konsepti esitetään kaavakuvalla ja selitteellä, huomioitavaa on, että kaikki kuvat eivät käsittele samaa tietoturvallisuuden osa-aluetta, koska eri tietoturvallisuuden osa-alueilla on luontaiset painotukset eri tasoille. Esimerkiksi tietoliikenteen turvallisuus painottuu loogiselle tasolle.

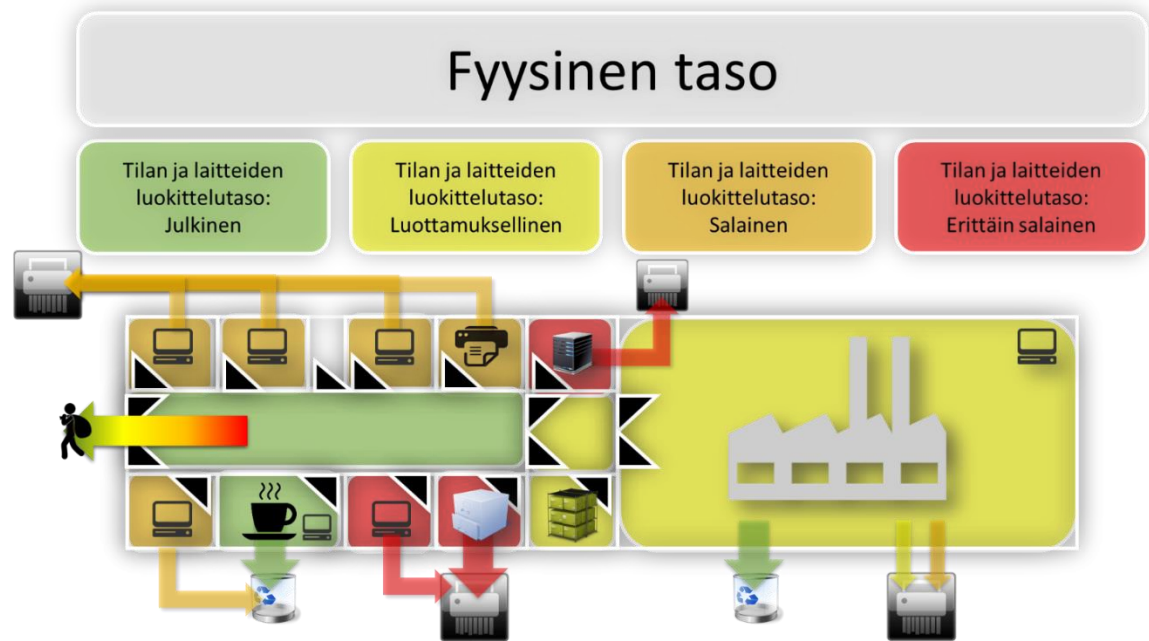


Kuvio 4. Direktiotaso

Tietoturvallisuus käsitellään ensin direktiotasolla, jolla laaditaan tietoturvallisuuden ohjaamiseksi vaadittavat strategiat, toimintamallit ja suunnitelmat. Direktiotaso käsittelee tietoturvallisuuden hallinnolliset aspektit (kuvio 4, Direktiotaso).

Kuviossa on esitetty direktiotason kannanotot laitteistoturvallisuuteen. Huomattavaa on, että laitteita on julkisissa tiloissa, toimistoissa (salainen tila), tuotantotiloissa (luottamuksellinen), serveritiloissa (erittäin salainen) sekä erikseen kriittiseksi merkityssä tilassa (erittäin salainen). Yrityksen johto on laatinut jokaiselle alueelle omat toimintaohjeet ja -rajoitukset, joiden puitteissa laitteistoturvallisuutta toteutetaan.

Esimerkki: Julkisen tilan tietoturvallisuusohjeen laiteturvallisuusosio: "... Tietokoneen keskusyksikön säilytyspaikka on sille hankitussa korotetussa telineessä toimiston sivupöydän alla siten, että ilma pääsee kiertämään keskusyksikön jäähdytysjärjestelmässä eikä riskiä ruuan tai juoman läikyttämisestä laitteen päälle ole. Ohjelmien asentaminen laitteeseen on kielletty. Tarpeellisten ohjelmien asennukset sekä ylläpidon hoitaa tietohallinto..."



Kuvio 5. Fyysinen taso

Fyysisessä tasossa (kuvio 5, Fyysinen taso) käsitellään tietoturvallisuuden osa-alueeseen liittyvät fyysiset aspektit. Tässä esimerkissä käsitellään fyysistä tietoturvalisuutta fyysisellä tasolla, jossa tarkastellaan tietoaineiston turvallisuus konkreettisesti (fyysisessä) ympäristössä:

Toimistoissa sijaitsevien tietokoneiden kiintolevyt on hävitettävä tehokkaasti käytöstä poiston yhteydessä (Ylemmissä toimistoissa), mutta toimistosta voidaan hävittää tietoa myös roskeen heittämällä (julkinen tieto, kahvion vasemmalla puolella oleva toimisto)

Julkisessa tilassa olevan tietokoneen muistit voidaan kierrättää yksinkertaisen tyhjäjätteen jälkeen, koska laite ei sisällä muuta kuin julkista tietoa.

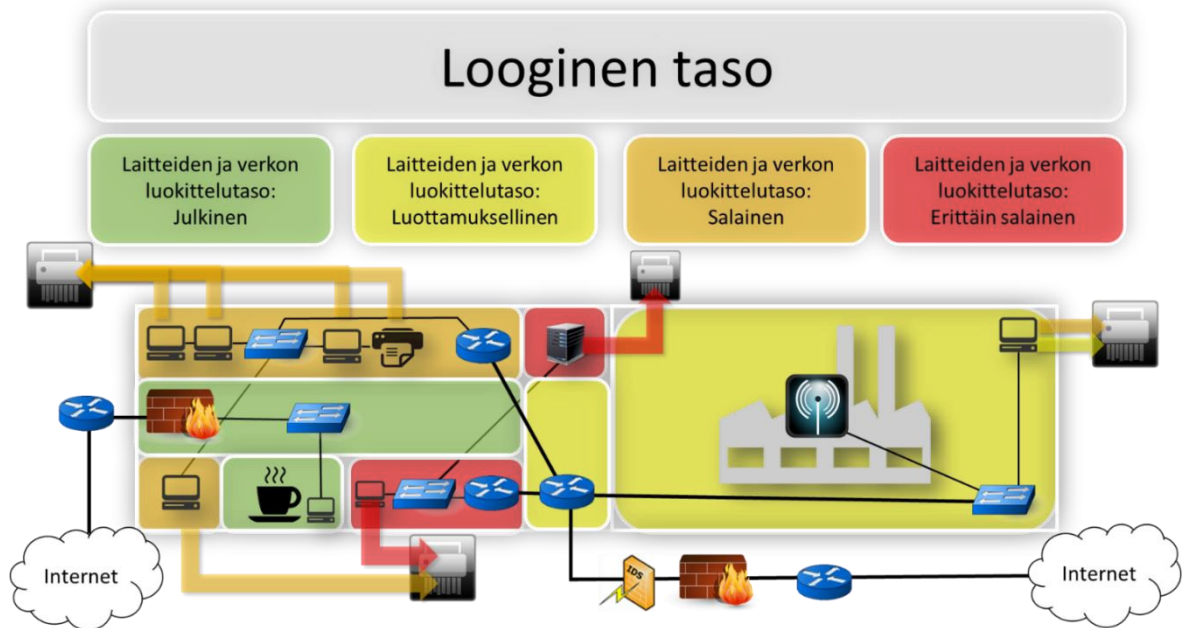
Virhetulosteet on voitava hävittää luotettavasti tulostimelta (silppuri tai keräysastia), lisäksi tulostin on asiattomilta suljetussa tilassa ja erittäin salaiseksi luokitellun tilan tiedot on voitava hävittää tehokkaasti. Lisäksi tietoja ei viedä tilan ulkopuolelle, vaan tieto hävitetään tilassa olevalla silppurilla (alhaalla keskellä).

Arkistot on tuhottava tehokkaasti arkistonmuodostussuunnitelman mukaan valvotusti. Lisäksi kulku arkistoon on rajoitettu. Arkisto on myös suojattu valolta ja kosteudelta. Lisäksi kriittisimmät asiakirjat on sijoitettu paloturvakaappiin (erittäin salaiseksi luokitellun toimiston vieressä).

Palvelintilan tarpeettomat tallenteet on hävitettävä tehokkaasti. Lisäksi palvelintilaan pääsy on rajattu sekä kulunvalvonnan piirissä.

Tuotantotilassa syntyvä tietoaineisto voidaan luokittelun mukaan joko kierrättää tai tuhota.

Yrityksen omaisuuden konkreettinen anastaminen estetään ovien lukituksella, kulunvalvonnalla sekä luontaisella valvonnalla.



Kuvio 6. Looginen taso

Looginen taso käsittelee tietoturvallisuutta tietokoneiden ja verkkolaitteiden näkökulmasta. Kuvassa 6 on esitetty tietoliikenneturvallisuutta ”kyberavaruudessa”.

Loogisen maailman roskakori on Microsoft Windows -käyttöjärjestelmistä tuttu -lähetä roskakoriin painike eli delete. Kuten fyysisestä roskakorista, myös loogisesta roskakorista tiedon takaisin poimiminen on helppoa. Siksi loogisessa ympäristössä käytetään omaa silppuria: Gutmann-metodia. Tieto poistetaan ja sen päälle ylikirjoitetaan, jolloin vaikeutetaan merkittävästi tiedon palauttamista.

Tietoliikenneverkkoja tässä yrityksessä on kaksi: Julkinen verkko, ja työverkko. Julkisessa verkossa on kytkettynä ainoastaan julkista käyttöä varten valittu tietokone, kytkin, palomuri ja reititin. Työverkossa suojaustoimenpiteet ovat järeämmät. Palomuurin lisäksi verkkoon on kytketty tunkeutumisen havaitsemis- ja estojärjestelmä (IDS/IPS). Lisäksi yrityksen eri tietoturvaluokkatasot on jaettu omiksi verkkoalueikseen.

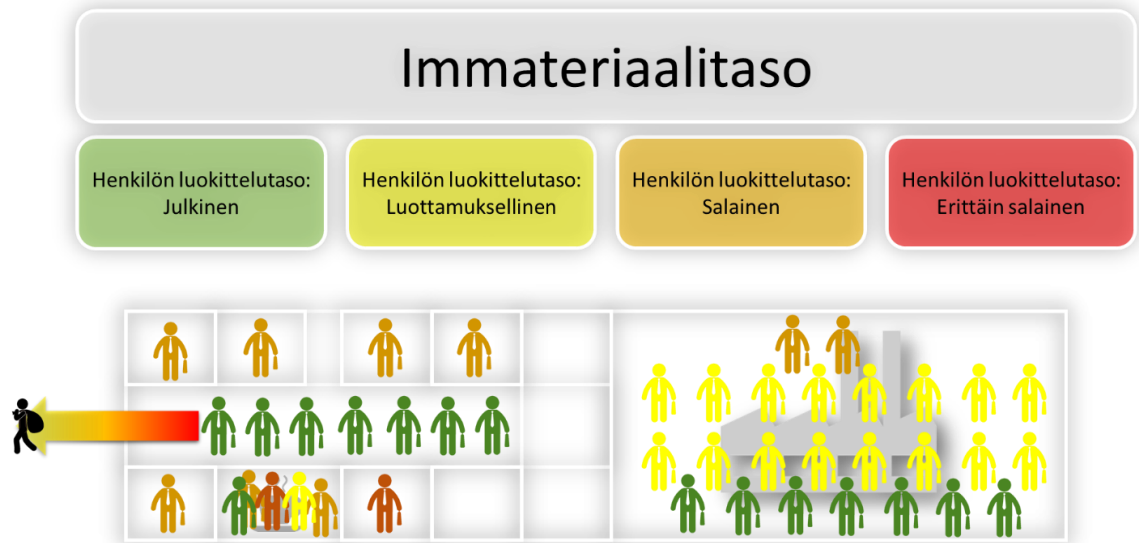


Ulkoa tuleva hyökkääjä pääsee työverkkoon kolmea reittiä pitkin:

1. Internetistä palomuurin ja IDS/IPS:n läpi.
2. Tuotantotilan langattomasta liitäntäpisteestä.
3. Reitittimeen, kytkimeen tai runkokaapelointiin kytkeytymällä.

Suurimman riskin tässä tapauksessa muodostaa langaton (WLAN) liitäntäpiste, koska langattoman verkon laajuutta on vaikea määritellä tarkasti, voidaan langattomaan verkkoon liittyä myös yrityksen ulkopuolelta. Tästä syystä langattomia verkkoja tulisikin käsitellä kuin ulkoisia yhteyksiä. WLAN-liitäntäpisteen jälkeen verkkoon tulisi kytkeä palomuri ja IDS/IPS-järjestelmä.

Jokainen reititin tulisi ajatella liikennevalona, josta voidaan ajaa ”punaisia päin”. Siksi verkossa tulisi olla tunkeutumisen havaitsemisjärjestelmä, joka havaitsee tunkeutumisen verkkoliikennettä seulomalla. Reaalimaailman analogia voisi olla seuraava: Palomuri on nostosilta ja IDS/IPS on tullimies. Palomuri päästää liikennettä läpi ja tullimies tarkastaa epäilyttävät liikennöijät.



Kuvio 7. Immateriaalitaso

Seuraavaksi tarkastellaan tietoa immateriaalitasolla eli työntekijöiden kognitiivista suorituskyykyä, minkä tarkoituksena on kartoittaa tilanteet, jotka aiheuttavat todennäköisesti tietoturvaluuhäiriön (kuvio 7, Immateriaalitaso).

Tässä käsitellään henkilöstöturvallisuutta immateriaalitasossa. Yrityksessä työskentelee eri tasolle luokiteltuja henkilöitä. Henkilöt ovat oletettavasti kanssakäymisessä toistensa kanssa sekä työtehtävissä, taukotilassa ja vapaa-ajalla. Tästä syystä ensiarvoisen tärkeässä roolissa on jokaisen työntekijän henkilökohtaisen tietoturva-ajattelun taso.

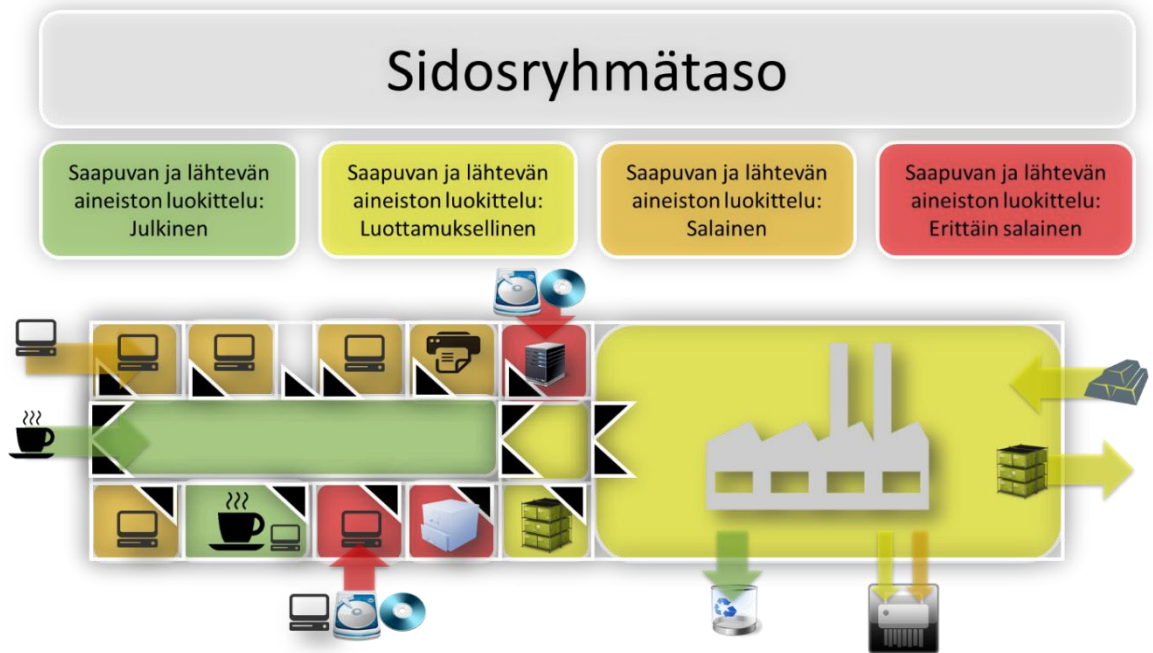
Tuotantotilojen esimiesten tulee osata keskustella ainoastaan luottamukselliseksi luokiteltuja asioita luottamuksellisen tiedon käsittelijöiksi hyväksytyjen henkilöiden kanssa. Esimiehet voivat keskustella salaisista asioista keskenään (reflektoida), olettaen että molemmat ovat oikeutettuja samoihin salaisiin tietoihin. On täysin mahdollista, että esimiehelle 1 on uskottu erilaisia salaiseksi luokiteltuja tietoja, kuin samassa tuotantotilassa toimivalle esimiehelle 2.

Tuotantotilojen luottamukselliset tiedot eivät ole tietoja, joita toimiston salaisen tiedon käsittelyyn luokitellut ovat oikeutettuja käsittelemään, ellei heille ole erityisesti vastuutettu myös tuotantotilojen luottamuksellisia tietoja. Toimistotilojen salaiset tiedot ja tuotantotilojen luottamukselliset tiedot ovat kaksi erillistä kokonaisuutta. Se,

että henkilölle on uskottu tiettyjä salaisia tietoja, ei tarkoita sitä että hänelle on uskottu kaikki salainen tieto.

Kuvasta 7 löytyy kaksi henkilöä, joille on uskottu erittäin salainen tieto. Asema tällaisella henkilöllä on luontaisesti toimitusjohtaja tai varatoimitusjohtaja. Heidän on käytettävä erityistä harkintaa, sillä heillä on tosiasiallisesti lähes rajaton pääsy yrityksen tietoihin. Heidän tulee tiedostaa muiden työntekijöiden tietoturvaluokitus ja jakaa heidän kanssaan ainoastaan heidän tasoilleen luokiteltua tietoa tai jakaa tietoa sensuroidusti siten, että salainen tieto putoaa luokituksessa yhden tai useamman tason alemmas.

Sosiaaliseen manipulointiin on varaudutaan ohjeistamalla työntekijät siten, että ainoastaan julkista tietoa kerrotaan ulkopuolisille. Silloin potentiaalisessa manipulointitapauksessa ainoastaan harmiton julkinen tieto vuotaa ulos. Työntekijät tulee myös ohjeistaa raportoimaan manipulointiyrityksistä esimiehelleen, joka aloittaa tarvittaessa tapauksesta sisäisen tutkinnan, jonka tulosten perusteella päätetään, onko rikostutkinta poliisin toimesta myös tarpeen.



Kuvio 8. Sidosryhmätaso

Viimeisenä tarkastellaan sidosryhmille asetettavat vaatimukset vähintään yrityksen omaa tietoturvasoaa vastaaviksi. Mikäli sidosryhmät ovat asettaneet kartoitettavalle yritykselle tietoturvavaatimuksia, tulisi ne käsitellä direktiotasolla (kuvio 8, Sidosryhmätaso).

Kahvilan kahvitarvikkeiden vastaanotossa ei ole tarvetta suurelle tietoturvatoimelle, koska vastaanotetut tarvikkeet eivät ole tietoturvallisuuden piirissä.

Toimistoihin tuotavat tietokoneet on sisällytettävä elinkaaren hallintaan, kuten laitteistoturvallisuuden osiossa on selvitetty (laitteistoturvallisuus).

Palvelimen ylläpito on myös elinkaaren hallinnan piirissä, lisäksi on selvitettävä ohjelmistojen testaustiedot sekä vianhaku- ja käyttöönoton saatavuus. On myös varmistuttava, että ohjelmistotoimittajan sekä laitteistotoimittajan edustajat ovat riittävän perehtyneitä ja soveltuvia ylläpitotehtäviin (laitteistoturvallisuus, ohjelmaturvallisuus).

Tuotantopuolen raaka-ainetoimittajat on katselmoitava ja luokiteltava alueen luokituksen mukaisesti. Raaka-ainetoimittajille on myös ohjeistettava, miten luokitellulla alueella toimitaan (fyysinen turvallisuus).

Mikäli valmiiden tuotteiden toimituksesta vastaa ulkopuolinen yritys, toimitusyrityksen henkilöstö on tarkastettava ja luokiteltava tilan mukaisesti ja ohjeistettava toimintaan luokitellun tilan vaatimusten mukaisesti (tietoaineiston turvallisuus, fyysinen turvallisuus).

Mikäli salassa pidettävää tietoa tuhotaan ulkopuolisen toimijan toimesta, tulisi varmistua toimijan luotettavuudesta. Tulisi myös varmistua ohjeistuksin, ettei luokiteltua aineistoa päädy kierrätykseen (tietoaineiston turvallisuus, fyysinen turvallisuus, laitteistoturvallisuus).

## 5 KÄYTÄNNÖN TOTEUTUS

### 5.1 Objektiivinen tarkastelu

Tietoturvallisuuden kartoittamisen ensimmäinen toimenpide, on selvittää minkä kriteeristön mukaisesti auditointi tehdään. Seuraavaksi päätetään kartoituksen laajuus, eli mitkä liiketoiminnan osa-alueet sisällytetään kartoitukseen. Tältä pohjalta selvitetään tehokkain auditointitapa ja laaditaan auditointiaineisto. (ISO 27003 2010, 16, 19, 25, 40, 44.)

Auditointimallin päättämisen jälkeen laaditaan auditointiaineisto. Auditointiaineisto toimii auditoidijan työkaluna, jolloin saadaan suuri kokonaisuus asioita luonnosteltua helposti käsiteltäviin kokonaisuuksiin ja pystytään pitämään kirjaa käsiteltävistä asioista. Laadittu auditointipohja toimii checklist-periaatteella, johon on lisätty tilaa muistiinpanoille jatkotoimien suunnittelua varten. Auditointiaineistosta tuli tällä periaatteella 200 sivuinen ja käsittää 1272 tarkasteltavaa kohtaa ISO-tietoturvallisuuden osioittain jaoteltuna. Käytännön syistä koko aineistoa ei julkaista. Liitteessä 2 on esitelty auditointiaineistoesimerkki. (ISO 27003 2010, 44, 46.)

Auditoinnissa selvitetään tarvittavat tiedot haastatellen eri asemassa olevia työntekijöitä, sekä suoritetaan omatoimista havainnointia. Tulokset kirjataan auditointiraporttiin, joka toimitetaan toimeksiantajalle. Auditointiraportin perusteella voidaan luoda vertailutaso, sekä alustava kustannusarvio kehityskustannuksista, tätä käytetään kehityksen arvioimisessa. Lisäksi voidaan samalla tarkastella, millä yleistasolla tietoturvallisuus on.

Lopuksi laaditaan kehityssuunnitelma ja -aikataulu, jolla tietoturvallisuutta kehitetään. Seuraavassa kuviossa (Kuvio 9 Opinnäytetyön toteutuskaavio) on esitetty opinnäytetyön toteutus vaiheittain sekä osioihin kulunut aika. Karkeasti jako on kolmitahoinen: Alkutoimet (6 viikkoa), käytännön toimet (6 viikkoa) ja jälkitoimet (2 viikkoa).



Kuvio 9. Opinnäytetyön toteutuskaavio

## 5.2 Subjekttiivinen tarkastelu

Työn tavoite oli selkeä: Kehittää yrityksen tietoturvaluustaso, laatia tietoturvaluusauditointimalli ja samalla soveltaa ISO 27000 -standardeja. Aineistona käytettiin pääasiallisesti ISO 27000-, 27001-, 27002- ja 27003-standardien sisältöä sekä henkilökohtaista osaamista tietoturvaluudesta ja turvallisuusauditoinnista. Auditointiaineiston laatiminen oli ensimmäinen suuri kokonaisuus työn tekemisessä. Auditointiaineiston laadinta eteni hitaasti, mutta johdonmukaisesti, tietoturvaluuden auditoinnin ollessa vierasta.

Auditoinnin rakenne esiteltiin toimeksiantajalle, joka hyväksyi toteutusmallin. Toimeksiantajan kanssa pidettiin aloituspalaveri, jossa allokoitiin auditointiin käytettävät resurssit sekä toimeksiantajan toivomat painotukset, sekä henkilöstö, joka osallistuisi auditointiin. Seuraavaksi suoritettiin haastattelut ja katselmukset. Paras tulos saavutetaan, kun haastatellaan eri tavoilla tietoturvaluutta käsitteleviä henkilöitä, jolloin saadaan paras kuva toimeksiantajan todellisista toimintamalleista. Esimerkiksi haastatteleamalla erilaisissa tehtävissä työskenteleviä henkilöitä.

Toimeksiantaja saa kopion työ julkisesta osasta sekä salaisesta auditointiraportista. Yhdessä nämä kaksi asiakirjaa toimivat tiedoksiantona tietoturvallisuusauditoinnin tuloksista, joiden pohjalta toimeksiantaja voi ryhtyä haluamiinsa toimenpiteisiin tietoturvallisuutensa kehittämiseksi.

Yhteistyö toimeksiantajan kanssa sujui hyvin ja tietoturvallisuuteen suhtauduttiin riittäväällä vakavuudella. Tietoturvallisuusauditointi pakotti toimeksiantajan ajattelemaan omaa asemaansa tietoyhteiskunnassa uudelleen. Tietoturvallisuuden kehittäminen kustannustehokkaasti vaatii avointa mieltä sekä luovaa olemassa olevien resurssien käyttöä. Uusia aluevaltauksia on tehtävä, uudenlaisia resursseja on allokoitava muuttuvassa tietoyhteiskunnassa toimiessa.

Auditoinnin aikana kyettiin havaitsemaan selkeää kehitystä toimeksiantajan tietoturvaluustietoisuudessa sekä -asenteissa, mutta lopullisen toimintakulttuurimuutoksen näyttää vain aika.



## LÄHTEET

Kaasusammutuslaitteistot. Huhtikuu 2015. Finanssialojen keskusliitto. Inerttikaasusammutuslaitteistot: suunnittelu ja asentaminen

L 26.1.2001/55. Työsopimuslaki.

L 19.12.1889/39. Rikoslaki.

ISO 27000. 2009. Suomen Standardisoimisliitto SFS. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto.

ISO 27001. 2013. Suomen Standardisoimisliitto SFS. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

ISO 27002. 2013 Suomen Standardisoimisliitto SFS. Tietoturvallisuuden hallintakeinojen menettelyohjeet.

ISO 27003. 2010. Suomen Standardisoimisliitto SFS. Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita.

Viestintävirasto. Ei päiväystä. Ransomware [www-dokumentti] Viestintävirasto. [viitattu 15.4.2015]. Saatavissa: <http://www.ransomware.fi/>

Yritysturvallisuus. Ei päiväystä. Yritysturvallisuus [www-dokumentti]. Elinkeinoelämän keskusliitto. [viitattu 15.4.2015]. Saatavissa: <http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/>

Police Service of Northern Ireland (PSNI). Ei päiväystä. Crime prevention advice re tiger kidnap. [www-dokumentti]. Police Service of Northern Ireland. [viitattu 15.4.2015]. Saatavissa: [http://www.psni.police.uk/advice\\_tiger\\_kidnap.pdf](http://www.psni.police.uk/advice_tiger_kidnap.pdf)

## **LIITTEET**

Liite 1. TIETOTURVALLISUUSLUOKITELLUN ASIAKIRJAN KANSILEHTI

Liite 2. Auditointiaineistomalli

LIITE 1 TIETOTURVALLISUUSLUOKITELLUN  
ASIAKIRJAN KANSILEHTI

**ERITTÄIN SALAINEN – YTTERST HEMLIIG  
TOP SECRET**

**KÄYTTÖOIKEUS**

Toimitusjohtaja Matti Möttönen  
Turvallisuuspäällikkö Mikko Mallikas  
Tietoturvapäällikkö Erkki Esimerkki

**OMISTAJA/LUOKITTELIJA**

Tietoturvapäällikkö Erkki Esimerkki

**LUOKITTELU VOIMASSA**

1.1.2024

**KÄYTTÖRAJOITUS**

Tämä tietoaineisto on tarkoitettu ainoastaan käyttöoikeus -kohdassa merkittyjen henkilöiden käyttöön.

Tämän aineiston luvaton käyttö on rangaistavaa Suomen rikoslain

30 Luvun 4 §, 5 §, 6 § ja  
38 Luvun 3 §, 4 § mukaisesti

**MIKÄLI LÖYSIT AINEISTON**

Mikäli olet löytänyt tämän tietoaineiston, ole hyvä ja palauta aineisto sitä avaamatta tämän kansilehden alaviitteessä mainittuun osoitteeseen, tai ota yhteyttä alaviitteestä löytyvään numeroon tai sähköpostitse.

(Tämä kansilehti on julkinen)

## LIITE 2 Auditointiaineistomalli

Yritys: \_\_\_\_\_ Osoite: \_\_\_\_\_ Y-tunnus: \_\_\_\_\_ Päivämäärä: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

<b>Yhteenveto</b>							
Kohta		Kyllä	Osittain	Ei	%	Kohtia	Yhteensä
A.5	Hallinnollinen tietoturva					/	21
A.6	Tietoturvallisuuden organisointi					/	91
A.7	Henkilöstöturvallisuus					/	75
A.8	Suojattavan omaisuuden hallinta					/	98
A.9	Pääsynhallinta					/	163
A.10	Salaus					/	45
A.11	Fyysinen turvallisuus ja ympäristön turvallisuus					/	112
A.12	Käyttöturvallisuus					/	171
A.13	Viestintäturvallisuus					/	88
A.14	Järjestelmän hankkiminen ja ylläpito					/	157
A.15	Suhteet toimittajiin					/	76
A.16	Tietoturvahäiriöiden hallinta					/	62
A.17	Liiketoiminnan jatkuvuuden hallintaan liittyviä näkökohtia					/	32
A.18	Vaativuuden mukaisuus					/	81
<b>YHTEENSÄ</b>						/	<b>1 272</b>

Tämä auditointipohja on laadittu ISO 27000:2009; 27001:2006; 27002:2005 viitekehyksessä.

Auditointijankohta \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

Auditoidijat \_\_\_\_\_

Nimen selvennys

\_\_\_\_\_

Nimen selvennys

Toimeksiantajan edustajan hyväksyntä

Nimen selvennys

\_\_\_\_\_

Nimen selvennys

\_\_\_\_\_

Nimen selvennys

Tietoturvaluksauditoinnin yhteenveto

A.5. Tietoturvapoliitikat	Osio	Kuvaus	Kyllä Osittain Ei
A.5.1.1 Tietoturvapoliitikat	Hallintakeino	<b>Ylimmällä tasolla organisaation olisi määriteltävä ”tietoturvapoliittikka”, jonka johto hyväksyy ja jossa määritellään organisaation lähestymistapa tietoturvatavoitteiden hallintaan.</b>	
	Vaatimukset	Tietoturvapoliittikkojen olisi katettava vaatimukset, jotka ovat peräisin <ul style="list-style-type: none"> <li>a) liiketoimintastrategiasta</li> <li>b) asetuksista, laeista ja sopimuksista</li> <li>c) nykyisestä ja ennustetusta tietoturvaohjelmaympäristöstä.</li> </ul>	
	Lausumat	Tietoturvapoliittikan olisi sisällettävä myös lausumat, joissa <ul style="list-style-type: none"> <li>a) määritellään tietoturvallisuus, tietoturvatavoitteet ja -periaatteet, jotka ohjaavat kaikkea tietoturvallisuuteen liittyvää toimintaa</li> <li>b) jaetaan määritellyille rooleille yleiset ja kohdistetut vastuut tietoturvallisuuden hallinnasta</li> <li>c) määritellään prosessit, joilla käsitellään poikkeamia ja poikkeuksia.</li> </ul>	
	Alemman tason politiikat	Alemmalla tasolla tietoturvapoliittikkaa olisi tuettava asiakohteisilla politiikoilla, jotka tukevat laajemmin tietoturvallisuuden hallintakeinojen toteuttamista ja jotka ovat yleensä rakenteeltaan sellaisia, että ne vastaavat organisaation tiettyjen kohderyhmien tarpeisiin tai kattavat tietyt aiheet. <ul style="list-style-type: none"> <li>a) pääsynhallinta (ks. kohta 9)</li> <li>b) tietojen luokittelu (ja käsittely) (ks. kohta 8.2)</li> <li>c) fyysinen turvallisuus ja ympäristön turvallisuus (ks. kohta 11)</li> </ul>	

Auditointipohja