SAVONIA

OPINNÄYTETYÖ - **YLEMPI AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

TIETOTURVALLISUUDEN HALLINTAMALLIN KEHITTÄMINEN

TEKIJÄ/T: Janne Pollari

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Teknologiaosaamisen johtaminen	
Työn tekijä(t) Janne Pollari	
Työn nimi Tietoturvallisuuden hallintamallin kehittäminen	
Päiväys 11.6.2017	Sivumäärä/Liitteet 58/78
Ohjaaja(t) lehtori Pekka Granroth	
Toimeksiantaja/Yhteistyökumppani(t) Savon Voima Oyj	

Tiivistelmä

Tämä opinnäytetyön tavoitteena selvittää millainen on organisaation hyvä tietoturvallisuuden hallintamalli. Tarkoituksena on tunnistaa mistä hyvä hallintomalli koostuu ja mitkä ovat keskeisiä tekijöitä hallintomallin kehittämisessä ja millainen hallintamallin rakenne tulisi olla. Työssä tutkitaan, onko ISO/IEC 27000 standardiperhe hyvä viitekehys tietoturvallisuuden hallintamallin kehittämisen tueksi kohde organisaatiolle.

Työ aloitettiin tutkimalla ISO/IEC27000 standardiperheen dokumentaatiota, sekä IEC/ISO27001 standardin vaatimuksia. Kohde organisaatiolle tehtiin myös tietoturvallisuuden nykytilan selvittämiseksi ISO27001 nykytila-analyysi. Analyysin lisäksi organisaatiossa toteutettiin itsearviointityökalua hyödyntäen kysely tietoturvallisuuden hallinnan nykytilan selvittämiseksi. Näillä tutkimuksilla pystyttiin tunnistamaan ne keskeiset kehitettävät asiat, joilla tietoturvallisuuden tasoa lähdetään organisaatiossa nostamaan.

Opinnäytetyön lopputuloksena syntyy hallintamallin runko, joka voidaan toteuttaa erillisillä pienemmillä projekteilla. Tietoturvallisuuden hallintajärjestelmän kehittäminen vaatii opinnäytetyön kohde organisaatiolta useamman vuoden työn. Tämän opinnäytetyön tavoitteena oli tunnistaa ne vaiheet, joita organisaation kannattaa toteuttaa tavoitteisiin pääsemiseksi. Lopputuloksena organisaatiolle syntyi kattava käsitys toimenpiteistä, joilla organisaatio pystyy parantamaan omaa tietoturvallisuuden maturiteettia. Organisaatiolle tehtiin myös kehityssuunnitelma, jonka pohjalta se pystyy toteuttamaan tietoturvallisuuden kehitysohjelman.

Avainsanat
ISO/IEC 27001, tietoturvallisuuden hallintamalli, riskienhallinta, hallintakeino, NIS-direktiivi

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Janne Pollari			
Title of Thesis Security management governance development			
Date	11.6.2017	Pages/Appendices	58/78
Supervisor(s) Mr. Pekka Granroth, Lecturer			
Client Organisation /Partners Savon Voima Ltd			

Abstract

The purpose of this thesis was to clarify what is a good management model for information security for an organization. The aims were to recognize what are the components of a good management mode, what are central factors in development of a management model, and how the structure of a management model should be. This work investigated whether ISO/IEC 27000 standard family is a good frame to support development of information security management model for target organisation.

The work was initiated by investigating ISO/IEC27000 standard family documentation and IEC/ISO27001 standard requirements. ISO27001 current state analysis was carried out for the target organisation to determine the present situation of information security. In addition to analysis, questionnaire using self-assessment tool was conducted in the organisation to define the current state of information security management. Using these investigations, it was possible to recognize the central issues requiring development and these topics will be used to improve the level of the information security in the organisation.

As a result of this project, management model frame was developed and it can be implemented with separate smaller projects. The development of information security management model will require several years of work from the target organisation. The aim of this thesis was to identify the steps that the organisation should carry out to reach the goals. As a result, the organisation acquired comprehensive understanding of the actions that can used to improve the maturity of their information security. Additionally, a development plan was created for the organisation to implement the information security development program.

Keywords
ISO/IEC27001, Information security governance, information security management system, risk management, security controls

ESIPUHE

Haluan kiittää Savon Voima Oyj:tä mielenkiintoisesta opinnäytetyön aiheesta. Aihe on erittäin ajankohtainen ja oli mielekästä tutkia aihetta, joka auttaa kehittämään organisaation tietoturvallisuuden hallintaa.

Kiitokset haluan antaa myös ohjaavalle opettajelle lehtori Pekka Granrothille, joka antoi koko projektin ajan hyviä näkökulmia mitä aiheita opinnäytetyössä kannattaa käsitellä.

Lopuksi tahdon kiittää myös vaimoani Karoliina Pollaria tuesta ja kannustuksesta opinnäytetyöprosessin aikana.

Kuopiossa 5.6.2017

Janne Pollari

LYHENTEET JA TERMIT

Baseline	Perustaso jota voidaan käyttää vertailuarvona mitattaessa.
BCP	Business Continuity Plan, Liiketoiminnan jatkuvuussuunnitelma. Suunnitelma jolla määritellään toimenpiteet, joilla liiketoimintaprosessit palautetaan normaaliin tilaan keskeytyksen jälkeen.
BIA	Business Impact Analysis, Liiketoiminnan vaikuttavuusanalyysi. Jatkuvuuden hallintaan liittyvä toiminto, jolla tunnistetaan ydinliiketoimintojen riippuvuudet.
CIA	Confidentiality, Integrity, Availability. Luottamuksellisuus, eheys, saatavuus.
CMMI	Capability Maturity Model Integration. Prosessien kehittämisen lähestymistapa, jonka on kehittänyt Software Engineering –instituutti.
COBIT	Control Objectives for Information and releated Technology. Tiedon ja siihen liittyvän teknologian kontrollitavoitteet.
Governance	Organisaation hallintotapa.
CSIRT	Computer Security Incident Response Team. Kansallinen organisaatio joka huolehtii tietoturvapoikkeamien käsittelemisestä.
EFQM	European Foundation for Quality Management. Organisaation toiminnan ja laadun arvioimismalli.
ENISA	European Union Agency for Network and Information Security. Euroopan unionin verkko- ja tietoturvavirasto.
ERM	Enterprise Risk Management. Riskienhallintajärjestelmä.
ICT	Information and Communications Technology. Tieto- ja viestintäteknologia.
IEC	International Electrotechnical Commission. Kansainvälinen sähköalan standardisoimisjärjestö.
ISMS	Information Management System. Tietoturvallisuuden hallintajärjestelmä.
ISO	International Organization for Standardization. Kansainvälinen standardisoimisjärjestö.

ITIL	Joukko IT-palveluhallinnan parhaita käytäntöjä.
KATAKRI	Tietoturvallisuuden auditointityökalu viranomaisille.
LVM	Liikenne- ja viestintäministeriö.
NIS	Directive on security of network and informatiom system. EU:n Verkko- ja tietoturvadirektiivi.
NIST	National Institute of Standards and Technology. Kansainvälinen standardisoimisjärjestö.
OECD	Organisation for Economic Co-operation and Development. Taloudellisen yhteistyön ja kehityksen järjestö.
PDCA	Plan, Do, Check, Act. Suunnittele, tee, tarkista, korjaa ongelmien ratkaisumalli.
SOA	Statement of Applicability. Dokumentti jossa kuvataan ISO/IEC27002 – tietoturvakontrollit.

SISÄLTÖ

1 JOHDANTO

Tietojärjestelmien ja niitä yhdistävien tietoverkkojen merkitys organisaation toiminnalle on tänä päivänä perusedellytys. Organisaatiot ja niiden muodostamat yhteenliittymät ja ekosysteemit tarvitsevat toimiakseen kattavan digitaalisen toimintaympäristön, joka ei rajoitu enää pelkästään organisaation sisälle. Digitaalinen toimintaympäristö on tänä päivänä globaali järjestelmien, tietojärjestelmien ja tietoverkkojen verkosto, joka toimii maailmalaajuisesti. Tätä digitaalista toimintaympäristöä voi olla yksittäisenä organisaationa haastavaa edes määrittää ja sen hallinta ei ole enää kokonaan organisaation omissa käsissä. Voimakas riippuvuus digitaalisesta toimintaympäristöstä on aiheuttanut sen, että organisaatiot ja yhteiskunta ovat entistä haavoittuvaisempi, koska kokonaisuutta on entistä hankalampi hallita ja valvoa. Tästä syystä organisaatioiden on entistä enemmän panostettava tietoturvallisuuden hallintaan ja kehitettävä keinoja joilla se pystyy turvaamaan sen liiketoiminnoille elintärkeät toiminnot.

Tietoturvallisuuden hallinta tulee ulottu koko organisaation laajuudelle, jotta se on riittävän tehokas torjumaan alati lisääntyviä uhkia. Mahdollisten toteutuneitten riskien jälkeen on kyettävä palautumaan mahdollisimman tehokkaasti ja nopeasti normaaliin toimintatilaan kärsimättä liian suuria taloudellisia vahinkoja. Tietoturvallisuuden hallinta ei ole pelkkää tekniikkaa tai hallinnollista toimintaa. Se on ennen kaikkea näiden yhdistämistä ja niiden tuomista osaksi organisaation normaalia toimintaa. Tietoturvallisuuden tulee olla osa organisaation liiketoimintaprosesseja, jolloin tietoturvallisuudesta tulee läpinäkyvää ja helpommin ymmärrettävää toimintaa.

Kappaleessa kaksi esitellään opinnäytetyön sisältöä ja aiheen valintaa, sekä esitellään kohdeorganisaatio Savon Voima. Tarkoituksena on kuvata, mitkä tekijät vaikuttivat aiheen valintaan. Kolmannessa kappaleessa esitellään lyhyesti tutkimukseen käytettävät tutkimusmenetelmät, aiheen rajaaminen sopivan kokoiseen kokonaisuuteen ja kuinka opinnäytetyön on tarkoitus edetä ja mitä aineistoja tiedon hankintaan on käytetty.

Tietoturvallisuuden tavoitteet ja velvoitteet esitetään lyhyesti kohde organisaation näkökulmasta tämän päivä tietoturvallisuus vaatimuksia silmällä pitäen. Kappaleessa viisi esitellään mikä on tietotuvallisuuden hallintamalli ja mistä osista hyvä hallintamalli rakentuu. Hallintamallissa on tärkeää, että se on hyvin organisoitu ja toimintamallit ovat yhtenäisiä koko organisaatiossa ja ne on kattavasti kuvattu ja dokumentoitu. Kehittäminen perustuu jatkuvaan riskienhallintaan, jonka pohjalta valitaan organisaatiolle sopivimmat hallintakeinot, joilla se pyrkii näitä riskejä hallitsemaan riskienhallintapolitiikan mukaisesti. Kyvykkyyden eli maturiteetin parantamiseksi organisaation tulee myös mitata tietoturvallisuuden johtamisen tasoa, tietoturvaprosessien toimintaa ja kerättävä kattavista mittaustietoa riskienhallinnan päätöksen teon tueksi. Tietoturvallisuuteen kuuluu myös liiketoimintojen jatkuvuuden turvaaminen ja mahdollisimman tehokkaan palautumisen suunnitteleminen, jos riski on päässyt jo toteutumaan.

Tietoturvallisuuden hallintaan liittyvät prosessit on esitelty kappaleessa kuusi. Tietoturvallisuuden hallintaa liittyviä prosesseja ovat tietoturvallisuuden jatkuvan kehittämisen prosessi,

tietoturvallisuuden jatkuvien palveluiden hallinnan prosessi ja tietoturvariskienhallinnan prosessi. Riskienhallinta on keskeinen osa-alue tietoturvallisuuden hallinnassa ja kehittämisessä ja tästä syystä sitä on kuvattu muita prosesseja laajemmin. Riskienhallinnan tuloksena valittavat ISO27002 standardin mukaiset hallintakeinot on esitelty kappaleessa seitsemän.

Tietoturvallisuuden hallintaan liittyvä organisaatio ja siihen liittyvät vastuut on esitelty lyhyesti kappaleessa kahdeksan. Tietoturvallisuuden maturiteetin arvioimista ja tietoturvallisuuden mittaamista on esitelty kappaleessa yhdeksän. Tietoturvallisuuden mittareita voidaan määritellä vasta kun organisaatio on toteuttanut tietoturvallisuuden kehitysohjelman. Alussa organisaatio pystyy mittaamaan omaa kyvykkyyttä eli maturiteettia vain vertaamalla olemassa olevia hallintakeinoja standardeissa suositeltuihin keinoihin. Organisaatio pystyy ainoastaan toteamaan mitkä tietoturvallisuuteen liittyvät toiminnot sillä on jo kunnossa ja mitä toimintoja sen tulisi lisätä ja kehittää.

Opinnäytetyön työn tuloksia ja pohdintaa on esitelty kahdessa viimeisessä kappaleessa. Pohdinnassa on myös tarkoitus ottaa kantaa, kuinka kohde organisaation kannattaisi lähteä omaa tietoturvallisuuden hallintaa kehittämään.

2 OPINNÄYTETYÖN TAVOITTEET JA NÄKÖKULMA

Opinnäytetyön tavoitteena on kehittää Savon Voima Oyj:lle tietoturvallisuuden hallintamalli, jonka pohjalta voidaan tulevaisuudessa kehittää tietoturvallisuuden hallintajärjestelmä (ISMS, Information Security Management System).

Tietoturvallisuuden hallintamallin kehittäminen aloitetaan tekemällä ISO27001 standardiin pohjautuva yrityksen tietoturvallisuuden nykytila-analyysi. Analyysin tarkoitus on tunnistaa tietotuvallisuuden nykytaso yrityksessä peilaten ISO27001 vaatimuksiin ja löytää ne keskeiset kehityskohteet joita parantamalla organisaation tietoturvallisuuden tasoa voidaan nostaa.

Hallintamalli rakentuu valituista hallintakeinoista, joiden avulla muodostetaan tietoturvan hallintamalli, joka vastaa ISO27001 vaatimuksia.

2.1 Taustaa aiheen valintaan

Savon Voima Oyj toimii Suomen huoltovarmuuden kannalta kriittisellä toimialalla. Energian tuotanto, siirto ja jakeluverkot katsotaan kuuluvan kriittiseen infrastruktuuriin yhteiskunnan toimikyvyn näkökulmasta. Häiriöt energian jakelussa ja tuotannossa vaikuttavat laajalti nykyaikaisen tietoyhteiskunnan toimintaan hyvin nopeassa ajassa. Tietoyhteiskunta on entistä riippuvaisempi energiasta ja sen saamisesta. Toisaalta energian tuottaminen ja jakelu ovat entistä riippuvaisempia tieto- ja viestijärjestelmistä.

Maailmalla vallitseva epävarmuus ja uuden tyyppiset uhkakuvat ovat aiheuttaneet sen, että yhteiskunnan kannalta kriittisten toimijoiden on varauduttava entistä paremmin myös kyberuhkiin ja huolehdittava omasta kyberturvallisuudesta. Energia yhtiönä myös Savon Voima haluaa huolehtia kyberturvallisuuden parantamisesta, jossa yhtenä keskeisenä osa-alueena tietoturvallisuus on. Tietointensiivisyys on lisääntynyt yhteiskunnassa merkittävästi. Erilaiset tieto- ja viestintäjärjestelmät integroituvat toisiinsa muodostaen entistä monimutkaisempia kokonaisuuksia toiminnan turvaamisen kannalta.

Sidosryhmät ovat entistä riippuvaisempia toisistaan ja eri organisaatiot tekevät yhteistyö globaalisti verkottuneina. Näin ollen organisaatioiden on yhdessä huolehdittava kyberturvallisuuden toteutumisesta ja huolehdittava riittävästä yhteistyöstä myös yksityisten organisaatioiden välillä. Kaikkien sidosryhmien tulee kantaa vastuu digitaalisen toimintaympäristön turvallisuudesta ja huomioida myös toisiin osapuoliin vaikuttavat tekijät riskienhallinnassa ja päätöksen teossa. (Valtionvarainministeriö 2016, 13-14).

Huoltovarmuuskeskuksen energia-alan kyberturvallisuuden tilannekuvan perusteella Suomessa energiasektorin tietoturvan painopiste on ollut tiedon suojaamisessa teknisin menetelmin. Raportissa todetaan, että tekninen suojaustaso on pääosin kohtuullisella tasolla. Suurimmat ongelmat nähdään olevan nimenomaan tietoturvan hallinnollisella puolella. Organisaatioilla ei ole formaalia tietoturvan hallintamallia (Immonen 2015, 5). Organisaation tietotuvan hallintaan tarvitaan teknisen suojaamisen lisäksi hallinnollisia keinoja, joita ilman organisaatio ei voi saavuttaa riittävää kypsyyttä ja kyvykkyyttä kyberturvallisuuden toteuttamiseen. Savon Voimalla toteutettiin ISO27001 standardiin peilautuva nykytila-analyysi. Analyysin tuloksia perusteella, myös Savon Voimalla tunnistettiin keskeisiä kehityskohteita tietoturvan hallinnollisella puolella. Kyberturvallisuus tilannekuvaraportin mukaan suurin kehitys saadaan kehittämällä yrityksen tietoturvan hallinnollista puolta lisäämällä henkilöstön koulutuksia ja tietoisuutta, sekä päivittämällä yritysten tietoturvapolitiikat, toimintamallit ja ohjeistukset (Immonen 2015, 5).

Kansallinen kyberturvallisuus luo pohjan Suomen yritysten menestymiselle. Kansallinen kyberturvallisuus toteutuu vain eri organisaatioiden yhteistyön tuloksena. (Valtiovarainministeriö 2013, 1). Kyberuhkat ovat erilaisten entistä ammattimaisten ja jopa valtiollisten tahojen toteuttamia, joilta suojautuminen vaatii entistä enemmän panostamista, osaamista ja kybertoimintaympäristön toimijoiden välistä yhteistyötä. Varautuminen kybertoimintaympäristön uhkiin vaatii toimijoiden välisen yhteistyön tiivistämistä ja yhteisen tilannekuvan luomista. (Valtiovarainministeriö 2013, 4). Euroopan unionin asettaman verkko- ja tietoturvadirektiivin tärkein tehtävä on huolehtia Euroopan laajuisen yhteistyön lisäämisestä tietoturvallisuuden osalta. Sen tarkoituksena on muodostaa toimijoiden verkosto, joka yhdessä ylläpitää tietoturvallisuuden tilannekuvaa Euroopan laajuisesti. Direktiivi edellyttää myös riittävän tietoturvatason ylläpitämistä myös yksityisissä organisaatioissa, jotka toimivat huoltovarmuuden kannalta kriittisillä toimialoilla.

Savon Voimassa ollaan käynnistetty tietoturvallisuuden kehitysohjelma, jonka tavoitteena on luoda yhtiölle toimiva ja tehokas tietoturvaorganisaatio ja kehittää sen toiminta vastaamaan nykypäivän tarpeita. On myös odotettavissa, että huoltovarmuuden kannalta kriittisille yhtiöille on tulossa uusia vaatimuksia, joilla pyritään vastaamaan kyberturvallisuuden toteutumiseen niin kansallisella kuin kansainvälisellä tasolla. Kynnys vastata kiristyviin vaatimuksiin on pienempi, jos toimintaa lähdetään jo nyt kehittämään ISO27001 viitekehyksen vaatimusten mukaiseksi.

Savon Voimalla on tarkoitus kehittää uusia palveluita ja tehdä uutta liiketoimintaa hyödyntämällä esineiden internetiä IoT:tä. Tämä asettaa myös uusia velvollisuuksia huolehtia tietoturvan ja kyberturvallisuuden toteutumisesta näissä palveluissa. IoT:n myötä yhteiskunta on entistä haavoittuvampi uusia uhkia vastaan ja mediasta saamme lukea viikoittain uusia artikkeleita, kuinka ihmisiä on kiristetty maksamaan lunnaita tai tekemällä massiivisia palvelunestohyökkäyksiä IoT laitteiden avulla. Palvelun tuottajilla on vastuu huolehtia palveluiden turvallisuudesta. Savon Voiman arvoissa todetaan, että meihin voidaan luottaa ja pidämme kiinni lupauksistamme ja teemme asiat laadukkaasti. Savon Voima tarjoaa asiakkailleen tulevaisuudessa enemmän digitaalisia palveluita, joiden perus edellytys on, että tietoturva on kunnossa. Tulevaisuudessa palveluntuottajilla on suuri vastuu varsinkin IoT tekniikkaan pohjautuvissa palveluissa huolehtia tietoturvasta. Tällä hetkellä suurimmassa osasta IoT laitteita tietoturva on hoidettu erittäin huonosti ja tämä voi olla myös merkittävä riski palveluita tuottavalle yritykselle.

Verkko- ja tietoturvadirektiivi (NISD) määrittelee, että kansallisella tasolla pitää olla yksi tai useampi toimivaltainen kansallisesta turvallisuudesta vastaava viranomainen. Viranomaisen lisäksi kansallisella tasolla tulee olla yksi keskitetty yhteyspiste, joka huolehtii viranomaisten rajat ylittävän yhteyden pidon onnistumisesta. Tähän yhteyspisteisiin ei kuitenkaan tehdä ilmoituksia poikkeamista, ellei se toimi CSIRT-toimijan roolissa. CSIRT-toimijoita tulee olla yksi tai useampi. CSIRT-toimija huolehtii poikkeamien seuraamisesta kansallisella taholla, ennakkovaroitusten ja tiedotusten antamisesta sidosryhmille, poikkeamiin reagoiminen ja analysoiminen ja kansainväliseen CSIRT-verkostoon osallistuminen. CSIRT-toimija pitää yhteystyösuhteita yllä myös yksityiseen sektoriin edistäen yhtenäisten standardoitujen toimintamallien omaksumista. Verkko- ja tietoturvadirektiivin alaisilla palveluntarjoajilla on velvollisuus ilmoittaa poikkeamista viiveettä CSIRT-toimijalle. Savon Voima kuuluu direktiivin määriteltyihin keskeisiin palveluntarjoajiin energia-toimialalla ja tulee näin ollen olemaan vaatimusten piirissä. (LVM 2017, 6-9).

2.2 Savon Voiman esittely

Savon Voima on pitkä perinteet omaava energia-alan yritys, joka perustettiin 1947 yhdistämällä useita pienempiä sähkölaitoksia. Konsernin liiketoiminta koostuu sähkön ja lämmön tuotannosta, myynnistä ja jakelusta. Sen lisäksi Savon Voima tarjoaa asiakkailleen erilaisia energia-alan asiantuntija palveluja. Savon Voima kuluu Suomen suurimpien energiapalveluja myyvien yritysten joukkoon noin 186 miljoonan euron liikevaihdolla. Konsernissa työskentelee noin 180 omaa

henkilöstöä. Sen lisäksi Savon Voima on alueella merkittävä työllistäjä työllistämällä vuosittain noin 300 henkilötyövuotta kumppaniyritysten kautta. (Savon Voima 2016, Konserni).

Vuositasolla investoimalla kymmeniä miljoonia euroja Savon Voima on merkittävä tekijä alueen hyvinvoinnin tekemisessä. Vuonna 2015 brutto investoinnit olivat yli 53 miljoonaa euroa. (Savon Voima 2016, Konserni).

Savon Voima konserniin kuuluvat emoyhtiö Savon Voima Oyj, Savon Voima Verkko Oy ja Savon Voima Salkunhallinta Oy. Savon Voima Oyj:n omistaa Savon Energiaholding Oy, jonka omistajina ovat alueen 21 kuntaa. (Savon Voima 2016, Omistajat).

Savon Voiman kulmakivenä on tuottaa asiakkailleen luotettavia energiapalveluita. Tavoitteena on turvata energiansaannin luotettavuus ja sitä kautta olla tukemassa koko yhteiskunnan toimivuutta. Meille tärkeitä ovat asiakkaat ja haluamme olla helposti lähestyttävä, avoin, kestävää jatkuvaa kehitystä ja energiapalveluita tarjoava yritys. (Savon Voima 2016, Toimintaperiaatteet).

Savon Voima on arvonsa ja vastuunsa tunteva yritys, jonka kantaa vastuunsa ympäristöstä ja työturvallisuudesta. Tavoitteena on, ettei tapahdu yhtään työtapaturmaa eikä ympäristövahinkoa. Savon Voima on myös merkittävä tekijä kehittäessä yhteiskunnan kannalta tärkeää energiatehokkuutta. Tavoitteisiin pääsemiseksi tehostamme omaan energiankäyttöämme investoimalla uusiin teknologioihin ja neuvomme asiakkaitamme, kuinka he voivat olla energiatehokkaampia tarjoamalla erilaisia energiankäytön neuvonta ja seurantapalveluita. (Savon Voima 2016, Ympäristö ja turvallisuus).

3 OPINNÄYTETYÖN TUTKIMUSMENETELMÄT

Opinnäytetyössä tutkitaan aihetta, jossa pyritään muuttamaan yrityksen vallitsevia tietoturvakäytäntöjä. Tällöin kysymyksessä on toimintatutkimus, jossa etsitään ratkaisua ammatilliseen ongelmaan. Tutkimuksen aiheen valintaan vaikuttaa yritykselle tehtävä tietoturvallisuuden nykytila-analyysi, johon osallistui eri osa-alueiden asiantuntijoita. (Saaranen-Kauppinen & Puusniekka 2006, 41).

Opinnäytetyössä hyödynnetään myös kvalitatiivisia eli laadullisia menetelmiä, koska tutkiminen perustuu aiemmin aiheesta tehtyihin aineistoihin, teorioihin ja julkaistuihin viitekehyksiin, joita täydennetään tutkijan omalla päättelyllä ja havainnoilla. Tutkimus on aineistolähtöinen, jos teoreettista viitekehystä verrataan olemassa oleviin toimintamalleihin ja käytäntöihin. (Saaranen-Kauppinen & Puustniekka 2006, 5-7).

Opinnäytetyössä on myös määrällisiä elementtejä, koska tietoturvallisuuden itsearviointityökalun tulokset pisteytetään ja arvioidaan painoarvon mukaan.

Tutkimuksessa käytetään eri tutkimusotteita rinnakkain jolloin tutkimuksellinen ja toiminnallinen menettely yhdistyvät. Tällaista rinnakkaista tutkimusotetta voidaan kutsua triangulaatioksi. (Saaranen-Kauppinen & Puustniekka 2006, 41).

Tietoturvallisuuden nykytila yrityksessä selvitetään haastattelemalla yrityksen eri osa-alueista vastaavia ihmisiä ja asiantuntijoita. Nykytila-analyysi pohjautuu ISO27001 viitekehyksen vaatimuksiin ja noudattaa viitekehyksen rakennetta. Saatujen vastausten perusteella muodostetaan käsitys, millainen nykytila on ja mitä asioita tulisi kehittää.

Määrällinen tutkimusmenetelmä on menetelmä, joka antaa tietoa mitattavien muuttujien välisistä eroista ja suhteista. Määrällisen tutkimusmenetelmän avulla saadaan vastaus kysymykseen kuinka paljon tai miten usein. Määrällinen tutkimus on objektiivista eli tutkija ei vaikuta tutkimustulokseen. Määrällisessä tutkimuksessa tietoa tarkastellaan numeerisesti. Määrällisen tutkimuksen tulokset voidaan esittää tunnuslukuina. (Vilkka 2007, 13-14.)

Laadulliset tutkimukset muodostuvat empiirisistä aineistoista, tutkijan omasta päättelystä ja ajattelusta sekä tekstimuotoisista aineistoista (Saaranen-Kauppinen ym. 2009, 5). Laadullisen tutkimuksen pyrkimyksenä on saada kokonaisvaltaisesti empiirisesti tietoa siten, että myös laatua ja yksityiskohtia luonnehtivat tiedot tulevat esiin (Niskanen 1994, 140). Laadullisessa tutkimuksessa johtopäätökset voidaan tehdä ilman tilastomatemaattisia keinoja (Niskanen 1994, 140). Tavoitteena on saada vastauksia kysymyksiin miksi, miten ja millainen (Heikkilä 2004, 16-17).

3.1 opinnäytetyön aiheen rajaaminen

Opinnäytetyön aihe rajataan tietoturvallisuuden hallintamallin kehittämiseen yrityksen käyttöön. Tietoturvallisuuden hallintajärjestelmän (ISMS, Information Security Management System) toteuttaminen vaatii yritykseltä usean vuoden työn ja paljon eri resursseja. Näin ollen hallintajärjestelmän toteuttamien rajataan opinnäytetyön aiheen ulkopuolelle.

Nykytila-analyysin perusteella tunnistetaan ne keskeisimmät kehitystarpeet, joita yrityksen tietoturvallisuuden tason nostamiseksi vaaditaan. Hallintamallin hallintakeinoiksi valitaan parhaat hallintamenetelmät, joilla pystytään NIS –direktiivin ja ISO27001 vaatimuksiin vastaamaan.

NIS direktiivi ei varsinaisesti määritä viitekehystä, jonka vaatimuksiin yrityksen toiminnan tulisi perustua. Direktiivi määrittelee erilaisia velvoitteita ja vastuita, jotka yrityksen tulee täyttää, jos se kuuluu toimialalle, jonka tulee täyttää nämä vaatimukset. Tutkimuksessa on tarkoitus selvittää, minkälaisella hallintamallilla yritys täyttää nämä tulevat vaatimukset hyödytän yleisesti laajasti käytettyä ISO27001 viitekehystä.

NIS direktiivi on hyväksytty elokuussa 2016 ja sen toteuttaminen tehdään kansallisella tasolla implementoimalla direktiivin vaatimukset kansallisiin lakeihin 9.5.2018 mennessä.

Energiatoimia-ala on direktiivin näkökulmasta yksi niistä toimialoista, joilla on keskeinen rooli kansallisen ja EU laajuisen kyberturvallisuuden kyvykkyyden rakentamisessa. Tietoturvallisuuden toiminnan kehittäminen vaatii aikaa, resursseja ja ymmärryksen lisäämistä on yrityksen kannalta tärkeää aloittaa toiminnan kehittäminen vaatimusten mukaiselle tasolle hyvissä ajoin.

3.2 Aloittaminen

Työ aloitetaan kartoittamalla yrityksen tietoturvallisuuden nykytaso tekemällä Energiateollisuuden Ry:n tarjoama itsearviointityökalu TIKKA2016, joka perustuu ISO27001 ja KATAKRI III vaatimuksiin. Arviointityökalu toimii kyselytutkimuksena, jonka tehdään yrityksen avainhenkilöille, jotka vastaavat eri osa-aluista yrityksessä. Itsearviointi tehdään kyselylomakkeella ja tulokset pisteytetään vaikuttavuuden mukaan. Tulosten perusteella voidaan arvioida yrityksen tietoturvallisuuden kypsyyttä (Valtiovarainministeriö 2006, 34-37).

Tämän jälkeen yritykselle tehdään ISO27001 standardin vaatimuksiin pohjautuva tietoturvan nykytila-analyysi, jonka tarkoituksena on selvittää keskeiset kehitettävät kohteet yrityksen tietoturvallisuuden parantamiseksi.

Tutkimustuloksia vertaamalla on tarkoitus löytää ne keskeiset hallintamenetelmät ja keinot joita tulisi yrityksen toiminnassa kehittää. Tarkoitus on myös varmistaa, että yrityksen kyberturvallisuuden tasoa lähdetään nostamaan NIS direktiivin vaatimusten mukaiselle tasolle. Valitaan sopivimmat ISO27001 viitekehyksen mukaiset hallintakeinot, joiden pohjalta muodostetaan yrityksen tietoturvallisuuden hallintamalli.

Itsearviointityökalun ja ISO27001 nykytila-analyysin varsinaisia tuloksia ei voida esittää opinnäytetyön liitteenä tietoturvasyistä. Toteutetut raportit esitetään opinnäytetyötä arvioivalle opettajalle opinnäytetyön arvioinnin tueksi.

3.3 Ymmärryksen luominen

Nykytilan arvioimisen jälkeen on tarkoitus luoda kuva, millainen kypsyys yrityksellä kyberturvallisuuden osalta on ja kasvattaa tietämystä millaisilla toimenpiteillä yritys kykenee kypsyyttä ja kyvykkyyttä parantamaan. Kokonaiskuva pyritään muodostamaan tutustumalla keskeisimpiin tieturvastandardeihin ja niiden vaatimuksiin.

Tarkoitus on muodostaa tietoturvasta vastaaville ihmiselle käsitys, millaisia vaatimuksia tietoturvallisuuden toteutumiselle on ja millaisella hallintamallilla toimintaa voidaan kehittää vastaamaan noita vaatimuksia. Nykytila-analyysin tulokset puretaan yhteisessä purkutilaisuudessa kokonaiskuvan muodostamiseksi.

Nykytila-analyysin tulokset esitellään myös yrityksen johdolle erillisessä tilaisuudessa. Näin yrityksen johdon tietoisuutta nykytilasta pyritään vahvistamaan ja esittämään ne keskeisimmät kehitystoimenpiteet, joilla tietoturvallisuuden tasoa yrityksessä lähdetään nostamaan. Tietoturvallisuuden toteutuminen vaatii johdon ymmärrystä ja sitoutumista. Tietoturvallisuuden tavoitteet pitäisi tulla yrityksen strategiasta.

3.4 Ratkaisujen suunnittelu ja toimenpiteistä sopiminen

Tietoturvan nykytila-analyysin pohjalta luodaan yritykselle tietoturvan kehityssuunnitelma. Kehityssuunnitelman avulla on tarkoitus aikatauluttaa ne keskeiset kehitettävät kohteet, joita analyysin perusteella pystyttiin tunnistamaan.

Seuraavassa vaiheessa tunnistetaan tietoturvariskit ja käynnistetään tietoturvariskien arviointi. Tietoturvariskien hallinta toteutetaan osana yrityksen kokonaisriskien hallintaa. Riskit kuvataan ja arvioidaan yrityksen riskienhallintajärjestelmässä (ERM) omana kokonaisuutenaan. Riskienarvioinnin jälkeen yritykselle tulisi määritellä, tietoturvapolitiikka ja jatkuvuus- ja toipumissuunnitelmat. Tietoturvanhallintajärjestelmä kostuu useista ohjeistuksista, dokumenteista, tietoturvasuunnitelmasta, jotka kuvaavat ja määrittelevät tarkasti yrityksen käytössä olevat tietoturvaratkaisut ja hallintakeinot.

Kehittämistarpeille määritellään keskeiset hallintakeinot, joilla niiden toteutuminen varmistetaan. Jokaiselle tunnistetulle kehittämisen osa-alueelle määritellään vastuullinen henkilö, jonka vastuulla kyseisen alueen kehittäminen ja seuranta ovat.

Riskiarvioiden perusteella määritellään yritykselle tietoturvapolitiikka, jonka tehtävänä on kuvata ne toimenpiteet, joilla tietoturvariskejä lähdetään torjumaan tai minimoimaan. Tietoturvapolitiikka määrittää yrityksen yleiset tietoturvakäytänteet ja tavoitteet. Organisaation hallitus hyväksyy politiikan ennen sen täytäntöönpanoa.

Kun tarvittavat hallintakeinot on määritelty ja vastuut jaettu, määritellään organisaatiolle tietoturvallisuuden vuosikello, johon sijoitetaan kaikki vuosittaiset hallinnolliset kontrollit, joilla yrityksen tietoturvallisuutta hallitaan ja kontrolloidaan. Näin varmistetaan, että yrityksellä on jatkuva kontrolli tietoturvan seurantaan.

Näiden vaiheiden jälkeen on tarkoitus kuvata tietoturvallisuuden hallintamalli, jossa on määritelty, hallintakeinot, resurssit ja mittari joilla tietoturvallisuuden kehittymistä seurataan.

3.5 Keskeinen kirjallisuus

Keskeinen aineisto joita opinnäytetyössä tullaan käyttämään, on yleiset tietoturva standardit, valtionvarainministeriön VAHTI ohjeistukset, sekä erilaiset tietoturvallisuustutkimusten tulokset ja julkaisut. Lisäksi tukevana aineistona käytetään kirjallisuutta tutkimusmenetelmien valitsemisesta ja soveltamisesta tutkimukseen.

4 TIETOTURVALLISUUDEN HALLINAN KESKEISET TAVOITTEET JA VELVOITTEET

Tietoturvallisuuden hallintamallin yhtenä tavoitteena on tunnistaa organisaation digitaalinen toimintaympäristö, jossa se toimii. Tavoitteena on myös turvata organisaation taloudellisen toiminnan jatkuvuus. Organisaation toiminta on monesti erittäin riippuvainen digitaalisen ympäristöstä. Harvat organisaation toiminnot ja prosessit pystyvät enää toimimaan ilman digitaalista toimintaympäristöä tai toiminta on tehotonta tai taloudellisesti kannattamatonta. Organisaatioiden ja yhteistyöverkostojen entistä suurempi riippuvuus digitaalisesta toimintaympäristöstä aiheuttaa myös sen, että organisaatioiden on kiinnitettävä entistä enemmän huomioita toimintaympäristön toimivuuden varmistamiseen ja huolehtimalla organisaation kyberturvallisuudesta.

Kyberturvallisuuden keskeinen tavoite on tunnistaa digitaalista toimintaympäristöä uhkaavat kyberturvallisuus riskit ja pienentää niitä hyväksyttävälle tasolle. Organisaation tulee määrittää riskienhallintapolitiikassa mikä on hyväksyttävä riskitaso, joka voidaan ottaa. Suomen tietoturvallisuus strategian mukaan turvatoimenpiteitä tulee arvioida riskiperusteisesti ja ne tulee olla osana organisaation muuta riskienhallintaa (LVM 2017, 14).

Sähköjakeluverkonhaltijoilla ja siirtoverkonhaltijoilla on sähkömarkkinalain (588/2013) mukainen velvoite huolehtia verkon kehittämisestä, varautumissuunnittelusta ja yhteistoimintavelvoite häiriötilanteissa (LVM 2017, 17). Käytönvalvontaverkon toiminnan varmistaminen poikkeustilanteissa on edellytys velvoitteen täyttämisessä.

Direktiivi määrittelee vähimmäisvelvoitteet korkean verkko- ja tietojärjestelmien turvallisuuden ylläpitämiseksi. Direktiivi ei kuitenkaan määrittele yksiselitteisesti mikä tämä vähimmäisvelvoite on. Jäsenvaltioilla on laaja vastuu ja harkintavalta näiden vaatimusten laatimisessa. (LVM 2017, 35).

Tavoitteena on myös ennaltaehkäistä kyberturvallisuusriskien toteutuminen riittävien turvatoimenpiteiden ja kontrollien avulla. Riskien toteutuessa tavoitteena on vaikutusten lieventäminen siedettävälle tasolle ja toiminnan jatkuvuuden turvaamien myös poikkeustilanteissa. Näiden tavoitteiden saavuttamiseen pyritään vaikuttamaan ennalta tehtävän jatkuvuus- ja palautumissuunnitelmien avulla.

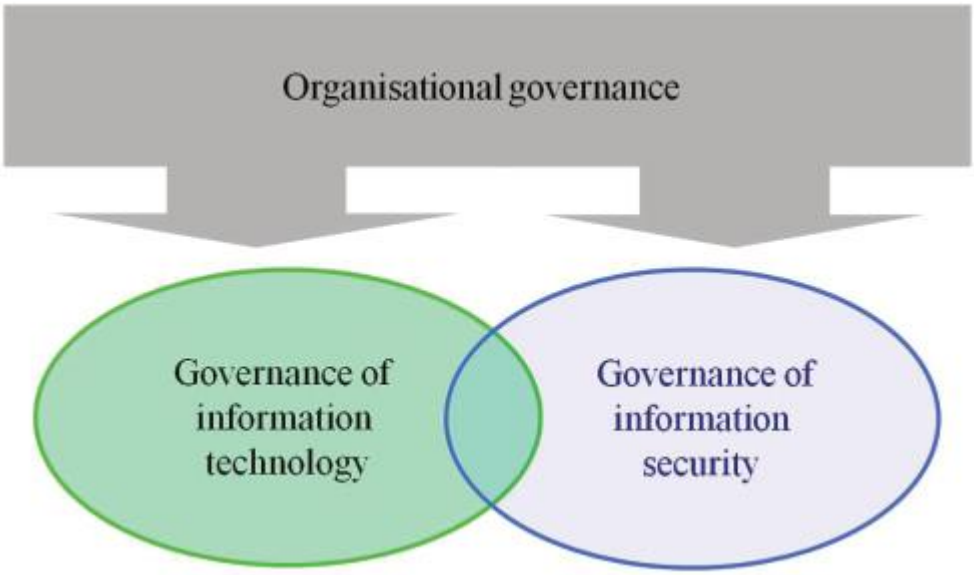
NIS-direktiivin mukaan verkko- ja tietojärjestelmien turvallisuudella tarkoitetaan järjestelmien kykyä suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen, siirrettyjen tai käsiteltyjen tietojen luottamuksellisuuden, eheyden tai saatavuuden. Keskeisten palveluntarjoajien tulee varmistaa käyttämiensä verkkojen ja tietojärjestelmien turvallisuus riippumatta siitä hallinnoiko niitä oma tietotekninen henkilöstö vai ulkoistettu tietoturvahallinto. Myös ilmoitusvaatimuksia sovelletaan riippumatta siitä, onko verkko- ja tietojärjestelmien ylläpito hoidettu sisäisesti tai ulkoisesti. (LVM 2017, 10).

Tietoturvallisuuden tavoitteiden asettamisesta vastaa aina organisaation ylin johto. Tavoitteet kirjataan yleensä tietoturvapolitiikkaan. Organisaatiolla on yleensä ICT toiminnoista vastaava ryhmä, joka vastaa tietoturvan toteuttamisesta operatiivisella tasolla ja toteuttaa johdon asettamat tavoitteet.

5 TIETOTURVALLISUUDEN HALLINTAMALLI

Tietoturvallisuuden hallintamallin tavoitteena on yhdenmukaistaa tietoturvan tavoitteet ja tietohallintostrategia liiketoimintatavoitteiden ja liiketoimintastrategian kanssa. Hallintamallin tavoitteena on myös huolehtia, että tietoturvariskit on käsitelty riittävällä tasolla organisaation riskienhallinnassa ja se noudattaa organisaation riskienhallintapolitiikkaa. Hallintamallin avulla tietoturvariskeihin liittyvä päätöksen teko helpompaa. Toimivan tietoturvallisuuden hallintamallin avulla organisaation johto on tietoinen tietoturvallisuuden tilasta. Myös tietoturvaan tehtävät investoinnit ovat tehokkaampia ja ne on kohdennettu paremmin oikeisiin investointikohteisiin. Hallintamallin tehtävä on huolehtia, että organisaatio noudattaa oikeudellisia, lainsäädännöllisiä ja sopimuksellisia velvoitteita. (ISO27014 2013, 2).

Organisaation hallintotapa ohjaa tiedonhallinnan ja tietoturvallisuuden hallintamalleja. Jokainen hallintamalli on olennainen osa koko organisaation hallintotapaa, jossa korostuu liiketoimintatavoitteiden yhdenmukaistamisen merkitys. Hallintoelimen on kehitettävä kokonaisvaltainen ja integroitu näkemys hallintomallistaan, josta hallinnoidaan tietoja ja tietoturvallisuutta. Hallintomallien ulottuvuudet ovat osittain päällekkäisiä. Hallintamallien välinen suhde on kuvattu kuviossa 1. (ISO27014 2013, 3).



Kuva 1 Organisaation hallintavan ja hallintamallien välinen suhde. (ISO27014 2013, 3).

Tiedonhallinnan hallintamalli varmistaa resurssit joita tarvitaan, kun tietoa hankitaan, käsitellään, tallennetaan ja siirretään. Tietoturvallisuuden hallintamalli huolehtii tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta.

Hallintamallissa on tarkoitus kuvata ne keskeiset hallintakeinot, jonka pohjalta voidaan lähteä kehittämään yrityksen tietoturvan hallintajärjestelmää (ISMS). Tietoturvallisuuden hallintajärjestelmä on organisaation formaali tapa suojata organisaation tieto-omaisuutta. Hallintajärjestelmän avulla organisaatio määrittää organisaation tietoturvan hallinnan resurssit, toimintamallit ja periaatteet, ohjeet ja menettelytavat, joilla tietoturvallisuuden toteutumista, valvotaan, ohjataan ja johdetaan. (ISO27000 2015, 19-20). Hallintamalli kuvaa myös menetelmät ja menettelytavat, prosessit ja mittarit joilla toiminnan tehokkuutta ja yrityksen tietoturvan tasoa seurataan ja parannetaan. Se määrittelee tietoturvan näkökulmasta organisaation hyvän hallintotavan edellyttämät vaatimukset ja hallintakeinot joilla nämä vaatimukset täytettään. Tietoturvan hallintamalli on läpinäkyvä ja olennainen osa koko yrityksen hallintoa. IT Governance instituutin mukaan tietoturvallisuuden hallintamalli tulisi sisällyttää seuraavat viisi kohtaa. (ITGI 2006, 11):

1. Yhdenmukaistaa tietoturvastrategia yhdessä liiketoimintastrategian kanssa tukemaan organisaation tavoitteita.
2. Toteuttaa riskienhallintaa, jonka avulla parannetaan valmiuksia hallita ja vähentää riskejä ja pienentää niiden vaikutusta yrityksen tietoresursseihin.
3. Hallita resursseja tehokkaasti hyödyntämällä infrastruktuurin resursseja ja tietoturva-osaamista tehokkaasti.
4. Suorituskyvyn mittaaminen mittaamalla, monitoroimalla ja raportoimalla organisaation tavoitteiden saavuttamiseksi.
5. Optimoida tietoturva-investoinnit tukemaan organisaation tavoitteita.

Hyvällä tietoturvan hallintamallilla organisaatio voi lisätä organisaation arvoa, kasvattaa mainetta luotettavana toimijana. Hallintamalli lisää ennustettavuutta ja vähentää epävarmuutta yrityksen liiketoiminnalle vähentämällä tietoturvaan liittyviä riskejä hyväksyttävälle tasolle. Se pienentää myös riskiä joutua oikeudelliseen vastuuseen tietosuojarikkomuksien, tietojen virheellisyyden tai puuttumisen takia. Tietoturvallisuuden hallintaan kuuluu myös tietototurvapolitikka, jota noudattamalla luodaan hyvä pohja tehokkaalle tietoturvariskien hallinnalle, tietoturvakontrollien kehittämiselle, sekä kyvylle reagoida poikkeamiin nopeasti ja tehokkaasti. Se turvaa yrityksen tieto-omaisuuden ja varmistaa, että yrityksen päätökset perustuvat oikeaan tietoon. Se turvaa liiketoiminnan kannalta kriittisiä prosesseja ja mahdollistaa niiden palauttamisen häiriötilanteissa. Hyvä hallintamalli auttaa myös vastaamaan regulaation ja lainsäädännön asettamiin vaatimuksiin. Se lisää asiakkaiden ja kumppaneiden luottamusta yrityksen toimintaan. (ITIG 2006, 11-13).

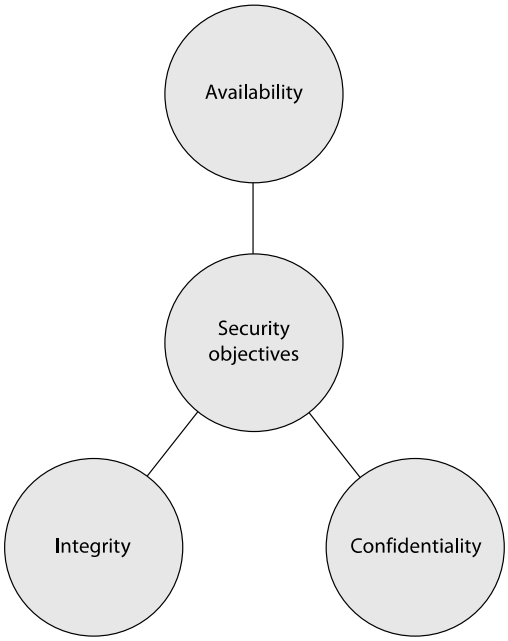
ISO27002 standardi määrittelee 14 osa-aluetta, jotka hallintamallissa tulee huomioida. Nämä osa-alueet sisältävä kaikkiaan 114 hallintakeinoa, joilla tietoturvallisuutta hallinnoidaan. Nämä hallintakeinot muodostavat yhtenäisen johtamisjärjestelmän. Organisaatio valitsee sille sopivimmat hallintakeinot tietoturvallisuuden toteuttamiseen riskienhallinnan kautta. ISO27001 vaatimuksissa todetaan, että tietoturvallisuuden hallinjärjestelmään valittujen hallintakeinojen täytyy perustua riskien arviointiin (ISO27005, 24). Ilman riittävää toimintaympäristön tuntemusta ja kattavaa riskienhallintaa ei organisaatio pysty suunnittelemaan ja toteuttamaan sille sopivinta tietoturvallisuuden hallintamallia. Jos organisaatio pyrkii täyttämään kaikki vaatimukset toteuttamalla kirjaimmellisesti kaikki ISO27002 standardin määrittelemät hallintakeinot voi lopputulos olla, että tietoturvallisuuden hallinta on raskas, tehoton ja se ei kohdistu oikeisiin kohtiin organisaation toiminnassa. Saavutetut hyödyt voivat jäädä pieniksi, koska tieturvallisuudesta vastaava organisaatio ei kykene hoitamaan sille asetettuja velvoitteita. Liian raskas tietoturvallisuuden hallintajärjestelmä ei myöskään ole taloudellisesti järkevää, koska panostukset kohdistuvat vääriin paikkoihin, jolloin tekeminen on kallista saavutettuihin tuloksiin nähden. Tietoturvallisuuden hallinta perustuu tietoturvariskien hallintaan. Riskienhallinta on keskeisessä roolissa tietoturvan suunnittelun lähtökohtana. Suojattavaa omaisuutta voi uhata erilaiset tahattomat ja tahalliset uhkat, jotka pyrkivät vaikuttamaan prosessien, järjestelmien, tietoverkkojen ja henkilöiden luontaisten haavoittuvuuksien kautta. Myös erilaiset muutokset liiketoimintaprosesseissa ja järjestelmissä voivat luoda uuden tyyppisiä tietoturvariskejä. Uusia tietoturvariskejä voi muodostua myös organisaation ulkopuolella, kuten esimerkiksi lainsäädännön muutokset ja esilaiset viranomaismääräykset. Kaikilta tietoturvariskeiltä ei voi täydellisesti suojautua ja näin ollen organisaatioiden tulee riskienhallinnan kautta pyrkiä suojaamaan omaisuuteen kohdistuvilta uhilta minimoimalla tietoturvariskien vaikututtavuutta tieto-omaisuuteen, sekä pienentää riskien toteutumisen mahdollisuutta minimoimalla hyökkäysvektorien hyökkäyspintaa mahdollisimman tehokkaasti. (ISO27002 2014, 8-10).

5.1 Tietoturvallisuuden hallintamallin vaatimukset

Tietoturvallisuuden hallinnan tulisi kattaa kaikki sille asetetut vaatimukset ja tavoitteet. On tärkeää ymmärtää mitkä kaikki tekijät vaikuttavat tietoturvallisuuden toteutumiseen ja sen hallintaa. Tietoturvallisuuden hallintaa ohjaavat alla luetellut erilaiset vaatimukset ja tavoitteet.

1. Lainsäädäntö ja direktiivit
2. Liiketoimintastrategian asettamat tietoturvavaatimukset
3. Tietohallintostrategian asettamat tietoturvavaatimukset
4. Eri sidosryhmien asettamat vaatimukset
5. Sopimukselliset vaatimukset

Tietoturvallisuuden tulisi huolehtia, että kaikki turvallisuuden perusperiaatteet toteutuvat. Tietoturvallisuuden yleiset periaatteet kuvataan yleensä CIA kolmiolla. Tavoitteena on suojata suojattavan omaisuuden luottamuksellisuus (Confidentiality), eheys (Intergrity) ja saatavuus (Availability).



Kuva2. Turvallisuuden perusperiaatteet CIA –kolmio (Harris, Maymi 2016, 3-4).

Luottamuksellisuudella tarkoitetaan sitä, että tietoon ja toimintoihin pääsevät käsiksi vain valtuutetut tahot. Eheys takaa, että tietoja ja toimintoja voidaan lisätä, muokata tai poistaa vain valtuutettujen tahojen hyväksynnällä. Saatavuudella varmistetaan, että järjestelmät, toiminnot ja data ovat saatavilla asetetun palvelutason mukaan. (Harris, Maymi 2016, 4-5).

Tasapainoinen turvallisuus saavutetaan, jos kaikki suojaamisen perusperiaatteet otetaan huomioon ja kaikista kolmesta alueesta huolehditaan. On ymmärrettävä, ettei pelkkä tietojen salaaminen suojaa tietoa, jos eheyttä tai saatavuus jää huomioimatta. Perusperiaatteiden toteuttaminen käytännössä voi olla todella haastavaa. On helpompi ymmärtää, alla olevan listan avulla millaisilla

kontrolleilla ja toimenpiteillä tiedon saatavuus, eheys ja luottamuksellisuus voidaan varmistaa. (Harris, Maymi 2016, 5-6):

Saatavuus:

- Levyjen kahdentaminen muodostamalla useammalla fyysisellä levyllä yksi looginen levy (RAID).
- Järjestelmien klusterointi
- Kuorman tasaus useampaan järjestelmään
- Kahdennetut tiedon ja sähkönsiirtokaapelit
- Ohjelmisto ja data varmistukset
- Peilaus
- Maantieteellinen hajauttaminen
- Palautustoiminnallisuudet
- Vikasietoiset konfiguraatiot

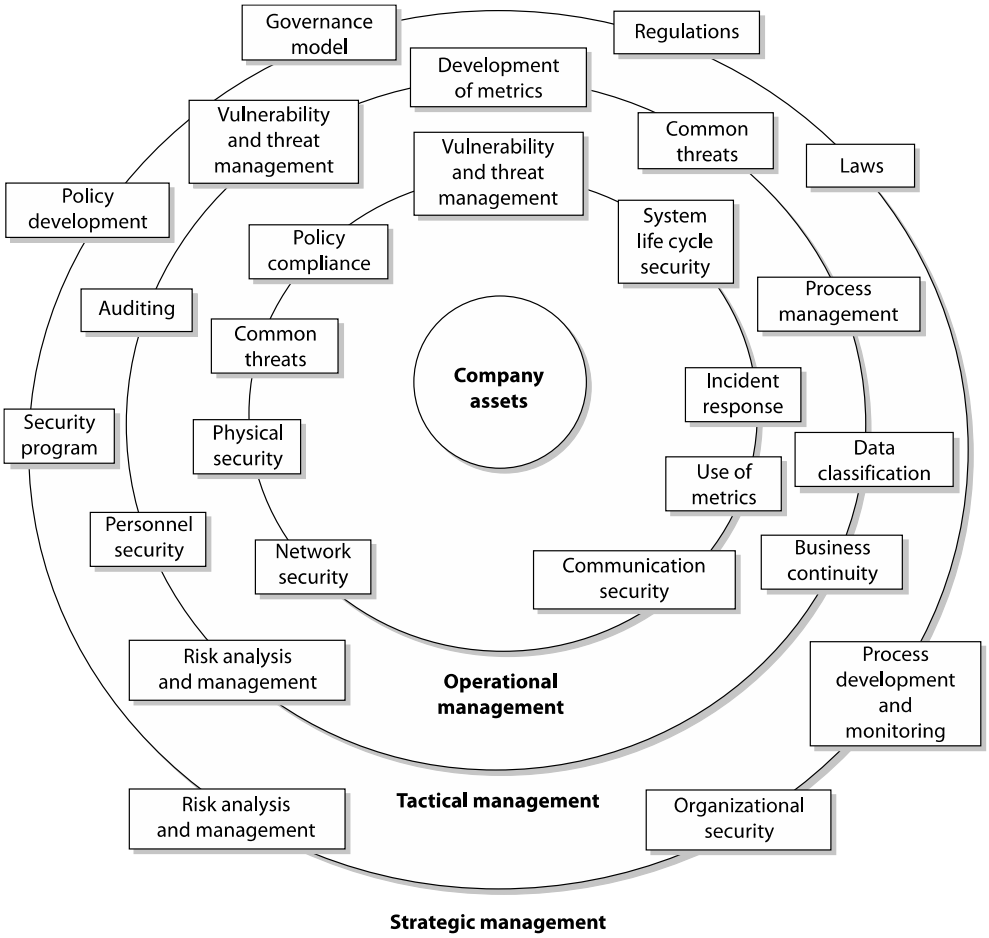
Eheys:

- Hash –tunnisteet (datan eheys).
- Konfiguraation hallinnalla (järjestelmien eheys).
- Muutosten hallinta (prosessit)
- Pääsyn hallinta
- Ohjelmistojen digitaalinen allekirjoitus

Luottamuksellisuus:

- Datan salaaminen säilytettäessä (levyjen tai tietokantojen salaaminen).
- Datan salaamien siirrettäessä (IPSec, SSH, TLS).
- Fyysinen ja tekninen pääsynhallinta

Tietoturvallisuuden hallinta on osa organisaation koko turvallisuuden hallintaa. Hallinta tulisi ulottua kaikille tasoille organisaation toiminnassa. Tietoturvallisuuden hallinta tulee ulottaa, niin strategiselle, taktiselle kuin operatiiviselle tasolle. Harris ja Maymi kuvaavat nämä turvallisuuteen vaikuttavat ja ohjaavat tekijät seuraavassa kuvassa.



Kuva3. Organisaation turvallisuusohjelman eri tasot (Harris, Maymi 2016, 169).

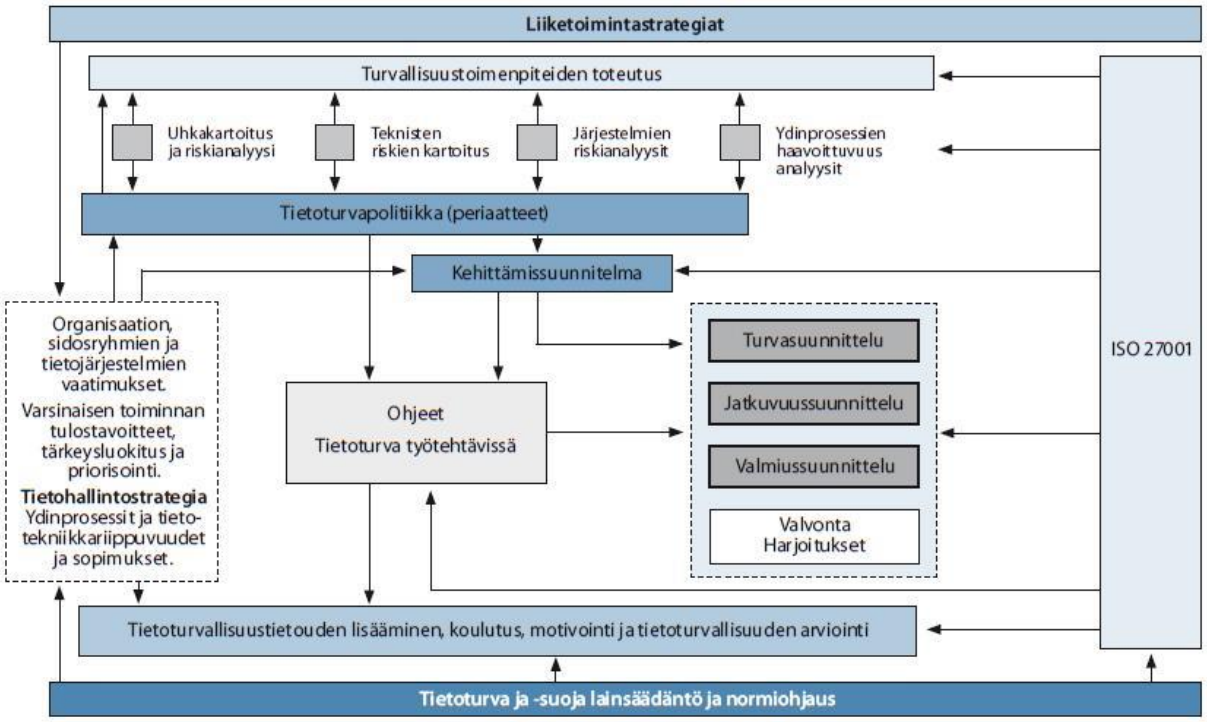
Strategisella tasolla määritellään organisaation tietoturvapolitiikka, joka määrittelee organisaation keskeiset tietoturvallisuusperiaatteet. Tietoturvapolitiikan hyväksyy organisaation ylin johto. Tietoturvapolitiikan tulee noudattaa yrityksen strategisia ja liiketoiminnallisia tavoitteita ja päämääriä. Tietoturvallisuuspolitiikkaa tarkastellaan yleensä 6-12 kuukauden välein. Taktisella tasolla organisaatiolle valitaan standardit, jotka sisältävät tarkemmat ohjeet, säännöt ja toimenpiteet joilla tuetaan tai vahvistetaan organisaation tietoturvapolitiikkaa. Standardien pohjalta laaditaan organisaatiolle tarkemmat ohjeistukset, jotka määrittelevät suositeltavat tavat toteuttaa standardien vaatimuksia. Ohjeistukset ovat operatiivisia toimintaohjeita henkilöstölle ja IT:stä vastaaville työntekijöille esimerkiksi missä salasanoja voidaan säilyttää. Menettelytavoilla kuvataan yksityiskohtaiset vaihe vaiheelta ohjeet, jotka tekemällä halutut tavoite saavutetaan. On kuitenkin syytä huomioida, että ilman näiden ohjeiden ja standardien jalkauttamista ne ovat vain tiedostoja, joissain organisaation järjestelmässä. On tärkeää kertoa ohjeiden ja sääntöjen olemassa olosta ja kouluttaa henkilöstöä säännöllisesti toimimaan niiden mukaan. (Harris, Maymi 2016, 90-93).

Harris ja Maymi määrittelevät, että tietoturvallisuuden hallintamallin mukaan organisaatiolla tulisi olla tietoturvallisuuden kehitysohjelma, joka on integroitu osaksi organisaation liiketoiminta-arkkitehtuuria. Lisäksi organisaation tulee kehittää tietoturvariskien hallintaohjelma osaksi organisaation riskienhallintaa. Tietoturvallisuuden hallinnan osa-alueet tulee dokumentoida ja kuvata riittävän kattavasti. Tietoturvallisuuden hallintamallin tulisi toimia organisaatiossa eräänlaisena

viitekehyksenä, joka mahdollistaa tietoturvallisuus tavoitteiden asettamisen eri organisaation tasoille ja niiden jalkauttamisen osaksi organisaation toimintaa. Organisaatiolle tulee kehittää valvontamekanismi, joka velvoittaa tietoturvasta vastaavat seuraamaan ja raportoimaan tietoturvallisuuden tilaa organisaation eri tasoilla. On tärkeää ymmärtää, ettei tietoturvallisuuden vastuuta voida pelkästään laittaa ICT –organisaation vastuulle, koska tietoturvallisuus kostuu tekniikan lisäksi myös erilaisista hallinnollisista toimista. (Harris Maymi 2016, 159-160).

5.2 Tietoturvallisuuden hallintamallin rakenne

Tietoturvallisuuden hallintamalli koostuu useista eri osa-alueista. Se pitää sisällään tietoturvapolitiikan, joka kuvaa ne keskeiset periaatteet joilla organisaatio huolehtii tietoturvan toteutumisesta. Se sisältää tietoturvallisuuden kehittämissuunnitelman, jatkuvuussuunnittelun ja valmiussuunnittelun, sekä tietoturva ohjeet ja hallintakeinot, joiden avulla varmistetaan yrityksen tietoturvan toteutuminen, jatkuvuuden hallinta ja toimintakyky poikkeustilanteissa. Tietoturvallisuuden hallinta perustuu säännölliseen riskienhallintaan ja toiminnan suunnitteluun. Se määrittelee tietoturvaorganisaation ja sen vastuut, politiikat ja ohjeet, prosessit, menettelytavat ja hallintakeinot. Hallintamallin avulla seurataan ja arvioidaan organisaation tietoturvatoimenpiteiden kyvykkyyttä ja tehokkuutta, sekä huolehditaan jatkuvasta kehittämisestä ja parantamisesta. Se on organisaation viitekehys, jolla se pyrkii hallitsemaan systemaattisesti tietoturvan toteutumista. (VAHTI 8/2006).



Kuva 4. Tietoturvallisuuden hallintamallin rakenne. (VAHTI 8/2006).

Tietoturvallisuuden hallintamallin vaatimukset ja tavoitteet koostuvat liiketoimintastrategian asettamista vaatimuksista, sekä lainsäädännön ja normien asettamista vaatimuksista. Myös sidosryhmien kautta voi tulla omia erityisvaatimuksia tietoturvan toteuttamiselle.

Tietoturvallisuuden hallinta voidaan jakaa seitsemään eri aihe-alueeseen. Tietoturvallisuuden hallintamalli ottaa kantaan jokaiseen näistä seitsemästä aihe-alueesta. Aihe-alueet kattavat koko IEC27001 standardin asettamat vaatimukset. Alueet voidaan jakaa seuraavasti.

1. Tietoturvan johtaminen ja politiikka
2. Henkilöturvallisuus
3. Tietojärjestelmien tietoturvallisuus
4. Tietoliikenteen tietoturvallisuus
5. Fyysinen tilaturvallisuus
6. Suojeltavan omaisuuden ja tiedon hallinta
7. Toiminnan jatkuvuuden hallinta

Tietoturvallisuuden hallintamalli pitää sisällän seuraavia keskeisiä dokumentteja ja toimintamalleja. Kattavan dokumentoinnin avulla organisaatio kykenee myös osoittamaan, että toiminta on suunnitelmallista ja se on määrämuotoista ja sitä kehitetään jatkuvasti. Dokumentaation avulla organisaatio pystyy todentamaan, että toiminta on ISO27001 vaatimusten mukaista.

- Tietoturvapolitiikka
- Tietoturvakäytännöt ja ohjeet
- Keskeiset tietoturvan hallintakeinot ja kontrollit
- Tietoturvallisuuden kehittämissuunnitelma
- Tietoturva-arkkitehtuurin kuvaukset ja dokumentit
- Tietoturvan raportoinnin yrityksen johdolle
- Jatkuvuus- ja valmiussuunnitelmat
- Tietoturvariskien hallinnan
- Tietoturvaprosessit
- Viestintäsuunnitelmat
- Auditointisuunnitelman

Tietoturvallisuuden hallintamalli varmistaa, että tietoturvallisuuden tavoitteet asetetaan ja julkaistaan koko organisaation laajuudella. Se määrittelee mitä hallintakeinoja on toteutettava tietoturvallisuuden parantamiseksi ja kuinka niitä tulisi seurata ja mitata. On tärkeää luoda tietoturvallisuudesta kokonaiskuva ja varmistaa, että organisaatio ja johto ovat aina ajan tasalla turvallisuustilanteesta. On tärkeää luoda mekanismit, joilla läpinäkyvyyttä lisätään, jotta turvallisuudesta vastaavat voivat huolehtia, että turvallisuusmekanismit ja toimenpiteet ovat riittäviä ja ne toimivat oikein. Organisaatiolla tulee olla yhtenäiset kommunikointitavat koko organisaation läpi. Standardoitu tapa raportoida eri turvallisuuden osa-alueista ja turvallisuustoimien tehokkuutta mittaavat mittarit.

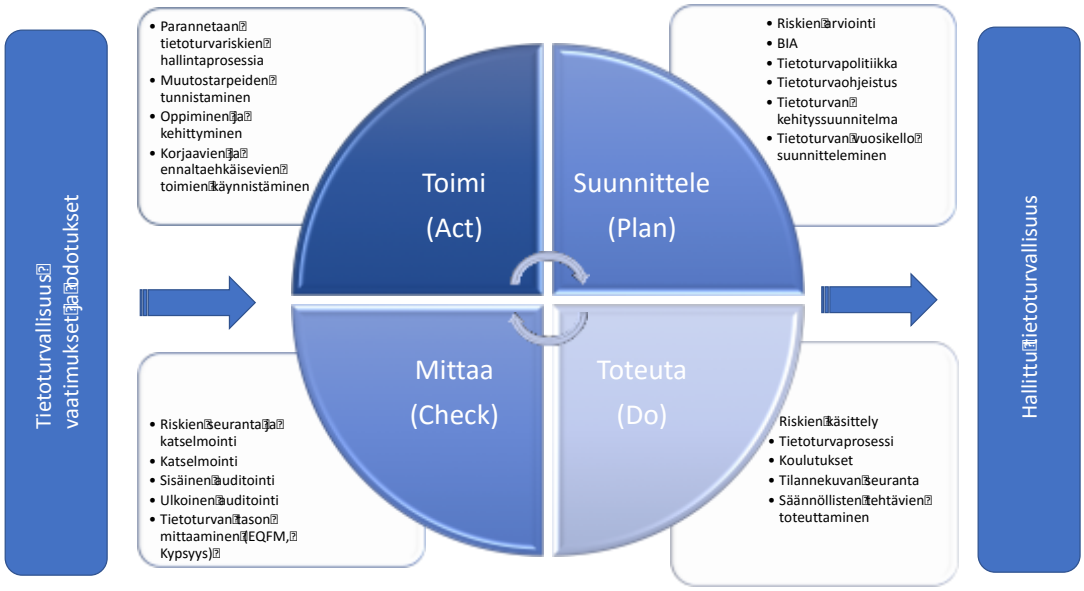
6 TIETOTURVAPROSESSIT

Tietoturvan hallinnalla on muutamia keskeisiä prosesseja, joilla tietoturvan toteutumisesta huolehditaan. Näiden lisäksi tietoturva tulisi ulottaa mukaan kaikkiin yrityksen prosesseihin, koska ainoastaan niin tietoturva on mukana koko organisaation toiminnassa. Organisaation ydinprosessien omistajilla on vastuu huolehtia, että prosessien eri vaiheet on arvioitu ja tunnistettu tietoturvan kannalta kriittiset kohdat. Tietoturvallisuuden hallinmallin hallintakeinojen tulisi ottaa kantaa tunnistettuihin kohtiin prosesseissa, niin että tietoturva toteutuu kaikissa sen vaiheissa.

6.1 Tietoturvallisuuden hallinnan kehittämisen prosessi

Tietoturvan toteuttaminen on jatkuvan kehittämisen ja oppimisen prosessi. Se on johtamisen prosessi, jota toistamalla säännöllisesti turvataan tietoturvan ylläpito ja kehittäminen. (Suomen kyberturvallisuus strategia 2013, 19). Jatkuvan kehittämisen malli voidaan kuvata PDCA-mallin avulla, jota yleisesti käytetään myös laadun johtamisessa ja prosessien kehittämisessä. PDCA-malli soveltuu myös tietoturvan johtamiseen, koska sen avulla organisaatio voi varmistaa standardin ISO27001 jatkuvan parantamisen vaatimuksen toteutumisen (ISO27001, 22). PDCA-mallin avulla kuvataan jatkuvan kehittämisen prosessi, jonka avulla tietoturvallisuuden hallintajärjestelmää pidetään yllä. PDCA-malliin kuuluu vaiheet suunnittele, toteuta, arvioi ja toimi. (ISO9001 2015, 7). Hallintamallin kehittäminen kuuluu PDCA –mallin suunnitteluvaiheeseen. Hallintamallin pohjalta rakennetaan tietoturvallisuuden hallintajärjestelmä, jota kehitetään PDCA –mallin mukaisesti seuraamalla toimintaa ja tekemällä arviointia joiden perusteella tehdään johtopäätöksiä hallintamallin toimivuudessa ja kehittämiskohteista. Kehittämiskohteet viedään takaisin suunnitteluvaiheeseen ja PDCA –mallin kierto alkaa alusta. Tietoturvan hyvä johtaminen toteutuu, jos PDCA-mallin kaikki osa-alueet ovat siinä mukana.

Tietoturvallisuuden vaatimukset ja tavoitteet toimivat syötteenä PDCA –mallilla kuvatussa prosessissa. ISO27002 standardin mukaan vaatimukset tulevat kolmesta lähteestä. Ensimmäiset tavoitteet muodostuvat organisaation tekemän tietoturvariskien arvioinnin perusteella. Toiset tavoitteet tulevat lainsäädännöstä, viranomaisvaatimuksista ja erilaisista sopimuksien sisältämistä vaatimuksista. Kolmantena tavoitteita muodostavat organisaation omat toimintaperiaatteet, tavoitteet ja liiketoimintavaatimukset. (ISO27002 2014, 8-10).



Kuva 5. Tietoturvallisuuden PDCA-malli (VAHTI 2014, 15)

Suunnitteluvaiheessa keskeisessä roolissa on tietoturvariskien tunnistaminen ja niiden pohjalta tehtävä riskianalyysi ja riskien arviointi. Riskien arvioinnin perusteella hyväksytään riskit ja tehdään riskienkäsittelysuunnitelma. BIA –analyysin avulla arvioidaan näiden riskien vaikuttavuutta liiketoiminnalla. Yleensä vaikuttavuutta mitataan taloudellisilla mittareilla. BIA –analyysissa pyritään arvioimaan paljonko riski toteutuessaan aiheuttaa kustannuksia organisaation liiketoiminnoille. Näiden arvioiden pohjalta yritykselle luodaan tietoturvapolitiikka ja valitaan keskeiset hallintakeinot ja toimenpiteet. Hallintakeinojen säännölliset tehtävät on hyvä sijoittaa tietoturvallisuuden vuosikelloon, jolloin toiminta on suunnitelmallista ja erilaiset kontrollit toistetaan määrävälein.

Toteutusvaiheessa toteutetaan riskienkäsittelysuunnitelma, sekä suoritetaan tietoturvaprosessien mukaista toimintaa, johon kuuluvat tietoturvasuunnitelmassa ennalta määritellyt tietoturvatoimenpiteet ja hallintakeinojen toteuttaminen. Säännölliset koulutukset henkilöstölle, järjestelmien pääkäyttäjille ja tietoturvasta vastaaville henkilöille kuuluvat myös toteutusvaiheeseen.

Mittaaminen on kehittämisen näkökulmasta välttämätöntä tietoturvan hallintamallissa. Riskejä katselmoidaan ja seurataan jatkuvan riskienhallinnan periaatteiden mukaisesti. Ilman mittaamissa ja tietoturvallisuuden kypsyyden arvioimista ei voida tunnistaa kehitettäviä kohteita. Mittaamista voidaan tehdä monella eri tavalla. Myös erilaiset katselmoinnit, sisäiset ja ulkoiset auditoinnit säännöllisesti tehtynä voivat auttaa organisaatiota tunnistamaan kehitettäviä kohteita. Organisaation tulee määrittää sille parhaiten sopivat mittarit, joilla tietoturvallisuuden kehittymistä seurataan.

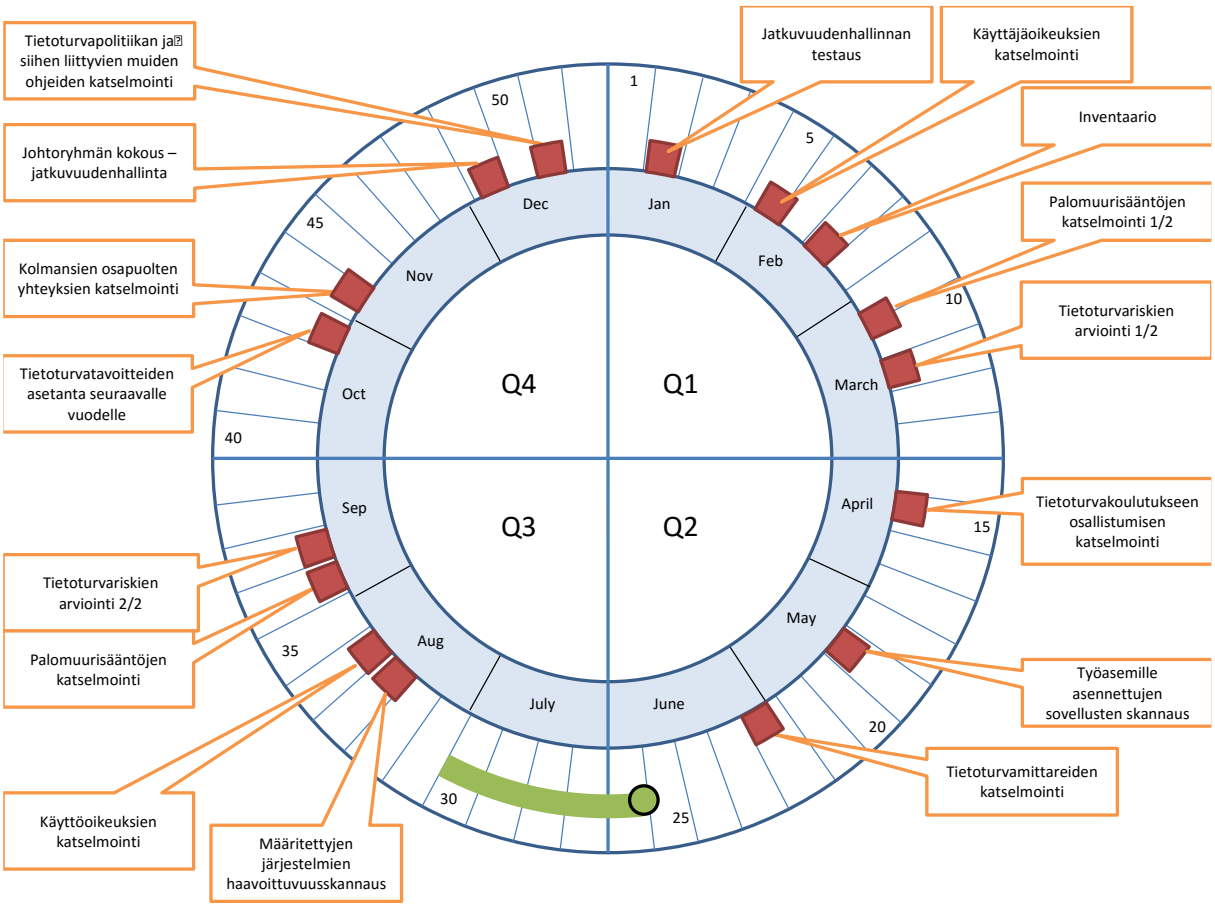
Toimintavaiheessa tulee tunnistaa ne muutostarpeet, joita yrityksen tietoturvan kehittäminen vaatii. Muutokset pohjautuvat tietoturvariskienhallintaprosessin ylläpitoon ja parantamiseen. Toiminnan tulee olla jatkuvaa kehittymistä ja oppimista. Toimintavaiheessa tulee käynnistää tarpeelliset ennaltaehkäisevät ja korjaavat toimenpiteet, jotka aloitetaan suunnitteluvaiheessa. Mallia toistamalla

lopputuloksena organisaatiolle kehittyy hallittu tietoturvallisuus, joka suojaa organisaation suojattavaa tieto-omaisuutta.

6.2 Tietoturvallisuuden jatkuvien palveluiden hallintaprosessi

Tietoturvapolitiikan ja sen mukaisen hallinmallin tulee toteuttaa tietoturvallisuuden vuosisuunnittelua. Johdon tulee huolehtia, että organisaatiolla on riittävät resurssit, toteuttaa kehittämistoimintaa ja vuosittaiset ylläpitotehtävät, sekä tietoturvatoiminnasta aiheutuvien kustannusten budjetointi. (VAHTI 2 2011, 19).

Tietoturvan jatkuvien palveluiden hallintaprosessi kuvataan yleensä vuosikellon avulla. Hallintamallin kontrollit sijoitetaan vuosikelloon toiminnan systemaattisuuden varmistamiseksi. Vuosikello auttaa aikatauluttamaan keskeiset toimenpiteet, joita toistamalla varmistetaan, että tietoturvan hallinta on jatkuvaa ja säännönmukaista.



Kuva 6. Tietoturvan vuosikello (KPMG 2016, 8).

Hallintamallin keskeiset kontrollit sisältävät erilaisia tarkistuksia ja katselmointeja, joilla huolehditaan tietoturva kontrollien pysymisestä ajan tasalla. Katselmoinneissa voidaan systemaattisesti käydä läpi pääsynhallintaan ja käyttöoikeuksiin liittyvä dokumentointi ja tarkistaa esimerkiksi annettujen käyttöoikeuksien ajantasaisuus.

Myös jatkuva henkilöstön, pääkäyttäjien ja tietoturvasta vastaavien koulutus ja tietoisuuden lisääminen ovat välttämätöntä nopeasti muuttuvassa kyberturvallisuus toimintaympäristössä. Myös ISO27001 vaatimukset edellyttävät säännönmukaista koulutusta ja osaamisen kehittämistä.

Säännönmukainen raportointi ja seuranta takaavat organisaation kyvykkyyden reagoida kehitettäviin asioihin. Tietoturvallisuuden tasoa tuleekin vaatimusten mukaan jatkuvasti arvioida ja mitata.

Myös jatkuvuuden varmistaminen ja erilaisten harjoitusten ja testaamisten avulla tulee olla säännönmukaista, jotta mahdollisten häiriötilanteiden sattuessa pystytään toimimaan ja huolehtimaan nopeasta palautumisesta normaaliin tilaan.

6.3 Tietoturvariskien käsittelyprosessi

OECD suosituksen mukaan digitaaliseen turvallisuuteen kohdistuvien riskien käsittely tulisi tehdä jatkuvan riskienarvioinnin periaatteiden mukaisesti ja sen tulisi integroitua koko organisaation riskienhallintaan. Johdon vastuulla on varmistaa, että riskien arviointi on systemaattisesti toistettava prosessi, jonka tavoitteena on arvioida uhkien ja haavoittuvuuksien vaikutuksia taloudelliseen toimintaan. Riskien käsittelyyn liittyvän päätöksen teon tueksi on kerättävä mahdollisimman paljon tietoa digitaalisen ympäristön muutoksista, sitä uhkaavista uhista ja haavoittuvuuksista, jotta kyberturvallisuusriskien minimointiin johtavien hallintakeinojen ja turvallisuustoimenpiteiden valinta voidaan kohdistaa oikeisiin kohtiin. (Valtionvarainministeriö 28/2016, 14). Tietoa tulisi kerätä tekemällä säännöllisesti uhkakartoitus ja riskianalyysejä, teknisiä riskikartoituksia, järjestelmien riskianalyysejä ja ydinprosessien haavoittuvuusanalyysejä. Myös erilaisten poikkeamien ja havaintojen raportoiminen auttaa havaitsemaan ne kohdat joihin uhkia eniten kohdistuu. Toistamalla riskienhallintaprosessia organisaatio voi syventää omaa tietoturvariskien arviointia ja saavuttaa yksityiskohtaisemman tason tietoturvallisuus riskien arvioinnissa. Syvemmän riskianalyysin avulla organisaation on helpompi valita oikeat turvatoimenpiteet ja hallintakeinot riskien pienentämiseksi. (ISO27005 2013, 22) Riskienhallinnan tulisi olla lähtökohtana, kun lähdetään organisaation tietoturvallisuuden hallinjärjestelmää suunnittelemaan. ENISA:n mukaan tietoturvariskienhallinnan onnistumiseen vaikuttaa kuinka hyvin se saadaan sisällytetty organisaation kulttuuriin ja liiketoimintaprosesseihin. Riskienhallinta tulisi olla organisaatiossa kaikkien vastuulla. (ENISA 2006, 12).

NIS-direktiivin mukaan keskeiset palveluntarjoajat velvoitetaan tekemään riskienhallintatoimenpiteitä. Palveluntarjoajien tulee huolehtia, että organisaatiolla on asiamukaiset oikeassa suhteessa toteutetut tekniset ja organisatoriset toimenpiteet riskien hallitsemiseksi, jotka kohdistuvat niiden verkko- ja tietojärjestelmien turvallisuuteen. Toimenpiteillä on varmistettava, että verkko- ja tietojärjestelmien turvallisuuden taso on suhteutettu riskiin nähden ja käytössä on huomioitu uusin tekniikka. (LVM 2017, 10).

ISO27001 standardi ei itsessään sisällä riskienhallintaan liittyviä menetelmiä, vaan se kuvaa pelkästään tietoturvallisuuden hallintajärjestelmälle asetettuja vaatimuksia. Organisaatioiden tulee

itse määrittää omat riskienhallintatoimintamallinsa. Hallintajärjestelmän vaatimukset voidaan täyttää monella eri tavalla ja tästä syystä organisaatioiden tulee valita heidän toimintaympäristölleen sopivimmat menettelytavat. (ISO 27005, 8). ISO27001 vaatimukset täyttäviä riskienhallintamenetelmiä on useita ja organisaation kannattaa valita sille soveltuvimmat menetelmät.

ENISA on julkaissut luettelon kolmestatoista eri riskienhallinta- ja riskienarviointimenetelmästä, joista osa täyttää sellaisenaan ISO27001 vaatimukset. Esitellyt viitekehykset lähestyvät riskienhallintaa ja riskienarviointia hyvin erilaisesti lähestymiskulmista ja organisaation kannattaa valita sille sopivin lähestymistapa. Osa kattaa koko riskienhallinnan ja riskienarvioinnin ja osa vai jommankumman osa-alueen. Myös menetelmien laajuudessa on suuria eroja. Osa menetelmistä pitäytyy hyvin ylätasolla ja osa lähestyy hyvin järjestelmä keskeisesti. (ENISA 2006, 30-36).

Attributes / Products	Threat identification	Threat characterisation	Exposure assessment	Risk characterisation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only)	Size of organisation	Skills needed[5]	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	••	•	•	••	•••	•••	•••	•••	GE	Free	All	**	N	N	Prototype (free of charge)
Cramm	•••	•••	•••	•••					EN, NL, CZ	Not free	Gov, Large	***	N	N	CRAMM expert, CRAMM express
Dutch A&K analysis	•••	•••	•••	•••					NL	Free	All	*	N	N	
Ebios	•••	•••	•••	•••	•••	•••	•••	•••	EN, FR, GE, ES	Free	All	**	Y	N	EBIOS version 2 (open source)
ISF methods	•••	•••	•••	•••	•••	•••	•••	•••	EN	For ISF members	All except SME	* to ***	N	N	Various ISF tools (for members)
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	••	••	••	••	••	•••	•••	•••	EN	Ca. €100	All	**	N	N	
ISO/IEC IS 17799	•					•			EN	Ca. €130	All	**	N	Y	Many
ISO/IEC IS 27001						•	•		EN, FR	Ca. €80	Gov, Large	**	Y	Y	Many
IT-Grundschutz	•••	•••	•••	•••	•••	•••	•••	•••	EN, GE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	•••	•••	•••	•••					EN, FR	Not free	Large	*	N	N	
Mehari	•••	•••	•••	•••					EN, FR	€100-500	All	**	N	N	RISICARE (ca. € 10.000)
Octave	••	••	••	••	••	••	••	••	EN	Free	SME	**	N	N	
SP800-30 (NIST)	•••	•••		•••	•••	•••	•••		EN	Free	All	**	N	N	

Taulukko 1. Tietoturvallisuuden riskienhallinta ja riskienarviointimenetelmiä (ENISA 2006, 37-38).

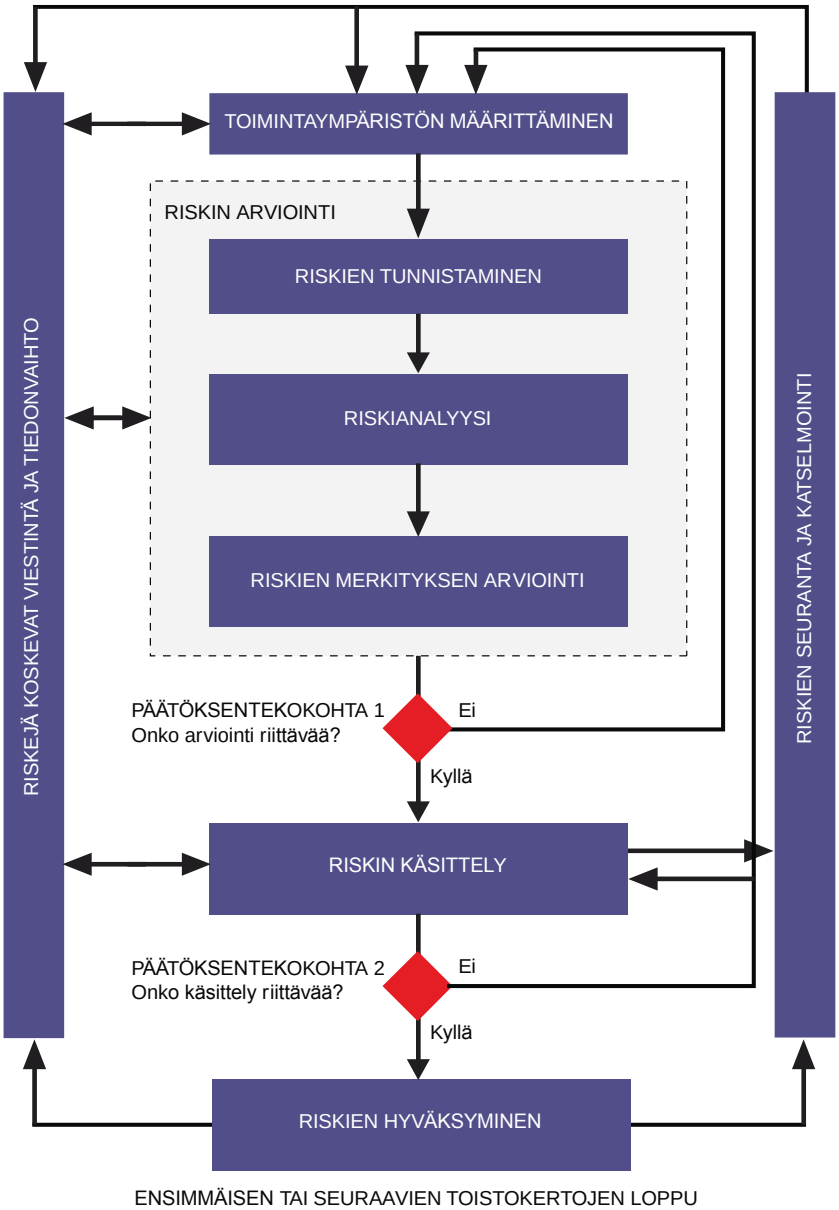
ENISA:n taulukon menetelmistä EBIOS, ISO/IEC 27005 ja IT-Grundschutz ovat yhteensopivia suoraan ISO27001 standardin vaatimuksille. (ENISA 2006, 11-55).

Tietoturvallisuusriskien hallinnan keskeinen tavoite riskien käsitteleminen ja hyväksyttyjen riskien pienentäminen hyväksyttävälle tasolle. Organisaatio määrittelee riskinottohalukkuuden, joka määrää

riskien riskitason, jonka organisaatio on valmis kantamaan. Se on tavoitetaso hyväksyttävälle tappion määrälle, jonka organisaatio on valmis toiminnassaan ottamaan riskin toteutuessa. Kun haluttu riskitaso on saavutettu, pyritään se ylläpitämään säännöllisen riskienhallintaprosessin avulla.

Riskien arvioinnin kautta pitäisi organisaation valita ne keskeiset hallintakeinot ja turvallisuustoimenpiteet, joilla asetettuihin tavoitteisiin päästää. Näillä toimenpiteillä on tarkoitus suojata organisaation digitaalisen toimintaympäristön toimivuus ja suojattava omaisuus. (ISO27005 2013, 18).

Tietoturvariskien hallinta tulisi olla osa koko yrityksen riskienhallintaa. Tietoturvariskit kannattaa kuitenkin hallita omana kokonaisuutenaan. Jos tietoturvariskien hallinta sisällytetään osaksi muita riskejä jää yleensä tietoturvariskien käsitteleminen liian kapeaksi.



Kuva 7. Tietoturvariskien hallintaprosessi (ISO27005 2013, 22).

6.3.1 Toimintaympäristön määrittäminen

Tietoturvariskien arviointi aloitetaan määrittelemällä organisaation sisäinen ja ulkoinen toimintaympäristö. Organisaation toimintaympäristön ymmärtäminen on tärkeää, jotta voidaan tunnistaa sitä uhkaavat uhkatekijät ja haavoittuvuudet, jotka voivat aiheuttaa organisaatiolle vahinkoa. Organisaatioiden tulee kuvata toimintojen, palveluiden, prosessien, tietojärjestelmien ja tietovarastojen väliset riippuvuudet riittävällä tasolla. VAHTI 2/2016 ohje määrittelee, että sisäinen toimintaympäristö koostuu organisaation sisäisistä tekijöistä, joilla on vaikutusta organisaation toimintaan tavoitteiden saavuttamiseen. Ulkoinen toimintaympäristön koostuu organisaatioon vaikuttavista ulkoisista tekijöistä, joissa asiakkaiden ja ulkoisten sidosryhmien tarpeet ja vaatimukset otetaan huomioon organisaation toiminnassa. ISO27005 standardin mukaan ulkoiseen ja sisäiseen toimintaympäristöön voi kuulua seuraavia tekijöitä, jotka tulisi huomioida myös riskienhallinnan näkökulmasta.

Ulkoinen toimintaympäristö:

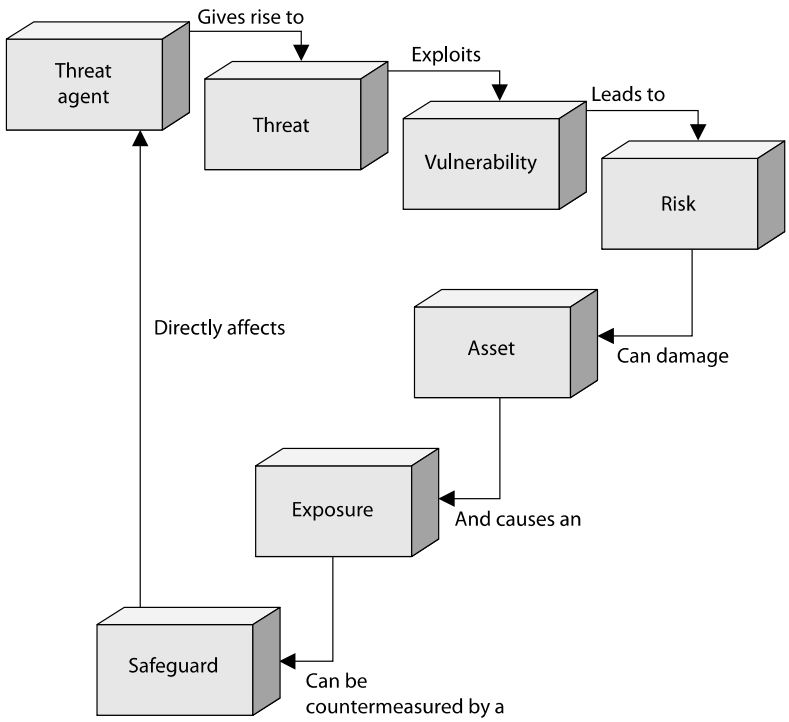
Ulkoinen toimintaympäristö voi koostua kansainvälisestä ja kansallisesta ympäristöstä. Sitä voi ohjata politiikka, lainsäädäntö, viranomaismääräykset ja erilaiset yhteiskunnalliset piirteet. Ulkoiseen toimintaympäristöön vaikuttavat myös rahoitusta, kilpailukykyä ja taloutta ohjaavat tekijät. Myös suhteet ulkoisiin sidosryhmiin ja niiden arvoihin voivat vaikutta organisaation toimintaympäristöön, joka vaikuttaa organisaation toimintaan organisaation ulkopuolelta. (ISO27005 2013, 12).

Sisäinen toimintaympäristö:

Sisäiseen toimintaympäristöön vaikuttavat yrityksen yleinen hallintotapa, organisaation rakenne ja erilaiset roolit ja vastuut. Strategia ja sen asettamat tavoitteet ohjaavat sisäisen toimintaympäristön toimintaa ja ne tulisi ottaa myös huomioon, kun organisaation tietoturvaa kehitetään. Sisäisten sidosryhmien näkemykset ja arvot vaikuttavat organisaation yleisen toimintakulttuurin lisäksi. (ISO27005 2013, 12).

6.3.2 Riskien arviointi

Riski toteutuu, jos uhkat yhdessä haavoittuvuuksien kanssa aiheuttavat taloudellisia seuraamuksia. Ilman uhkia haavoittuvuudet tai haavoittuvuudet ilman uhkia eivät aiheuta riskiä. On tärkeää ymmärtää, että riskienhallinnan näkökulmasta riski on seurausta uhkien toteutumisesta yhdessä haavoittuvuuksien kanssa. Yleensä riskiksi käsitetään uhka, haavoittuvuus tai poikkeama. (Valtionvarainministeriö 28/2016, 35).



Kuva 8. Uhkien ja haavoittuvuuksien suhde riskeihin (Harris Maymi 2016, 9).

Uhkien aiheuttajat synnyttävät uhkia, jotka mahdollistavat haavoittuvuuksien hyväksikäyttämisen. Uhkien ja haavoittuvuuksien yhdistelmä johtaa riskeihin, jotka voivat altistaa suojattavan omaisuuden vahingoittumiselle. Riskejä vastaan voidaan suojautua vastatoimilla ja hallintakeinoilla. Turvatoimet vaikuttava suoraan uhkien aiheuttajiin. (Harris Maymi 2016, 8). Näin ollen myös uhkien aiheuttaja kehittävät jatkuvasti toimintaansa ja luovat uusia uhkia ja pyrkivät tunnistamaan uusia haavoittuvuuksia, joita hyödyntämällä löytävät keinoja päästä käsiksi kohteena olevan organisaation tieto-omaisuuteen tai vahingoittamaan sitä.

Riskien arvioinnissa tulee riskit arvioida määrällisesti tai laadullisesti. Molemmissa lähestymistavoissa on omat hyvä ja huonot puolensa. Organisaation tulee valita sille sopivin tapa arvioida riskit. Määrällisessä menetelmässä laskenta voi olla monimutkaista ja voi olla hankalaa ymmärtää mihin arvoihin laskenta perustuu. Määrällinen lähestymistapa vaatii myös paljon lähtötiedon keräämistä ja ilman tehokkaita automaattisia työvälineitä voi arviointi olla työlästä. Laadullisessa menetelmässä laskentaa ei käytetä ja tulos voi olla subjektiivinen mielikuviin perustuva. Näin ollen se ei mahdollista kustannusten ja hyötyjen arvioimista rahassa ja lopputuloksen perustella tietoturvabudjetin laatiminen voi olla hankalaa. Toisin sanoen määrällinen lähestymistapa voi olla miltei mahdoton toteuttaa ja laadullinen tapa ei anna riittävästi tietoa taloudellisten päätösten tekemiseen. Tästä syystä molempien lähestymistapojen yhdistäminen voi olla paras tapa toteuttaa riskien arviointi. (Harris ja Maymi 2016, 118-119). Arvioinnissa riskit asetetaan tärkeysjärjestykseen vakavuuden ja asetettujen arviointikriteerien mukaisesti. Tämä auttaa organisaatiota priorisoimaan ne riskit joiden käsittelyllä on suurin merkitys organisaation toiminnalle. Riskien arvioinnissa tunnistetaan suojattavat kohteet ja yksilöidään niihin kohdistuvat uhkat ja mahdolliset olemassa olevat haavoittuvuudet. Suojattava kohde on asia, jolla on arvoa organisaatiolle. Suojattavat kohteet eivät

siis ole pelkästään laitteistoja tai ohjelmistoja. Suojattavista kohteista on kerättävä riittävästi tietoja riskien arviointia varten. Suojattaville kohteille tulisi määritellä suoritettavan riskienarvioinnin laajuus, suojattavan kohteen omistaja, jolla on vastuu ylläpidosta, käytöstä, kehittämisestä ja turvallisuudesta, sekä suojattavan kohteen arvo organisaatiolle. Tuloksena syntyy lista suojattavista kohteista, joihin riskienhallinta ulottuu ja niiden tärkeydestä liiketoimintaprosesseille. (ISO27005 2013, 32-34).

Suojattavien kohteiden lisäksi tulee tunnistaa niitä uhkaavat uhkat. Uhka voi vahingoittaa suojattavia kohteita. Se voi olla luonnon tai ihmisen tahallisesti tai tahattomasti aiheuttama. On syytä huomioida, että uhka voi ilmetä organisaation sisällä tai sen ulkopuolella. Kaikki uhkat tulisi tunnistaa olipa ne sisäisiä tai ulkoisia. (ISO27005 2013, 34). Uhkat tulisi tunnistaa luokitella kategorioittain, sekä arvioida niiden todennäköisyys aiheuttaa vahinkoa organisaatiolle (Harris, Maymi 2016, 95). Tärkeää on keskittyä vai niihin uhkiin, jotka voivat kohtuullisella todennäköisyydellä toteutua ja aiheuttaa vahinkoa organisaatiolle. Organisaation on tärkeää tiedostaa mitä suojattavia kohteita sillä on joiden toimintaan ulkoiset tahot voivat vaikuttaa tai aiheuttaa keskeytyksen tai jopa tuhota sen. On tärkeää kohdentaa rajalliset resurssit oikeiden kohteiden suojamiseen oikeilla keinoilla. Organisaation tulisi tiedostaa mitkä ovat mahdolliset potentiaaliset vastustajat ja mitkä ovat heidän motivaationsa ja millainen kyvykkyys heillä on hyökätä organisaatiota vastaan. (Harris, Maymi 2016, 98-99).

Tunnistettujen uhkien jälkeen on tärkeää tunnistaa jo olemassa olevat hallintakeinot ja turvallisuustoimenpiteet, jotka ovat käytössä. On tärkeää myös todeta näiden hallintakeinojen toimivuus. Myös toimimaton hallintakeino voi olla itsessään haavoittuvuus, joka mahdollistaa uhkan toteutumisen. Hallintakeinojen vaikuttavuutta tulisi mitata, jotta niitä voidaan täydentää toisilla hallintakeinoilla. Kannattaa tarkkailla kuinka hallintakeino vähentää uhkan todennäköisyyttä tai pienentää uhkan toteuttamisen helppoutta. Toteutettuja hallintakeinoja tulisi arvioida samalla tavalla kuin suunnitteilla olevia uusia hallintakeinoja auditointien ja katselmuksien yhteydessä. Seuraamalla hallintakeinoja vältetään myös päällekkäisten hallintakeinojen toteutus ja näin ollen vältytään niiden aiheuttamilta turhilta kustannuksilta. (ISO 27005 2013, 36).

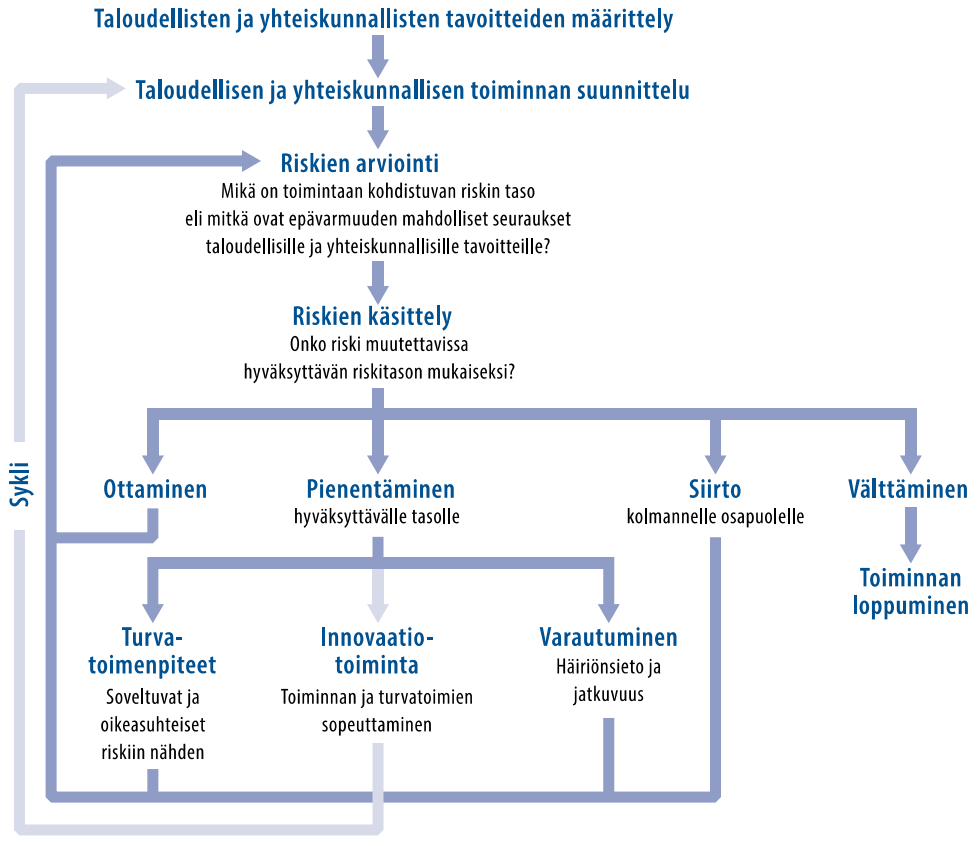
Myös haavoittuvuuksien tunnistaminen on tärkeää. Olemassa oleva haavoittuvuus ei välttämättä mahdollista minkään uhkan toteuttamista ja ei välttämättä juuri nyt vaadi mitään hallintakeinoa sen poistamiseksi. Tällaiset haavoittuvuudet ovat kuitenkin syytä tiedostaa, jotta muuttuneen tilanteen jälkeen niiden hallitsemiksesi voidaan valita sopiva hallintakeino. Huonosti toteutettu tai väärä hallintakeino voi itsessään olla myös haavoittuvuus, joka mahdollistaa uhkan toteuttamisen, joka ei muutoin olisi todennäköinen kyseisessä ympäristössä. Haavoittuvuudet eivät ole pelkästään tietojärjestelmiin ja sovelluksiin liittyviä. Haavoittuvuuksia voi olla organisaatiossa, prosesseissa, hallinnollisissa rutiineissa, henkilöstössä, fyysisessä ympäristössä ja riippuvuuksissa ulkoisiin sidosryhmiin.

Tarkoituksena on tunnistaa ne riskit, jotka voivat aiheuttaa tappiota ja selvittää miten, missä ja miksi tällainen tappio on mahdollinen. Riskien tunnistaminen tarkentuu mitä useammin

riskienhallintaprosessi on toteutettu ja päätökset riskien hallisemiseksi pohjautuvat kerättyyn tietoon.

6.3.3 Riskien käsittely

Riskien arvioimisen jälkeen riskit käsitellään ja tehdään päätökset, kuinka tunnistettuja riskejä käsitellään. Päätökset riksien käsittelystä tulisi perustua asetettuihin tietoturvatavoitteisiin ja ennalta tehtyyn toiminnan suunnitteluun. Riskienkäsittelyssä tehdään päätös riskien käsittelemisestä. Perusperiaatteiden mukaisesti päätetään, hyväksytäänkö riski sellaisenaan vai pienennetäänkö riskiä halutulle tasolle. Jos riskiä päätetään pientään, valitaan usein sopivia turvallisuustoimenpiteitä ja hallintakeinoja, joilla riskiä voidaan pienentää halutulle tasolle. Riskien vaikutusta voidaan myös pienentää kehittämällä häiriönsietoa ja tekemällä jatkuvuus ja palautumissuunnittelua. Riski voidaan siirtää myös kolmannen osapuolen hoidettavaksi, jolloin kyseeseen voisi tulla vakuutuksen ottaminen riskien varalle tai riski voidaan siirtää kokonaan kolmannelle osapuolelle sopimusteitse. Viimeisenä vaihtoehtona riski halutaan välttää, jolloin toiminta päätetään lopettaa riskin välttämiseksi. (Valtionvarainministeriö 28/2016, 38-39).



Kuva 9. Riskienkäsittely prosessi (Valtionvarainministeriö 28/2016, 38-39).

Tietoturvallisuuden toimintaan liittyvät päätökset tulisi toteuttaa siten, että riskienhallintaprosessi on siinä vahvasti mukana. Riskien arvioissa riskit tulisi käsitellä siten, että päästään tietoturvallisuudelle asetettuihin tavoitteisiin ja päämääriin.

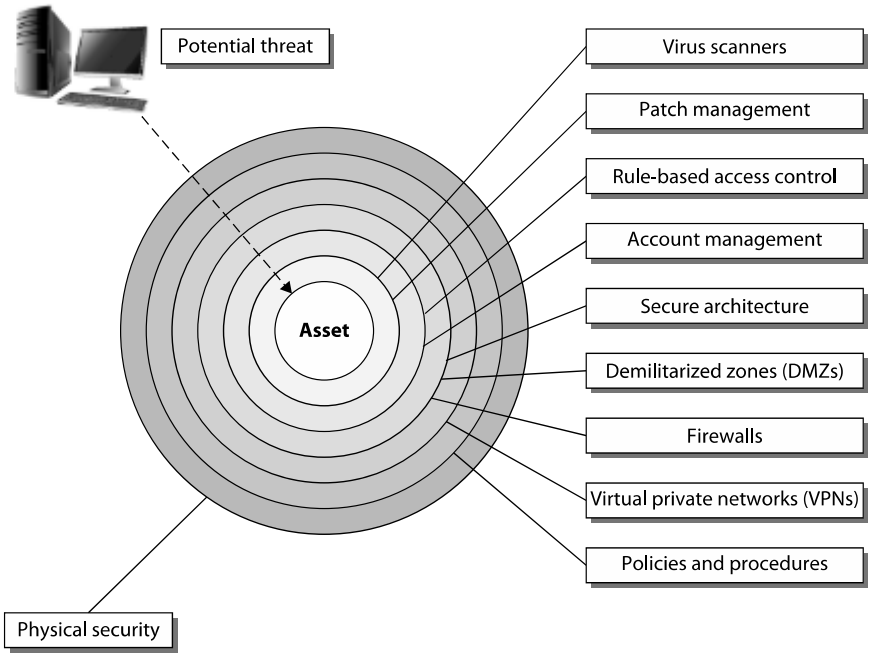
Isommissa organisaatioissa tietoturvariskien hallintaan tulisi käyttää jotain tunnettua viitekehystä. Näin voidaan varmistaa, että tietoturvariskien hallinta on koko organisaation kattavaa ja se

toteutetaan saman muotoisena organisaation kaikissa osissa. Valitun muodollisen viitekehyksen tulisi mukautua organisaation muun riskienhallinnan kanssa. Näin varmistetaan, että riskit käsitellään yhdenmukaisella tavalla ja ne ovat läpinäkyvästi esillä koko organisaation toiminnassa. (Valtionvarainministeriö 28/2016, 39).

Todellisten riskien mittaaminen voi olla hankalaa ja tästä syystä riskit kannattaa priorisoidaan ja aloittaa käsittely niistä riskeistä joilla saavutetaan eniten hyötyä pienimmillä panoksilla.

7 TIEOTURVALLISUUDEN HALLINTAKEINOT

Tietoturvallisuuden hallintakeinojen tehtävä on vähentää ja torjua riskejä, joita organisaatio kohtaa ja on tunnistanut. Sopivimmat hallintakeinot tulisi valita riskienhallinnan kautta. Tietoturvallisuuden hallintakeinot voidaan jakaa kolmeen eri osa-alueeseen hallinnollisiin, teknisiin ja fyysisiin kontrolleihin. Hallinnolliset kontrollit ovat enemmän johtamisen kautta tapahtuvia kontrolleja, jotka voivat liittyä riksien hallintaan, tietoturvan dokumentoimiseen, henkilöturvallisuuteen ja koulutukseen. Tekniset kontrollit on toteutettu, joko ohjelmallisesti tai laitteistopohjaisesti. Teknisiä kontrolleja voivat olla esimerkiksi keskitetty lokienhallinta, palomuurit, IDS ja IPS -järjestelmät, identiteetin- ja pääsyhallinnan järjestelmät. Fyysiset kontrollit puolestaan liittyvät usein tilojen, resurssien ja henkilöstön suojaamiseen esimerkiksi aidoilla, lukoilla, valaistuksella ja kameravalvonnalla. On tärkeää huomioida kaikki erilaiset hallintakeinot, jotta organisaatio pystyy saavuttamaan parhaan mahdollisen tietoturvallisuuden tason. Suojattava omaisuuden ympärille tulisi luoda useita hallintakerroksia, joiden avulla saavutetaan monikerroksinen suojaus, jota kutsutaan myös defence-in-depth malliksi. Tässä mallissa hallinnolliset, tekniset ja fyysiset kontrollit luovat päällekkäisiä suojauskerroksia, jotka on kuvattu kuvassa. (Harris, Maymi 2016, 8-10):



Kuva 10. Suojaavat kontrollit Defense-in-depth (Harris, Maymi 2016, 9).

Kerroksellisen suojaamisen avulla organisaatio pystyy tehokkaasti suojautumaan sitä uhkaavia riskejä vastaan. Yhden kerroksen pettäessä on vielä useita kerroksia, jotka suojaavat suojattavaa omaisuutta hyökkääjiltä. Erilaiset suojauskerrokset auttavat myös luomaan monikerroksisen havannointikyvyn, jolloin mahdolliset hyökkäykset pystytään paremmin havaitsemaan. Suojaavat kerrokselliset kontrollit tulisi valita siten, että ne on kohdistettu tunnistettuja uhkia vastaan. Suojaavien kerrosten lukumäärään vaikuttaa suojattavan omaisuuden arvo organisaatiolle ja suojattavan omaisuuden herkkyys.

On tärkeää ymmärtää mitä suojaavilla kontrolleilla tavoitellaan ja millaisia toiminnallisuuksia ne sisältävät. Harris ja Maymin mukaan kontrollit voidaan jakaa kuuteen osa-alueeseen toiminnollisuuksien mukaan. Nämä toiminnollisuudet lueteltu alla (Harris, Maymi 2016, 10):

- Ehkäisevä (Preventive)
- Tunnistava (Detective)
- Korjaava (Corrective)
- Varoittava (Deterrent)
- Palauttava (Recovery)
- Kompensoiva (Compensating)

Liitteen 1 taulukossa on esitetty kaikki ISO/IEC 27002 standardin hallintakeinot ja niille asetetut CIA –mallin mukaiset tavoitteet.

Suurin osa hallintakeinoista perustuu ennaltaehkäisyyn. On kuitenkin tärkeää ymmärtää, että kontrollien täytyy toimia hyvin yhteen ja niiden tulee olla toisiaan täydentäviä. Muutoin pahimmassa tapauksessa kontrollit ovat ristiriidassa keskenään ja voivat näin ollen aiheuttaa turvallisuusriskin. Harris ja Maymi kuvaavat alla olevassa taulukossa esimerkkejä erilaisista kontrollityypeistä ja niiden toiminnollisuuksista. (Harris Maymi 2016, 12):

	Ehkäisevä	**tunnistava**	**korjaava**	**varoittava**	**palauttava**
Fyysinen					
Aidat				X	
Lukitukset	X				
Tunnusjärjestelmä	X				
Vartija	X				
Biometriset järjestelmät	X				
Mies ansa ovet	X				
Valaistus				X	

Liiketunnistimet		X			
Valvontakamerat		X			
Maantieteellinen hajauttaminen					X
Hallinnollinen					
Tietoturvapolitiikka	X				
Monitorointi ja valvonta		X			
Tehtävien eriyttäminen	X				
Työnkierto		X			
Tiedon luokittelu	X				
Henkilöstömenettelyt	X				
Tutkimus		X			
Testaaminen	X				
Tietoturvallisuus koulutus	X				
Tekninen					
Pääsylista (ACL)	X				
Salaus	X				
Auditointi lokit		X			
IDS		X			
Anti Virus	X				
Serveri imaget			X		
Älykortit	X				
Takaisin soitto järjestelmä	X				
Varmuuskopiot					X

k

Taulukko 2. Kontrollit ja toiminnallisuudet (Harris Maymi 2016, 12).

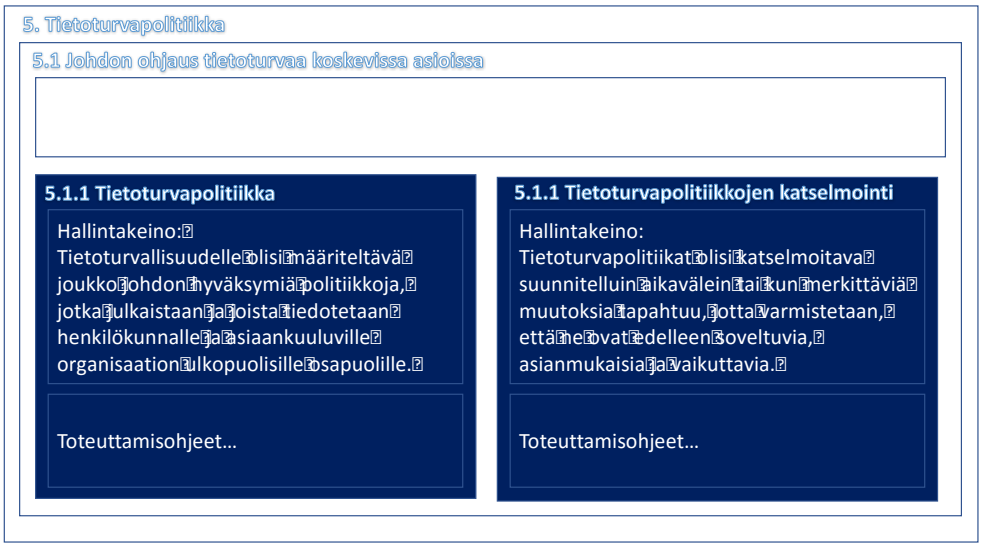
Turvallisuuskontrollien ja vastatoimien valinta kannattaa tehdä riskienhallinnan jälkeen. Alussa kontrolleilla pyritään saavuttamaan yrityksen tietoturvallisuuden perustaso (baseline), jota parannetaan riskienhallinnan kautta. Ensin luodaan kokonaisarkkitehtuurin näkökulmasta kontrollit, joilla huolehditaan kokonaisuuden tietoturvallisuuden toteutumisesta. Näin varmistetaan, kun tulee uusi järjestelmä tai sen osa, se on automaattisesti mukana organisaation kokonaisarkkitehtuurin tietoturvassa. Tietoturvallisuutta arvioitaessa uudelleen riskienhallinnan kautta voidaan peruskontrollien lisäksi luoda kontrollien yhdistelmiä tai luoda kokonaan uusia järjestelmäkohtaisia kontrolleja, joilla organisaation tietoturvan perustasoa nostetaan ylöspäin. Uudet kontrollit tulee myös dokumentoida, jolloin organisaatiolla säilyy käsitys mitä kontrolleilla suojataan ja mitä toimenpiteitä olisi lisättävä, jotta tietoturvallisuuden taso olisi riittävä. Dokumentointi on myös

tärkeää sen takia, että organisaatiossa kaikilla on sama käsitys mitä kontrolleja on käytössä ja mihin niillä pyritään. Jos tehdään muutoksia, ne täytyy myös viedä kaikkien osapuolien tietoisuuteen. Dokumentoidut kontrollit on myös helpompi integroida osaksi kokonaisuuden hallinnan ja seurannan suunnitelmaa. Dokumentoimattomat kontrollit menettävä yleensä tehonsa ja voivat pahimmillaan aiheuttaa huonosti toimiessaan tietoturvariskin. Kaikki turvakontrollit tulisi kohdistaa riskeihin joita on tunnistettu ja joita pyritään kontrollien avulla pienentämään halutulle tasolle. Kontrollien dokumentointi, raportointi ja toteuttamisvastuu tulisi kirjata osaksi tietoturvallisuuden kokonaissuunnitelmaa. Raportoinnin tarkoituksena olisi tunnistaa mitkä kontrollit toimivat tehokkaasti ja mitkä vaativat jatkokehitystä. Raportoinnin tuloksia voidaan hyödyntää riskienhallinnassa, kun se seuraavan kerran toteutetaan. Sen avulla voidaan arvioida ovatko kontrollit olleet riittäviä ja tarvitaanko riskien pienentämiseksi tehdä uusi tehostavia toimenpiteitä. Riskien ja kontrollien arvioimisen kautta saadaan päätöksenteon tueksi uutta tietoa, jolloin riskienhallinnasta vastaavat tahot pystyvät määrittelemään onko saavutettu hyväksyttävä riskitaso, jonka organisaatio pystyy kantamaan. Kontrollien tehokkuutta tulee seurata säännöllisesti, jotta pystytään reagoimaan muutoksiin. On myös tärkeä havaita, jos on syntynyt uusia uhkia tai vanhat uhat ovat muuttaneet muotoaa ja kontrolleja on muutettava tai tehtävä uusia kontrolleja uusien uhkien torjumiseksi ja riskien pienentämiseksi. (Harris Myami 2016, 128-130).

ISO/IEC 27002 standardi kuvaa tarkemmin ISO/IEC 27001 vaatimukset täyttävät hallintakeinot. Hallintakeinot on jaettu 14 pääkohtaan, joiden alle on koottu yhteensä 35 pääturvallisuusluokkaa. Pääturvallisuusluokat sisältävät hallintatavoitteet ja yhden tai useamman hallintakeinon tavoitteiden saavuttamiseksi. Kaiken kaikkiaan standardissa on kuvattu yhteensä 114 hallintakeinoa, jotka sisältävät kuvauksen, lyhyen toteuttamisohjeen ja mahdollisia lisätietoja. Standardissa ei määritellä yksityiskohtaisesti, kuinka hallintakeinot tulisi toteuttaa. Riskienhallinnan tukemana organisaatio pystyy valitsemaan riittävät hallintakeinot ja soveltamaan niitä omaan toimintaan. Pääkohdat on kuvattu alla olevassa kuvassa.

Kuva 11. Tietoturvallisuuden hallintakeinojen pääkohdat (ISO/IEC27002 2014).

Alla olevassa kuvassa on esimerkki, kuinka Tietoturvapolitiikka hallintakeinon pääkohta jakautuu pääturvallisuusluokkaan, jossa määritellään hallintakeinojen tavoite. Turvallisuusluokka on tässä tapauksessa jaettu kahteen hallintakeinoon, joiden toteuttamisesta on tarkemmat ohjeet standardissa.



Kuva 12. Esimerkki hallintakeinojen pääkohdan jakautumisesta hallintakeinoiksi (ISO/IEC 27002 2014, 14-16).

Organisaation valitsemat hallintakeinot dokumentoidaan ja ylläpidetään SOA dokumentissa (Statement of Applicability). SOA –dokumentti pitäisi syntyä riskienarvioinnin lopputuloksena. Siihen dokumentoidaan kaikki tietoturvakontrollit ja tavoitteet, joihin kontrolleilla pyritään. Dokumenttiin kirjataan lainsäädännölliset ja oikeudelliset vaatimukset, mahdolliset sopimukselliset velvoitteet, riskien hoitamisesta vastaava taho ja mahdolliset omat liiketoiminnan tarpeiden asettamat vaatimukset. Alla olevassa taulukossa on esitetty malli, kuinka aikaisemman esimerkin kontrollit voidaan dokumentoida.

Statement of Applicability

Current as of: DD/MM/YYYY

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection				Remarks (overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	Sec	Control Objective/Control							
5 Security Policies	5.1	Management direction for information security							
	5.1.1	Policies for information							
	5.1.2	Review of the policies for information security							

Taulukko 3. Statement of Applicability (ISO27k Toolkit 2016).

Liitteessä 2 olevassa taulukossa on esitetty SOA -mallin mukaisesti kaikki ISO/IEC 27002 hallintakeinot.

8 TIETOTURVA ORGANISAATIO

Tietoturvallisuuden hallinnassa on tärkeää määritellä organisaatio, joka vastaa tietoturvasta ja ymmärtää jokaisen organisaatioon kuuluvan vastuut ja velvollisuudet tietoturvallisuuden näkökulmasta. Tietoturvallisuuden tulee olla organisoitua toimintaa koko organisaation laajuudelta.

Hallitus (Board of Directors)

Organisaation hallitus hyväksyy organisaation tietoturvapolitiikan ja asettaa näin ollen organisaation tietoturvallisuudelle tavoitteet.

Ylin johto (Senior Management)

Organisaation ylin johto koostuu toimitusjohtajasta, liiketoimintajohtajista, talousjohtajasta ja tietohallintojohtajasta/päälliköstä. Johto koordinoi koko organisaation toimintaa vastamaalla visiosta ja strategisista päätöksistä. Toimitusjohtaja valvoo organisaation toimintaa, strategista suunnittelua, organisaation taloutta ylätasolla. Ylin johto asettaa myös strategiset tavoitteet tietoturvaa hoitavalle organisaatiolle. Yleensä nämä tietoturvallisuuden ylätason tavoitteet kuvataan tietoturvapolitiikassa. Ylin johto huolehtii myös, että organisaatiolla on riittävät resurssit ja edellytyksen tietoturvatavoitteisiin pääsemiseksi. Ylin johto asettaa tietoturvavastuun siitä vastaavalle taholle. Yleensä organisaation tietoturvasta vastaa tietoturvapäällikkö.

Tietohallintojohtaja (Chief Information Officer)

Vastaa organisaation tietojärjestelmien ja teknologioiden käyttämisestä ja hallinnoimisesta strategisella tasolla. Huolehtii omalta osaltaan liiketoimintojen ja tietohallinnon välisestä yhteistyöstä strategisella ja taktisella tasolla. Tietohallintojohtaja huolehtii organisaation kokonaisarkkitehtuurin hallinnasta. Huolehtii, että liiketoimintojen ja tietohallinnon välillä on riittävä vuorovaikutus. Tavoitteena on auttaa organisaation tavoitteiden saavuttamisessa ja vision toteuttamisessa. Tietohallintojohtaja vastaa organisaation kokonaisarkkitehtuurin hallinnasta. Tietohallintojohtaja huolehtii, että organisaation ydinarkkitehtuurin tieto-, sovellus- ja teknologia arkkitehtuurit integroidaan osaksi liiketoiminta arkkitehtuuria. ICT -arkkitehtuuri on tänä päivänä liiketoiminta-arkkitehtuurin perus edellytys. Erilaisten ekosysteemien, asiakkaiden ja kumppanien yhdistäminen vaatii lähes aina toimivaa ICT -arkkitehtuuria. IT for business kuvaa alla kokonaisarkkitehtuurin hallintaprosessin. (IT for business 2016, 78-80):

Kuva 13. Kokonaisarkkitehtuurimallin hallintaprosessi (IT for business 2016, 79).

Tietohallintojohtaja huolehtii yhdessä IT:stä huolehtivan kontrollerin kanssa IT-palveluiden taloudellisesta arvioinnista ja toimii linkkinä taloushallinnon ja tietohallinnon välissä. Vastaa IT-palveluiden taloussuunnittelusta ja seurannasta ja on mukana päätöksenteossa liittyen IT hankintoihin ja osallistuu IT palveluiden ohjaukseen.

Tietohallintojohtaja huolehtii organisaation strategisten tavoitteiden toteuttamisesta tietohallintostrategiassa. On tärkeää, että tietohallintojohtajalla on riittävät tiedot nykypäivän teknologioista ja niiden hyödyntämisessä liiketoimintarpeiden täyttämisessä. On myös tärkeää, että tietohallintojohtajalla on riittävän kattava ymmärrys organisaation liiketoiminnoista.

Tietohallintojohtaja huolehtii organisaation tietoturvaohjelman toteuttamisen onnistumisesta. Tietohallintojohtaja kommunikoi toimitusjohtajan ja johtoryhmän kanssa, sekä raportoi tietoturvallisuuden ja tietosuojan tilannakuvasta heille. Se välittää myös johdon ja johtoryhmän asettamat tavoitteet IT –organisaatiolle. (Harris Maymi 2016, 201).

Tietoturvapäällikkö (Chief Information Security Officer)

Tietoturvapäälliköllä on tietoturvallisuuden kokonaisvastuu tietoturvallisuuden operatiivisesta toiminnasta. Tietoturvapäällikön tehtävä on huolehtia, että organisaation tieto-omaisuus on suojattu riittävällä tasolla luotettavuuden, eheyden ja saatavuuden näkökulmasta. (ISO27003, 104). Tietoturvapäällikön tehtävä on tukea tietohallintoa tietoturva-asioissa. Tietoturvapäällikkö huolehtii, että tietoturvallisuus riskit ovat avioitu ja tarvittavat toimenpiteet riskien käsittelemiseksi on toteutettu. Tietoturvapäällikön tehtävä on huolehtia tietoturvallisuuden hallintajärjestelmän toiminnasta ja kehittämisestä. Tietoturvapäällikkö varmistaa, että liiketoiminnat ja tietohallinto lainsäädännön ja ulkoisten toimijoiden asettamat vaatimukset toteutuvat toiminnassa tietoturvan ja tietosuojan näkökulmasta. Tietoturvapäällikkö vastaa konsernin tietoturvaohjeistuksen laatimisesta

ja päivittämisestä ja tietoturvallisuuden valvonnasta hallinnollisesta ja teknisestä näkökulmasta. Tietoturvapäällikkö huolehtii, että toteutetut tietoturvaa parantavat ratkaisut on toteutettu hyväksi koettujen ajanmukaisten ratkaisuiden avulla. Tietoturvapäällikkö huolehtii, että järjestelmien kehittämisessä ja hankinnoissa otetaan organisaation tietoturvavaatimukset huomioon ja järjestelmien pääkäyttäjät, tiedon omistajat ja projektiin osallistuvat ulkoiset tahot ovat tietoisia näistä vaatimuksista. Tietoturvapäällikkö tekee tiivistä yhteistyötä tietohallintojohtajan kanssa tavoitteiden toteuttamisessa ja tietoturvan tilannekuvan raportoimisesta johdolle. Tietohallintojohtaja raportoi säännöllisesti ylimmälle johdolle organisaation tietoturvallisuuden tasosta.

Tietosuojavastaava (Chief Privacy Officer)

Tietosuojavastaavan tehtävä on koordinoida tietosuojavaatimusten toteuttamista organisaatiossa. Se huolehtii, että organisaatiolla on riittävät tietosuojakontrollit, jotka on dokumentoitu ja katselmoidaan säännöllisin väliajoin. Tietosuojavastaa vastaa, että organisaation sensitiivinen data joka sisältää henkilötietoja on turvassa. Se huolehtii myös, että organisaatiossa on tietosuoja-asetuksen mukaiset toimintamallit, joilla tietoa käsitellään koko sen elinkaaren ajan. Tietosuojavastaava osallistuu tiedonhallintaohjeistuksen määrittelemiseen, jolla kuvataan, kuinka dataa kerätään, käytetään, suojataan, arkistoidaan, annetaan kolmansien osapuolien käyttöön ja lopulta tuhotaan. Huolehtii myös järjestelmien pääkäyttäjien tietosuoja-asioiden tiedottamisesta ja osallistuu tarvittavan tietosuojakoulutuksen järjestämiseen. Tietosuojavastaava muodostaa tilannekuvan tietosuojasta ja osallistuu johdon raportointiin tietoturvan osana. Tietosuojavastaava varmistaa myös, että organisaation prosessit ottavat huomioon tietosuojavaatimukset. Tietosuojavastaava kuuluu omana osana tietoturvallisuuden organisaation. Tietosuojavastaavalla tulee olla riittävät tiedot tietosuojan lainsäädännöllisistä ja sääntelyn asettamista vaatimuksista. (Harris Maymi 2016, 202).

Järjestelmien pääkäyttäjät (System owner)

Järjestelmien pääkäyttäjät vastaavat yhden tai useamman järjestelmän riittävästä tietoturvan toteutumisesta kontrollien, käyttäjähallinnan, etäyhteyksien ja järjestelmäpäivitysten osalta. Pääkäyttäjät huolehtivat, että järjestelmien haavoittuvuudet on arvioitu raportoitu poikkeamista vastaavalle ryhmälle. Pääkäyttäjät ovat mukana tietojärjestelmien hankinnassa ja kehityshakkeissa, joissa huolehtivat ohjelmistojen ja järjestelmien turvallisuuden toteutumisesta. (Harris Maymi 2017, 204).

Tiedon omistaja (Data owner)

Tiedon omistaja kuuluu yleensä osaksi tiettyä liiketoimintaa, jossa vastaa jonkun tietyn tieto-omaisuuden suojaamisesta. Tiedon omistajan tehtävä on huolehtia, että kyseinen tieto säilyttää eheyden ja luottamuksellisuuden. Tiedon omista yleensä osallistuu tiedon luokittelemiseen vastuullaan olevan datan ja liiketoiminnan näkökulmasta. Tiedon omista huolehtii, että riittävät

kontrollit tiedon suojaamiseksi on toteutettu ja kriittinen data on varmistettu ja suojattu riittävällä tasolla. Tiedon omistaja ei ole tekninen IT organisaation kuuluva henkilö vaan hän on johonkin liiketoimintayksikköön kuuluva henkilö. Tarvittaessa liiketoimintahenkilö tulee kouluttaa tiedon omistajan rooliin, jotta hänellä on riittävät edellytykset hoitaa omaa rooliaan. Tiedon omistaja vastaa myös tietosuoja-asetuksen vaatimusten toteutumisesta ja dokumentoimisesta omistamansa tiedon osalta. (Harris Maymi 0271, 203-204).

Tiedon hoitaja (Data Custodian)

Tiedon hoitaja huolehtii datan ylläpidosta ja suojaamisesta. Tiedon hoitaja kuuluu yleensä IT organisaatioon ja huolehtii tiedon varmuuskopioimisesta ja varmuuskopioiden testaamisesta. Se osallistuu tietoturvakontrollien määrittelyyn ja toteuttamiseen. Osallistuu myös datan suojaamiseen liittyvän ohjeistuksen ja dokumentoinnin tekemiseen. (Harris Maymi 2017, 204).

9 TIEOTURVALLISUUDEN MITTAAMINEN

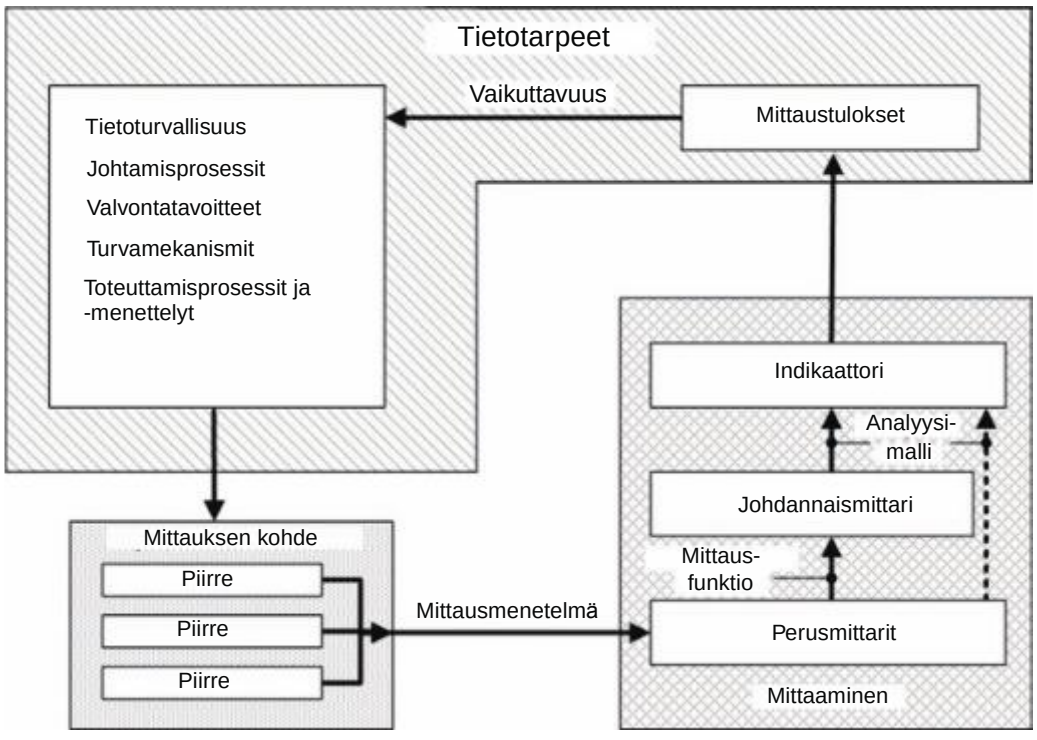
Ennen tietoturvan tason mittaamista organisaation tulee kehittää tietoturvallisuusohjelma, joka jalkautetaan organisaation toimintaan. Jos organisaatiolla ei ole tietoturvapolitiikkaa, joka on jalkautettu organisaation toimintaan, on mittaaminen mahdotonta. Mittaamisen tulee olla suorituskykyä mittaavaa ja tulee olla toistettavaa ja luotettavaa. Dataa mittaamiseen tulee kerätä toistuvasti, jolloin muutokset kehityksessä kyetään havaitsemaan. Mittausdataa tulee kerätä lukuisista eri lähteistä. Mittausdataa voidaan kerätä esimerkiksi erilaisista käsitellyistä järjestelmälokeista, poikkeama raporteista (incident response report), tarkistuslokeista (audit log), auditointiraporteista ja riskien arvioinnista. Mittaamisen tulokset tulee esittää kohderyhmän mukaan aina sopivassa muodossa. Ylin johto haluaa yleensä kosteen, joka esittää tietoturvan kokonaistilanteen organisaatiossa. Teknisille ihmisille raportin tulee olla riittävän yksityiskohtainen, jotta he voivat sitä paremmin hyödyntää omaan toimintaansa ja sen kehittämiseen. (Harris Myami 2016, 162).

Tietoturvallisuuden mittaamisella tavoitteena on arvioida tietoturvakontrollien ja turvamekanismien yhdistelmien tehokkuutta ja vaikuttavuutta. Sen avulla pyritään todentamaan kuinka laajasti turvallisuusvaatimukset täyttyvät organisaation toiminnassa. Tavoitteena on myös parantaa tietoturvallisuuden tasoa yleisiin liiketoimintariskeihin nähden. Mittaamalla hankitaan myös lähtötietoja päätöksen teon tueksi ja johdon raportointia varten. Mittareiden määrittelemisessä tulisi huomioida tietoturvallisuuden merkitys liiketoiminnalle, lainsäädännön, viranomaisten ja sopimusten asettamien vaatimusten vaikutukset, tietoturvatoimien kustannusten suhde saavutettuihin hyötyihin, sekä organisaation riskien hyväksymiskriteerit. (ISO/IEC 27004 2009, 18).

9.1 Standardin valitseminen mittaamisen määrittelemiseksi

Mittaamisen tueksi kannattaa organisaation valita sopivin standardi, jonka avulla se määrittelee millaisilla mittareilla organisaatio mittaa tietoturvallisuuden toteutumisen tehokkuutta. On olemassa erilaisia teollisuudelle suunnattuja parhaiden käytäntöjen ohjeita tietotuvan mittaamiselle. Harris ja Maymi suosittelevat kahta eri standardia riippuen siitä millaisessa toimintaympäristössä organisaatio toimii. Jos organisaation on päättänyt, että se kehittää toimintaa ISO/IEC27001 vaatimusten mukaiseksi ja organisaation tavoitteena on kehittää tietoturvallisuuden hallintajärjestelmä ISMS, kannattaa sen valita ISO/IEC 27004:2009 mittaamisen määrittelemisen tueksi. Jos organisaatiolla, on toimintaa Yhdysvalloissa tai toimii yhteistyössä organisaation kanssa, joka toimii NIST määritelmien mukaisesti, on sopivampi standardi NIST SP 800-55, koska siinä on otettu huomioon Yhdysvaltojen hallinnon vaatimukset. Molemmat standardit määrittelevät mittaamisen kontrollien tehokkuuden näkökulmasta ja soveltuvat tietoturvallisuuden mittaamiseen hyvin. On tärkeää, kun mittaamista lähdetään tekemään, että se on johdonmukaista ja säännöllisesti toistuvaa. Mittareille tulee valita sopiva asteikko, jotta suoraan toisiin yhteydessä olevat mittarit ovat käyttökelpoisia keskenään ja tuloksia voidaan arvioida rinnakkain. (Harris Maymi 2016, 162-163).

ISO/IEC 27004 määrittelee mittausmallin alla olevassa kuvassa. Mittausmallin on tarkoitus kuvata prosessi, jolla tietoturvallisuuden piirteet muutetaan määrälliseksi arvoksi, joista saadaan muutettua indikaattorit päätöksen teon tueksi. Mittausmalli kokoaa olennaiset mittauskohteet tarpeen mukaan. Mitattavia kohteita voivat esimerkiksi olla tietoturvallisuus kontrollit, prosessit, projektit ja käytettävissä olevat resurssit. On tärkeää, että mittaaminen on tarkoituksen mukaista ja kaikki mittaaminen perustuu johonkin tarpeeseen. (ISO/IEC 27004 2009, 22):

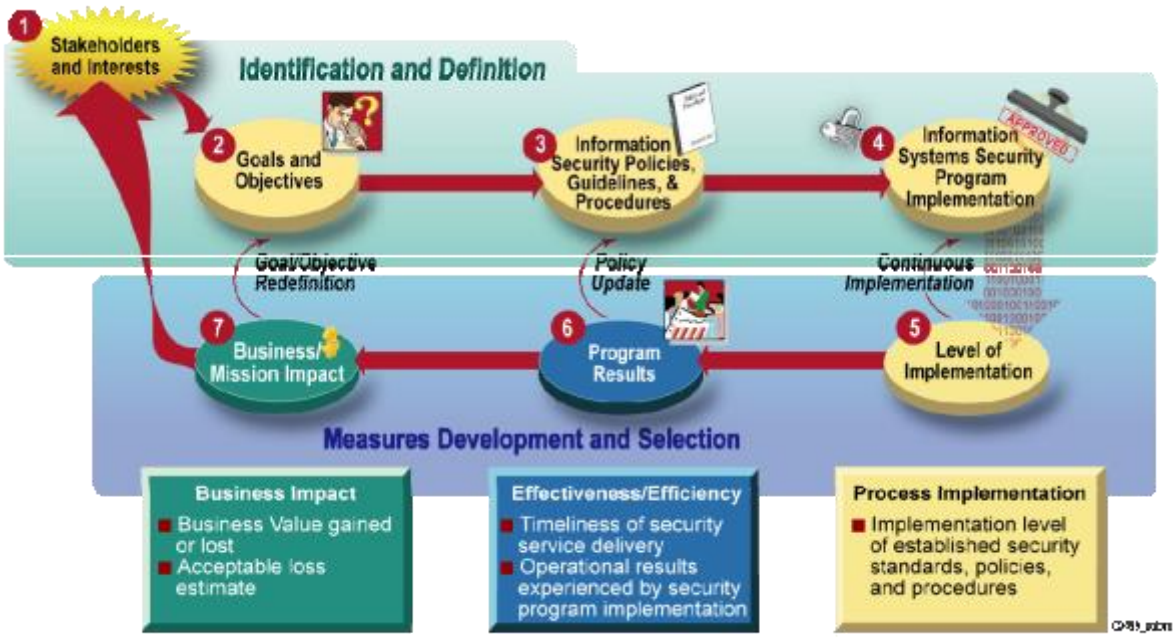


Kuva 14. Tietoturvallisuuden mittausmalli (ISO/IEC 27004 2009, 22).

Mittausmallissa turvamekanismeista tunnistetaan piirteet, joita voidaan mitata mittausmenetelmän avulla. Tuloksena saadaan perusmittareita. Perusmittareita voidaan käyttää sellaisenaan tai niitä voidaan yhdistää mittausfunktion avulla johdannaismittareiksi esimerkiksi keskiarvoon tai painokertoimeen perustuen. Johdannaismittarien ja perusmittarien arvoista muodostetaan indikaattoreita analyysimallin avulla. Analyysimallissa perus- ja johdannaismittarit yhdistetään arviointikriteereihin, joista saadaan tuloksena indikaattorit, joita tulkitsemalla laaditaan mittaustulokset. Arviointikriteerien avulla voidaan mittaustuloksista nähdä, vaatiiko mitattava kohde lisää toimenpiteitä, jotta asetettu tavoite saavutetaan tai vaaditaanko tarkempaa tutkimista mittaamisen luotettavuuden takaamiseksi. (ISO/IEC 27004 2009, 24-30).

9.2 Tietoturvallisuuden mittaamisen prosessi

NIST SP 800-55 määrittelee kuvan mukaisesti mittausten määrittelyprosessin. Sisäiset sidosryhmät määrittelevät päämäärät ja tavoitteet, joiden toimeenpanemiseksi organisaatiolle määritellä tieturvapolitikka, menettelytavat ja ohjeistukset, joilla tavoitteisiin pyritään pääsemään. Organisaation sisällä tällaisiin sidosryhmiin kuuluviksi voidaan laskea esimerkiksi tietohallintojohtaja, tietoturvapäällikkö, projektipäälliköt, talousjohtaja, järjestelmävastaavat, tietojärjestelmien pääkäyttäjät ja henkilöstöhallinto. Toisin sanoen tietoturvallisuuden tavoitteet ja päämäärät tulevat koko organisaation tarpeista. Organisaatiolle perustetaan tietoturvallisuuden kehitysohjelma. Mittaamisen määrittely aloitetaan, kun tietoturvan kehitysohjelma on implementoitu organisaation käyttöön. (NIST 2008,

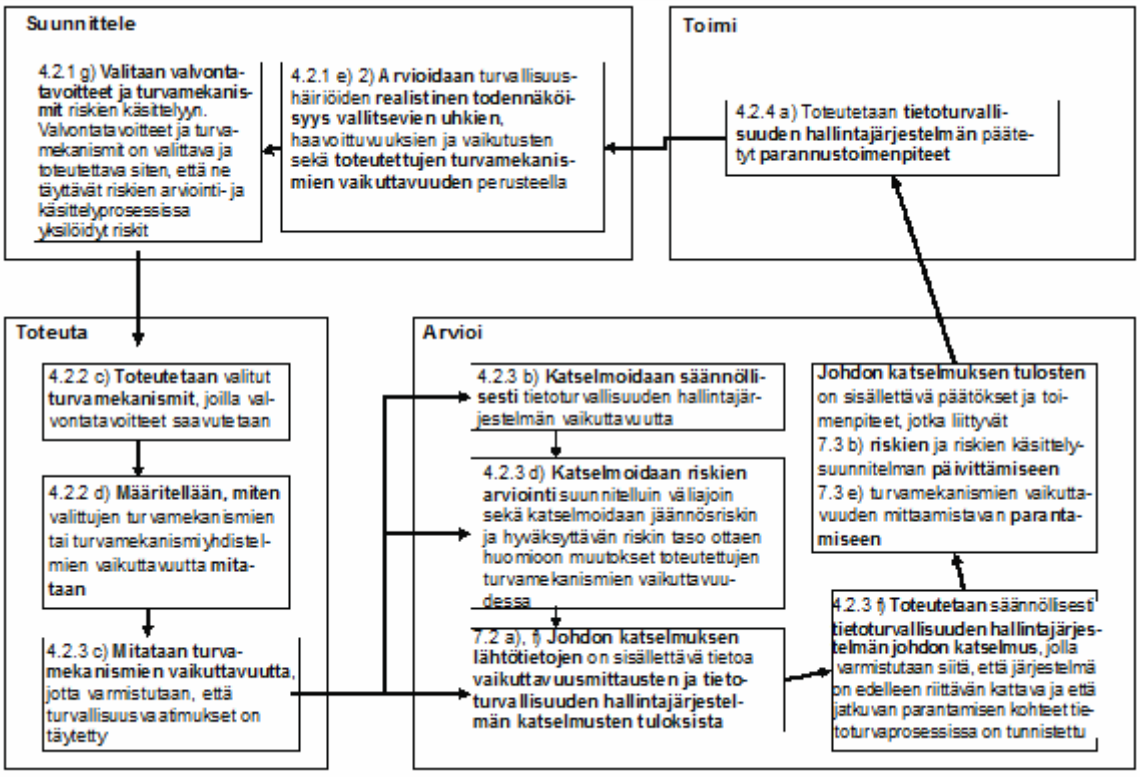


Kuva 15. Tietoturvallisuuden mittaamisen prosessi. (NIST 2008, 25).

Kehitysohjelman jälkeen voidaan aloittaa tietoturvallisuuden mittaamisen määritteleminen ja valitsemaan mittareita, joilla tietoturvallisuuden tilaa ja sen kehittymistä seurataan. NIST SP 800-55 määrittelee kolme näkökulmaa joita tulisi mitata. Prosessinäkökulmassa mitataan, kuinka hyvin tietoturvastandardien vaatimukset on otettu käyttöön ja kuinka politiikat ja menettelytavat vastaavat

vaatimuksia. Esimerkiksi voidaan mitata, kuinka monella tietojärjestelmällä on hyväksytty tietoturvasuunnitelma. Prosessimittarien tuloksien avulla tietoturvallisuus ohjelman kehittäminen tulisi olla jatkuvaa. Toisessa näkökulmassa mitataan tieturvakontrollien vaikuttavuutta ja tehokkuutta. Tarkoituksena on varmistaa, että tietoturvaprosessit ja tietoturvakontrollit ovat määritelty oikein ja ne toimivat riittävän tehokkaasti. Kontrollien mittaamisen avulla voidaan parantaa tietoturvapolitiikkaa ja ohjeistuksia ja tehostaa toimintaa tarvittaessa uusilla tietoturvakontrolleilla ja ohjeilla. Kolmannessa näkökulmassa arvioidaan vaikutuksia liiketoimintaan ja määritellään mikä on hyväksyttävä tappio riskin toteutuessa. Taloudellista vaikutusta seuraamalla pyritään pitämään tietoturvakontrollit oikein mitoitettuina ja kustannustehokkaina. Turvallisuuden valvonnan tai valvonnan vaikutusten tarkastelun sijaan liiketoimintavaikutusten mittaamisella pyritään arvioimaan tietoturvainvestointien suhdetta budjetointiin. (NIST 2008, 13-16).

ISO/IEC 27004 standardi esittää tietoturvallisuuden mittaamisen prosessin PDCA –mallin avulla.



Kuva 16. Tietoturvallisuuden mittaamisen prosessi (ISO/IEC27004 2009, 18).

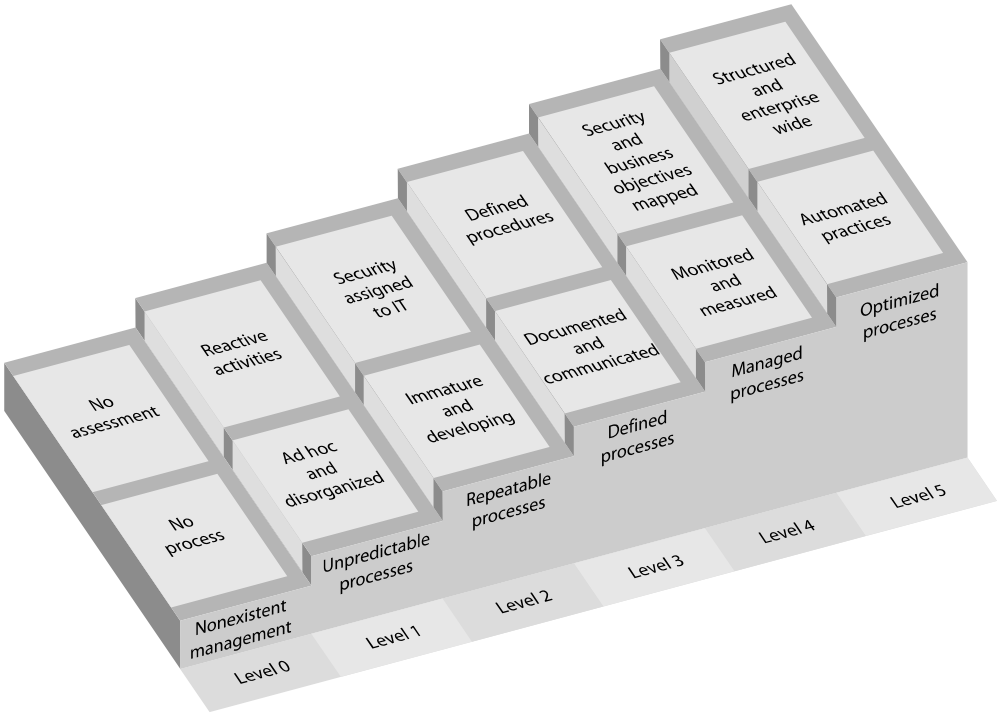
ISO27004 standardin mittaamisen prosessia on suunnittelu vaihe, jossa määritellään valvonnan tavoitteet ja turvallisuuskontrollit. Toteuttamisvaiheessa valitaan kontrollit ja määritellään kontrollien ja niiden yhdistelmien vaikuttavuuden mittarit. Mitataan tietoturvakontrollien vaikuttavuutta vaatimuksiin peilaten. Arviointi vaiheessa katselmoidaan mittaustuloksia säännöllisesti riskienhallinnan näkökulmasta ja raportoidaan johdolle. Katselmusten tuloksena päivitetään riskien käsittelysuunnitelmia ja huolehditaan, että tietoturvan jatkuvan kehittämisen vaatimukset täyttyvä. Toimintavaiheessa toteutetaan tietoturvallisuutta parantava toimenpiteet, joiden tulokset arvioidaan uudelleen alkavassa suunnitteluvaiheessa arvioimalla tietoturvariskien toteutumisen

todennäköisyyttä suhteessa toteutettujen tietoturvakontrollien vaikuttavuuteen. (ISO/IEC 27004 2009, 18-20).

9.3 Tietoturvallisuuden kypsyyden arvioiminen CMMI –mallin avulla

Organisaatiolle määritellään mittarit, joilla tietoturvallisuuden kehittymistä pyritään seuraamaan. Hyvä tapa mitata yrityksen tietoturvan toteutumista on arvioida säännöllisesti yrityksen tietoturvallisuuden kypsyyden tasoa. Hyökkäysyritysten ja niiden torjumisen määrän mittaaminen ei välttämättä anna todellista kuvaa yrityksen tietoturvallisuustasosta.

Itsearviointityökalun tuloksia ja nykytilan analyysin tuloksien perusteella määritellään tietoturvallisuuden hallintamallin kypsyyden taso ja asetetaan tavoitteet seuraavien vuosien tasolle. Harris Maymi esittelevät CMMI –mallin, jolla kypsyyttä voidaan arvioida viisiportaisella asteikolla. Asteikon avulla pyritään hahmottamaan, kuinka kehittynyt organisaation tietoturvallisuuden hallinta on. Arviointi tehdään prosessien näkökulmasta. Siinä pyritään arvioimaan kuinka hallittuja tietoturvallisuuden prosessit ovat ja onko toiminta dokumentoitu ja pyritäänkö prosessien toimintaa mittaamaan niiden toimivuuden varmistamiseksi. Ylimmällä tasolla toimita ulottuu koko organisaation leveydelle ja toiminta on hyvin automaattista ja optimoitua.



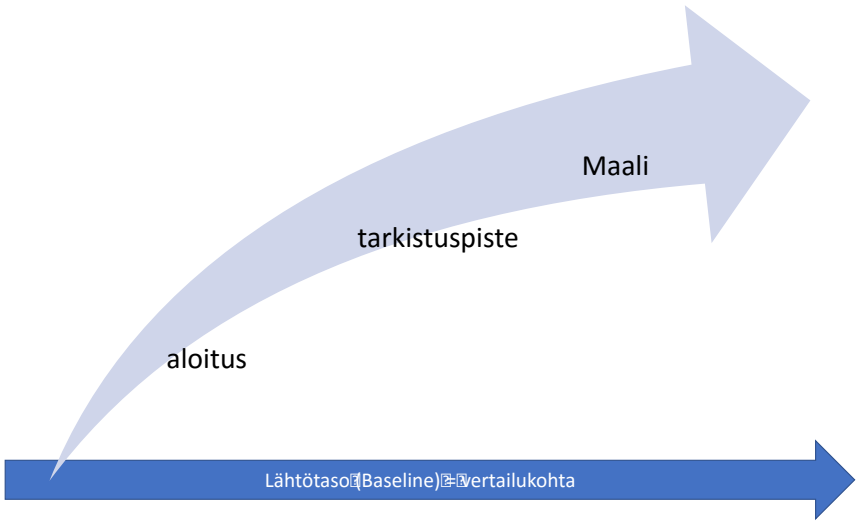
Kuva 17. CMMI –malli (Harris Maymi 2016, 39).

Yrityksen tulee arvioida toimintaa ja tietoturvallisuuden taso säännöllisesti. Arviointeja voidaan toteuttaa eritavoilla. Voidaan tehdä yrityksen sisäisiä arviointeja, joiden avulla pyritään mittaamaan yrityksen tietoturvan tasoa ja kehittymistä lyhyelle aikavälillä. Sen lisäksi voidaan teettää ulkoisia

arviointeja säännöllisin väliajoin. Ulkoiset arvioinnin toteuttaa organisaation ulkopuolinen taho, jotta arvioinnin riippumattomuus säilyy. (Valtiovarainministeriö 2014, 16).

10 TULOKSET

Tietoturvallisuuden hallintamallia ja tietoturvallisuus ohjelmaa, kun lähdetään toteuttamaan pitää alussa määritellä myös lähtötaso, joka toimii kehityksen aikana vertailupisteenä. Lähtötason määrittelemiseksi opinnäytetyössä on käytetty nykytila-analyysin, tietoturvallisuuden itsearviointityökalun tuloksia, sekä EQFM tietoturvavaatimusten arviointityökalu. Itsearviointityökalu ja EFQM vaatimusten arviointi työkalut ovat esitelty opinnäytetyön liitteenä. Työkaluista saatuja tuloksia ei voi esitellä tietoturvasyistä osana opinnäytetyötä. Lähtötason määrittelemisen jälkeen asetetaan organisaatiolle tavoitteet, joihin pyritään seuraavan kahden vuoden aikana. Tavoitteiden saavuttamisen välille on hyvä luoda tarkistuspisteitä, joissa tarkistetaan, että kehitys on menossa oikeaan suuntaan.



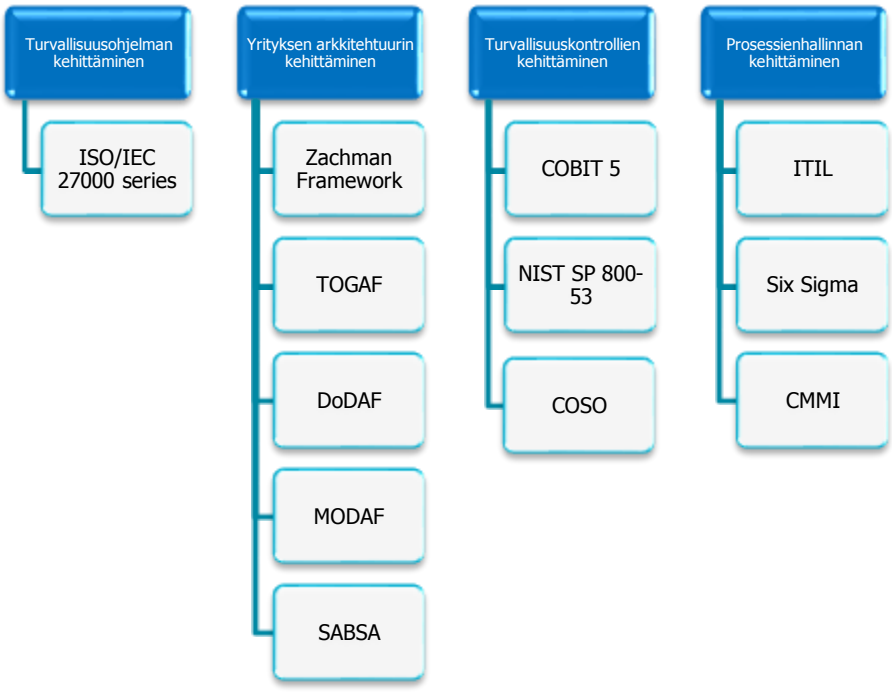
Kuva 18. Tietoturvallisuuden lähtötaso ja tavoitteiden asettaminen (Staf 2016, 27).

Savon Voimalle ensimmäisen vuoden tavoitteeksi asetettiin, että nykytila-analyysissä havaitut kriittiset välittömiä toimenpiteitä vaativat kohdat on käsitelty vähemmän kriittiselle tasolle. Seuraavien kahden vuoden aikana tavoitteena on tehdä toimenpiteitä joilla EFQM arviointityökalun tuloksissa organisaatio saavuttaa vähintään tietoturvallisuuden perustason kaikilla osa-alueilla.

10.1 Sopivien viitekehysten valinta

Tietoturvallisuuden hallintamallia, kun lähdetään kehittämään organisaation käyttöön kannattaa organisaation valita sopivimmat viitekehykset tukemaan kehittämistyötä. Viitekehykset ovat eri

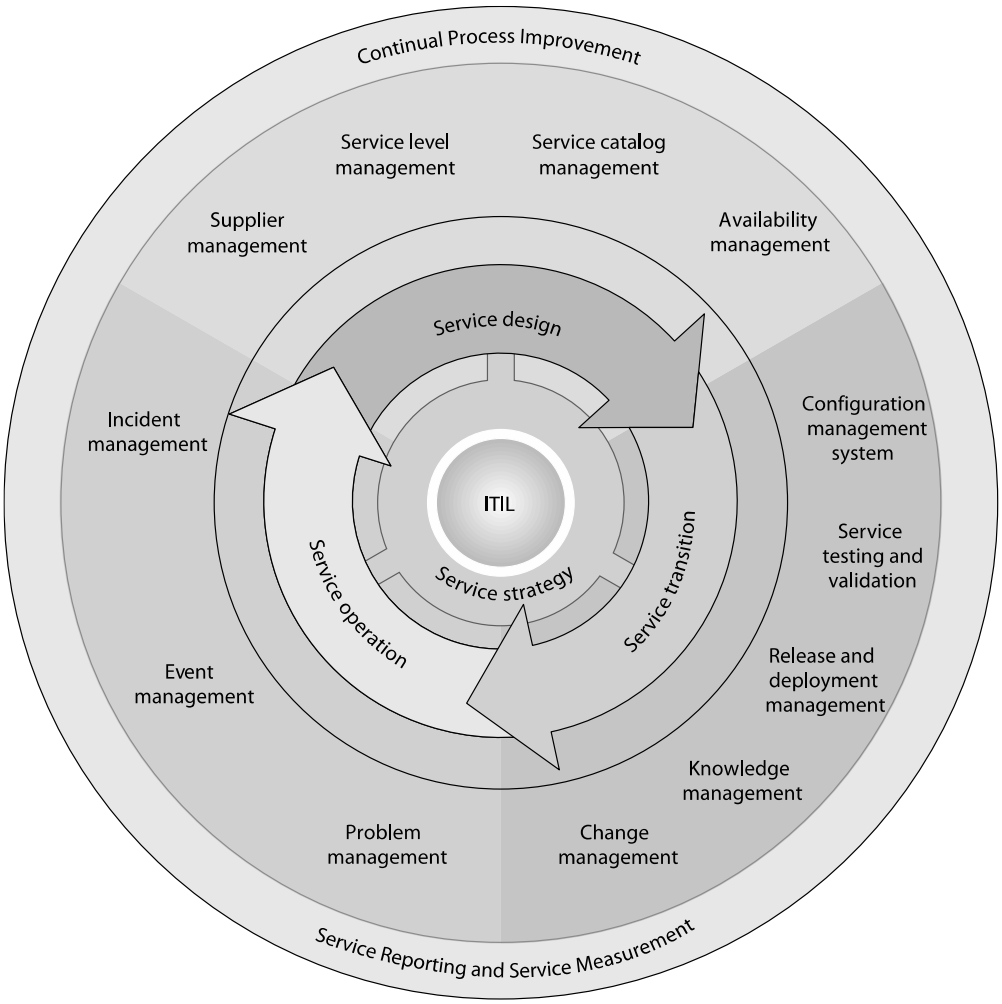
standardoimisjärjestöjen kehittämiä. On tärkeää tunnistaa mihin käyttöön eri viitekehykset on tarkoitettu. Useat viitekehykset menevät usein myös osittain päällekkäin. Viitekehyksillä on yleensä omat vahvuutensa eri osa-alueilla. Joten viitekehysten valintaan kannattaa käyttää aikaa. Harris ja Maymi esittävät yleisimpiä viitekehyksiä niiden roolien mukaan alla olevassa kuvassa.



Kuva 19. Eri viitekehykset ja niiden roolit (Staf 2016, 8).

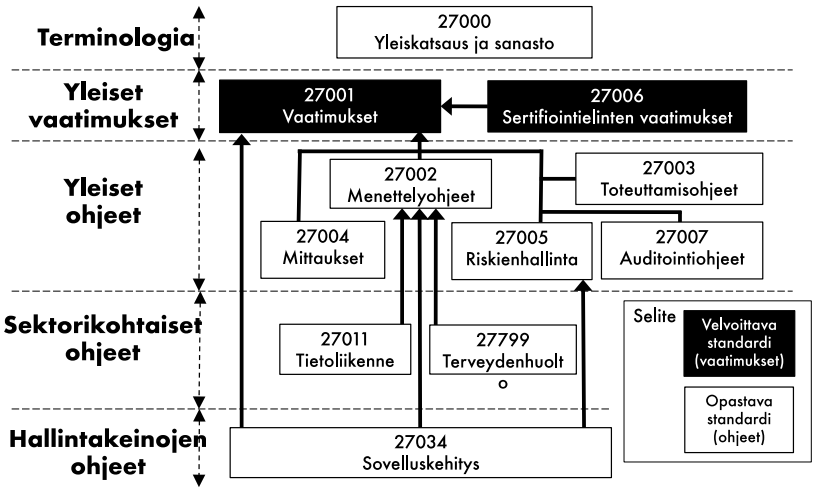
Savon Voiman ja ICT palveluita tarjoavan kumppanin väliset prosessit on kuvattu hyvin pitkälti ITIL standardin mukaisesti. ITIL on Suomessa ja Euroopassa varsin laajasti käytössä ja sen takia se on Savon Voimallekin luonteva tapa kehittää tietojärjestelmiin liittyvää palveluhallintaa ja sen prosesseja. ITIL:n avulla palvelutuottajan ja tilaavan organisaation palveluprosessit hioutuvat hyvin yhteen ja organisaatioilla on yhtenäinen näkemys kuinka eri prosessien tulisi toimia.

ITIL on alun perin kehitetty liiketoiminnan ja tietotekniikan yhteensovittamiseksi. Tarkoituksena on saada liiketoiminnoista ja ICT:stä vastaavat ihmiset keskustelemaan saamaa kieltä, jotta kumpikin osapuoli ymmärtäisi toistensa tarpeita paremmin. ITIL tavoitteena on jatkuva palveluhallinnan ja siihen liittyvien prosessien kehittäminen. ITIL ei kuitenkaan sisällä varsinaisia tietoturvallisuutta parantavia kontrolleja ja ei yksinään riitä tietoturvallisuuden kehittämisen avuksi. Se ainoastaan kuvaa tietoturvaan liittyvä prosesseja kuten poikkeuksien käsittelyprosessin (incident response process). (Harris Maymi 2016, 37-38). ITIL mukaiset prosessit on kuvattu kuvassa. (Harris Maymi 2016, 38):



Kuva 20. ITIL –malli. (Harris Maymi 2016, 38).

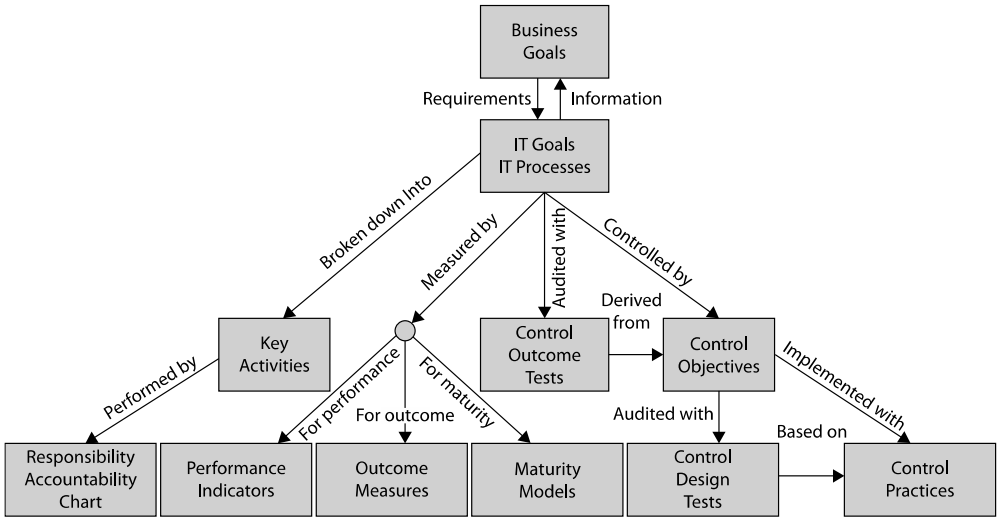
ISO27000 viitekehys sarja on yleisesti Suomessa ja Euroopassa tunnettu standardi ja monet tietoturvallisuuden auditoinnit pohjautuvat ISO27001 vaatimuksiin. ISO27000 sarja soveltuu Savon Voiman tietoturvallisuusohjelman rungoksi ja se auttaa ennen kaikkea kehittämään tietoturvan hallinnollisia kontrolleja. ISO27000 viitekehys sopii Savon Voiman tietoturvaohjelman rungoksi hyvin laajuutensa puolesta. Se ei kuitenkaan määrittele tarkkaan kuinka erilaisia tietoturvallisuuskontrolleja tulisi toteuttaa. Se keskittyy hyvin tietoturvallisuuden hallinnollisiin osa-alueisiin ja sopii näin ollen hyvin tietoturvallisuuden hallintajärjestelmän toteuttamisen avuksi.



Kuva 21. 27000 standardien väliset suhteet (SFS ry 2015, 22).

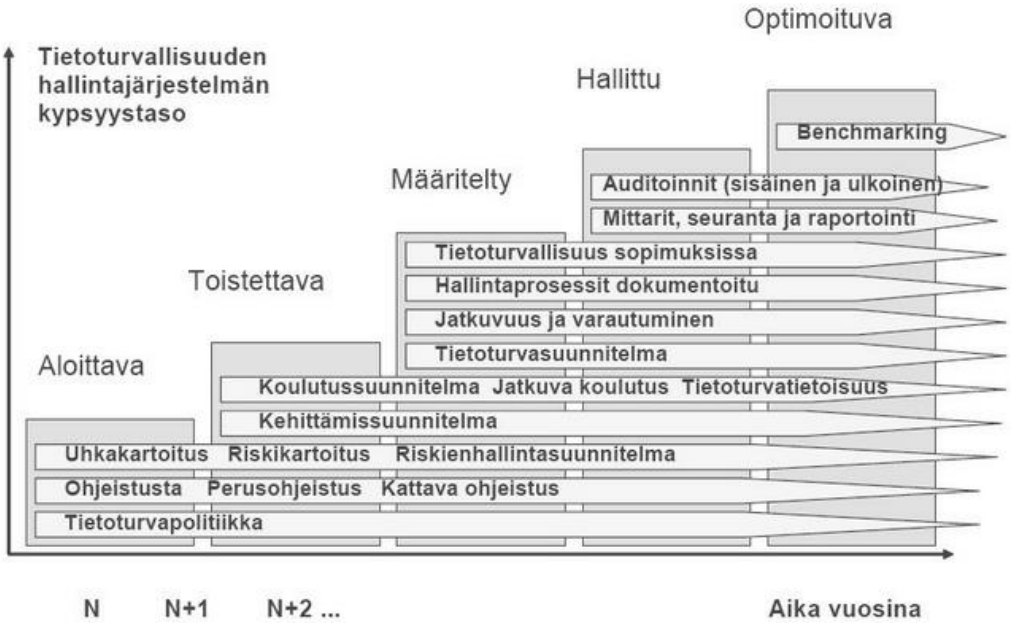
NIST SP 800-53 viitekehys auttaa parhaiten löytämään sopivimmat tavat toteuttaa tietoturvallisuus kontrollit. Tässä viitekehyksessä kontrollit on jaettu teknisiin, operatiivisiin ja hallinnollisiin kontrolleihin. Lisäksi kontrollit on määritelty tavoitteiden mukaan. Eli mihin CIA –mallin perustarpeen suojaamiseen sillä pyritään vaikuttamaan. Vaikuttaako se luottamuksellisuuteen, eheyteen vai saatavuuteen. Kontrollit on kuvattu ISO27000 sarjan kontrolleja tarkemmalla tasolla ja se antaa hyvinkin yksityiskohtaiset ohjeet, kuinka kontrollit tulisi vaatimusten mukaan toteuttaa. NIST on julkaissut yksityiskohtaisia parhaat käytännöt sisältäviä ohjeistuksia ja ne ovat ilmaiseksi kaikkien saatavilla.

COBIT viitekehyksen avulla voi yrityksen arkkitehtuuria kehittää niin, että tietoturvallisuuden hallinto ja johtaminen olisi huomioitu organisaation eri tasoilla mahdollisimman hyvin. Se auttaa määrittelemään organisaation sisällä tietoturvavastuut ja keskeiset kontrollit ja toiminnallisuudet, joista vastaava on velvoitettu huolehtimaan. Sen avulla myös liiketoimintojen ja IT organisaatioiden tavoitteet ovat helpommin sovitettavissa yhteen. COBIT avulla myös kontrollien testaamista ja mittaamista voidaan kehittää. COBIT viitekehyksen toimintaperiaate on kuvattu alla.



Kuva 22. COBIT viitekehys (Harris Myami 2016, 34).

CMMI malli voidaan hyödyntää, kun määritellään organisaation tietoturvallisuuden maturiteettia. Tietoturvallisuuden maturiteettia arvioidaan viisi portaisella asteikolla, jotka kuvaavat yrityksen tietoturvan tasoa ja kyvykkyyttä eri tietoturvan kehitysvaiheissa. Se havainnollistaa hyvin ja pelkistetyllä tavalla missä kehitysvaiheessa organisaatio on menossa. Sen avulla organisaation on helpompi määritellä, mikä on yleisellä tasolla organisaation tietoturvallisuuden kypsyystason tavoite, johon kehitys ohjelmalla pyritään esimerkiksi viiden vuoden aikana. Viisiportainen CMMI malli on kuvattu alla.

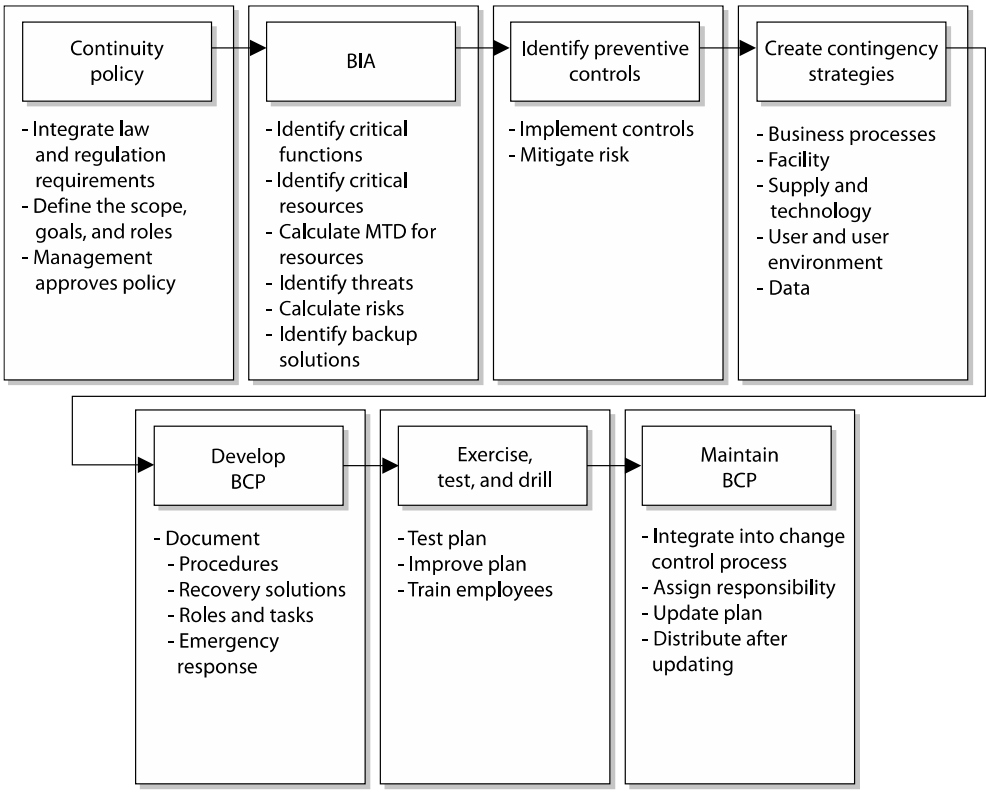


Kuva 23. CMMI malli. Tietoturvallisuuden maturiteetti (VAHTI 2006, 37).

Tietoturvallisuuden hallintamallin kehittämisessä ei kannata lähteä yksittäistä viitekehystä kirjaimellisesti toteuttamaan, vaan kannattaa määritellä mitkä tavat sopivat millekin organisaatiolle parhaiten. Hallintamallia suunniteltaessa on myös huolehdittava siitä, ettei mallista rakenneta hallinnollisesti niin raskasta mallia, ettei sitä kyetä toteuttamaan ja ylläpitämään olemassa olevilla resursseilla. Viitekehykset ovat siis hyvä apu tietoturvallisuuden kehitysohjelma pohjaksi.

10.2 Riskienhallinnan rooli tietoturvallisuuden kehittämisessä

Riskienhallinta on keskeisessä roolissa tietoturvallisuuden hallinnassa ja tietoturvallisuuden kehittämisessä. Riskienhallinnan kautta tulisi tehdä kaikki päätökset, jotka ohjaavat tietoturvallisuuden kehittämistä. ISO27001 vaatimukset edellyttävät, että tietoturvallisuuden hallinta noudattaa jatkuvan parantamisen mallia. Savon Voima saavuttaa jatkuvan oppimisen toimintakulttuurin parhaiten toteuttamalla tietoturvariskienhallinnan osaksi koko konsernin riskienhallintaa. Tietoturvariskit tulee käsitellä Savon Voima riskienhallintajärjestelmässä omana kokonaisuutena, noudattaen konsernin yleisiä riskienhallintaperiaatteita. Toteutettaessa tietoturvariskienhallinta osaksi riskienhallintajärjestelmää voidaan raportoida johdolle tietoturvan tilasta ja tehtävistä toimenpiteistä. Konsernin johdon tulee käsitellä riskienhallinnanraportti säännöllisin väliajoin ohjausryhmässä. Riskienhallintaperiaatteissa tulisi lisätä laajempi näkökulma tietoturvariskien hallinnan periaatteista. Tietoturvariskien arviointi tulee olla mukana asiantuntijoita kaikista liiketoiminta-alueista, jotta kaikki erityispiirteet tulee huomioitua riittävällä tarkkuudella ja riskien todennäköisyys ja vaikuttavuus voidaan arvioida. Liiketoimintojen tulee olla mukana arvioimassa riskien vaikutusta liiketoiminnalle. Myös keskeiset liiketoiminnoille kriittiset tietojärjestelmät tulee tunnistaa ja niille kannattaa tehdä BIA analyysi (business impact analysis). Analyysin avulla tunnistetaan liiketoiminnoille tärkeät tietojärjestelmät joihin ensisijaisesti tulisi turvallisuus toimenpiteet ja jatkuvuus suunnittelu kohdistaa. BIA analyysi auttaa organisaatiota tunnistaan kriittiset järjestelmät ja toiminnot ja priorisoimaan toimenpiteet kohdistumaan niihin. BIA –analyysi tulee olla osa myös liiketoiminnan jatkuvuuden hallintaa, joka on kuvattu alla. (Harris Maymi 2016, 134):



Kuva 24. BIA analyysi osana jatkuvuuden suunnittelua. (Harris Maymi 2016, 134).
Tietoturvallisuus tulee huomioida kaikissa kehityshankkeissa ja hankinnoissa. Savon Voimalla on käytössä kehityssalkkuohjelma, jossa kehityshankkeesta vastaavan projektipäällikön tulee ottaa kantaa, liittyykö hankkeeseen tietojärjestelmiä tai tiedon käsittelyyn liittyviä asioita. Tietoturvaryhmä käy säännöllisin väliajoin nämä hankkeet läpi ja varmistaa, että tietoturvallisuus on hankkeen määrittelyissä mukana ja tarvittaessa ohjaa hankkeen toteuttajia tietoturvallisuuden toteuttamisessa. Tarvittaessa kehityshankkeen tulee raportoida toteutetuista tietoturvallisuuden hallintakeinoista ja toimenpiteistä, joilla riittävä tietoturvallisuuden taso on hankkeessa saavutettu. Savon Voiman tulee kehittää myös tietoturva- ja tietosuoja liite osaksi kaikkia hankinta sopimuksia. Savon Voiman toiminta on erittäin riippuvainen kumppaniverkostoista, jotka käyttävät Savon Voiman järjestelmiä ja käsittelevät Savon Voiman tietoja Savon Voiman lukuun. On tärkeää huolehtia, että kaikilla kumppaneilla on tietoturvallisuus osana toimintaa ja velvoittaa heidät raportoimaan omasta tietoturvallisuuden tasosta.

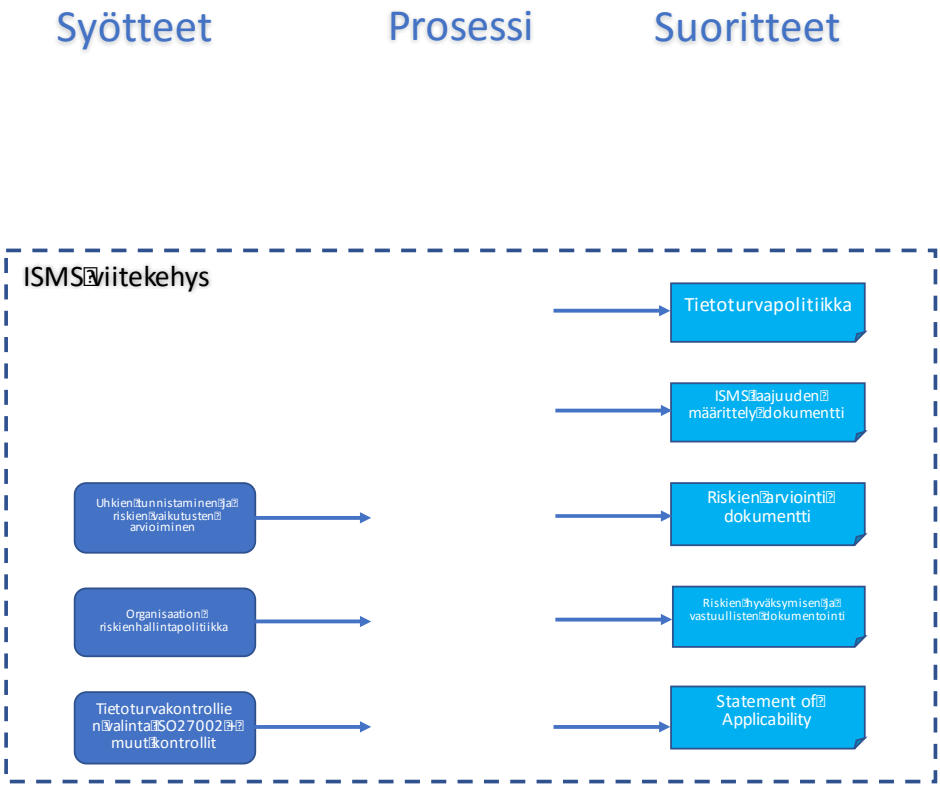
Savon Voiman tulee päivittää tietoturvapolitiikka vastaamaan tämän päivän vaatimuksia. Politiikka tulee myös katselmoida vuosittain johdon kanssa ja tarvittaessa siihen tehdään tarvittavat muutokset. Tietoturvapolitiikalla tulee olla hallituksen hyväksyntä. Keskeinen sisältö tietoturvapolitiikasta tulee viestiä koko organisaation laajuudella, jotta henkilöstö on tietoinen yrityksen tietoturvaperiaatteista ja pystyy näin ollen noudattamaan sitä. Tietoturvaan liittyvän viestintä tulee huomioida osana viestintäsuunnitelmia. NIS –direktiivi ja tietosuoja asetus edellyttävät tietoturvapoikkeamista viestimistä viiveettä kansalliselle valvovalle viranomaiselle ja tietosuojaloukkauksen kohteena oleville asiakkaille. Viestinnässä tulee noudattaa yhdenmukaisia käytäntöjä ja viestinnästä vastaavat tulee määritelty. Poikkeamista viestiminen tulee kuvata osana poikkeamien hallintaprosessia (incident response process). Siinä tulee ilmetä, kenellä on vastuu ilmoittaa poikkeamista valvovalle viranomaiselle ja kuinka se tulee tehdä. Ohjeistukseen kannattaa myös sisällyttää ohjeita, milloin poikkeamasta tulee tehdä rikosilmoitus poliisille. Eli millaisissa tapauksissa ollaan rikosoikeudellinen kynnys ylitetty.

Henkilöstön tietoturvakoulutuksesta tulee huolehtia järjestämällä säännöllisiä koulutuksia. Parhaiten säännölliset koulutukset voidaan toteuttaa koulutusportaalin avulla. Koko henkilöstön tulee suorittaa vuosittain itseopiskeluna tietoturvallisuus koulutus ja kysely portaalissa. Koulutukista laaditaan seurantaraportti, joka annetaan johdolle tiedoksi. Koulutusportaalin lisäksi henkilöstölle järjestetään tietoturva aiheisia tietoiskuja viikkoinfojen yhteydessä.

Uusien henkilöiden aloittaessa työt edellytetään tietoturvakoulutuksen läpikäyminen ja allekirjoitetaan salassapitosopimukset ja järjestetään riittävä perehdytys yrityksen tietoturvaperiaatteista ja käytännöistä ennen kuin heille annetaan pääsy tarvittaviin yrityksen tietojärjestelmiin. Henkilön työsuhteen päätyttyä tulee Savon Voimalla olla dokumentoitu määrämuotoinen prosessi työsuhteen päättämisestä. Prosessin tarkoitus on huolehtia, että henkilö on luovuttanut kaikki Savon Voiman tiedot ja välineet, joita hän on käyttänyt työssäoloaikana. Prosessissa huolehditaan myös, että henkilön tunnukset päätetään ja pääsy yrityksen verkkoon estetään viiveettä.

10.3 Jatkotoimenpiteet Savon Voiman tietoturvallisuuden kehittämisessä

Savon Voiman kypsyys on arvioitu olevan toistettavan ja määritellyn kypsyystason välimaastossa. Savon Voimalla on paljon toteutettuja tietoturvallisuuden hallintaan liittyviä toimenpiteitä ja menetelmiä. Hallintamenetelmien osalta osa on dokumentoitu varsin kattavasti ja osassa on merkittäviä puutteita, jotka on tunnistettu nykytila-analyysin ja itsearviointityökalun avulla. Savon Voimalla ei ole koko organisaation kattavaa tietoturvallisuuden hallintamallia ja paras tapa toteuttaa hallintamalli olisi lähteä toteuttamaan tietoturvallisuuden kehittämisohjelmaa, jonka tavoitteena olisi luoda ISO27000 standardin mukainen tietoturvallisuuden hallintajärjestelmä. ISO27000 standardin mukainen hallintajärjestelmä, vastaa myös hyvin tulevan verkko- ja tietoturvadirektiivin vaatimuksiin ja takaisi näin ollen Savon Voimalle hyväksyttävän riittävän tietoturvatason jota direktiivi edellyttää. Hallintajärjestelmän avulla tietoturvallisuus saadaan ulottumaan osaksi koko konsernin ja sen ulkoisten sidosryhmien toimintaan paremmin, koska hallinta olisi hyvin organisoitua ja säännönmukaista. Hajanaisten tietoturvallisuus kontrollien toteuttaminen eri puolilla organisaatiota ei tuota toivottua tietoturvallisuuden tasoa, eikä tietoturvallisuudesta synny riittävää kokonaiskuvaa. Ilman kunnollista hallintajärjestelmää ei organisaatiolle synny yhtenäisiä tietoturvakäytäntöjä, jotka toteuttaisivat organisaation tietoturvapolitiikassa asetettuja tavoitteita. Alla on kuvattu tietoturvallisuuden hallintajärjestelmän kehittämisprosessi ja siihen liittyvät syötteet ja suoritteet. Johdon tulee hyväksyä, että järjestelmä lähdetään toteuttamaan ja toteuttamiselle on varattu riittävät resurssit ja projektin toteuttamisen vastuut on jaettu.



Kuva 25. Tietoturvallisuuden hallintajärjestelmän toteuttamisen prosessi. (The ISO 27000 Directory, 2017).

Savon Voimalla on kattava kumppaniverkosto, jonka on otettava myös paremmin huomioon tietoturvallisuuden hallintaa kehitettäessä. Erilaisia ulkoisia sidosryhmiä on paljon ja tietoturvallisuuden hallinta niiden osalta voi olla haastavaa. Sen takia tietoturvallisuus on otettava laajemmin mukaan sopimuksissa ja toimintamalleissa. Sopimuksiin tulee liittää tietoturva- ja tietosuojaliite, jotka määrittelevät kumppanille tietoturvan ja tietosuojan näkökulmasta minimivaatimukset kumppanin roolin mukaan, jotka heidän tulee täyttää. Tärkeämpien kumppaneiden tietoturvallisuutta tulee myös arvioida järjestämällä kumppanien tietoturvallisuuden auditointeja. Kumppanien kanssa tulee myös tehdä kattavampaa yhteistyötä tietoturvallisuuden kehittämisen osalta. Tietoturvallisuuden taso voi olla myös yksi hankinnan kriteereistä laadun ja taloudellisten kriteerien lisäksi tulevaisuudessa. Tietoturvallisuuden lisääminen hankintatoimeen kannattaa toteuttaa hankintatoimen kehittämisprojektin yhteydessä, jolloin koko organisaatiolle muodostuu yhdenmukaiset käytännöt kumppanien tietoturvallisuuden toteuttamiselle.

Riskienarviontimallia tulee kehittää säännönmukaiseksi ja toistettavaksi malliksi. Tietojärjestelmien rooli tulee kuvata tarkemmin osaksi jatkuvuuden ja varautumisen suunnittelua. Eli on tunnistettava tarkemmalla tasolla mitkä tietojärjestelmät ja niitä yhteen liittävät tietoverkot ovat kriittisiä ja kuinka ne tulisi huomioida liiketoimintojen jatkuvuussuunnittelussa. BIA –analyysi auttaa tunnistamaan liiketoiminnoille tärkeät järjestelmät ja se kannattaa toteuttaa riskienhallinnan kehittämisen jälkeen.

Koulutusta tietoturvasta tulee lisätä koko organisaatiolle ja sen tulee olla osa vuosittaista toimintaa. Myös organisaation uusille henkilöille tulee perehdytyksen yhteydessä kouluttaa organisaation tietoturvallisuuden periaatteet ja käytännöt. Järjestelmien pääkäyttäjille tulee lisätä tietoturvallisuuskoulutusta, jotta he pystyvät paremmin vastamaan järjestelmien kehittämisestä tietoturvallisempaan suuntaa. Kriittisille tiedoille tulisi määritellä tiedon omistajat, joiden velvollisuus on huolehtia omistamansa tiedon luottamuksellisuudesta ja eheydestä.

Savon Voimalla on paljon erilaisia tuotantolaitoksia, sähköverkon verkosto- ja sähköasema-automaatiota ja kriittisiä automaatiojärjestelmiä, joiden suojaaminen vaatii syvällisempää osaamista myös järjestelmien toiminnasta. Näille kriittisille automaatiojärjestelmille ja niihin liittyville tietoverkoille tulee jatkossa tehdä myös säännöllistä tietoturvallisuuden teknistä testaamista. Näiden järjestelmien erityispiirteiden takia testaamiseen tulisi valita riittävän korkeatasoinen kumppani, jolla on aikaisempaa kokemusta ICS järjestelmien penetraatiotestaamisesta. Hallinnollisesta tietoturvallisuudesta huolehtiminen ja auditoiminen ei pelkästään riitä suojaamaan kriittisiä ympäristöjä, joten myös teknisiä tietoturvakontrolleja tulee kehittää ja testata säännöllisesti osana organisaation tietoturvallisuuden kokonaisuutta.

11 YHTEENVETO

Opinnäytetyön tavoitteena oli selvittää, millainen on hyvä tietoturvallisuuden hallintamalli ja millaisista osa-alueista se kostuu. Hallintamallin rakenne ja osa-alueet saatiin selvitettyä hyvin. Hallintamallin rakenne osoittautui työn edetessä laajajemmaksi kuin alussa osasi määritellä. Tästä syystä kaikkia hallintamallin osa-alueita ei pystytty tässä yhteydessä käymään läpi kattavasti. Oli kuitenkin hyödyllistä selvittää mitä osa-alueita hallintamalli sisältää ja mistä eri viitekehyksistä voisi hallintamallin kehittämisessä olla apua.

Varsinainen hallintamalli syntyy, kun organisaatio lähtee toteuttamaan tietoturvallisuusohjelmaa ja kehittämään tietoturvallisuuden hallintajärjestelmää. Tietoturvallisuuden hallintamalli ei ole mikään irrallinen yksittäinen toteutettava asia, vaan se muodostuu organisaation tietoturvallisuuden hallintakeinoista, toiminnan suunnittelusta ja kehittämisestä, toimintamalleista ja jatkuvasta riskienhallinnasta. Näin ollen tietoturvallisuuden hallintamallia ei saatu opinnäytetyön aikana toteutettua Savon Voiman käyttöön, vaan sen toteuttaminen jää organisaation jatkotoimenpiteiden tehtäväksi hallintajärjestelmän kehittämisen yhteydessä.

Opinnäytetyö antoi minulle erittäin laajan käsityksen mistä organisaatioiden tietoturvallisuus kostuu ja kuinka koko kokonaisuutta tulisi hallita. Tietoturvallisuuden kattavan hallinnan toteuttaminen vaatii useiden vuosien kehittämistä ja sen kehittäminen kannattaa toteuttaa pieninä projekteina iso kuva ja tavoite mielessä.

Opinnäytetyön aikana tutustuin kattavasti eri tietoturvallisuuden standardeihin ja sain käsityksen mitkä standardit auttavat parhaiten Savon Voiman tietoturvallisuuden kehittämisessä. Tutustuin opinnäytetyön aikana myös kattavasti muuhun tietoturvallisuutta käsittelevään aineistoon ja sain sitä kautta arvokasta lisätietoa koko tietoturvallisuuden pelikentästä. Tätä tietoa pystyn hyödyntämään myös tulevaisuudessa kehittäessäni organisaatioiden tietoturvallisuutta.

Tämän opinnäytetyön pohjalta on helpompi lähteä kehittämään organisaation tietoturvallisuuden hallintaa yhdessä tietoturvasta vastaavan organisaation kanssa ja toteuttamaan tietoturvallisuuden kehittämisohjelmaa.

LÄHTEET JA TUOTETUT AINEISTOT

IT Governance Institute ITGI, 2006. Guidance for Board of Directors and Executive Management 2nd Edition. [Viitattu 2016-12-17.] Saatavissa: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx

IT for Business, 2016. Tietohallintomalli. [Viitattu: 2017-05-04]. Saatavissa: https://www.itforbusiness.org/content//uploads/2016/12/Tietohallintomalli-20-10-2016_.pdf

HARRIS Shon, MAYMI Fernando 2016, CISSP Exam Guide Seventh Edition. New York: McGraw-Hill Education.

HEIKKILÄ, Tarja 2004. Tilastollinen tutkimus. Helsinki Edita Prima Oy. [Viitattu 2016-10-22.]

IMMONEN, Aapo 2015, Kyberturvallisuuden tilannekuva energia-alalla. [Viitattu 2016-10-16]. Saatavilla: www.huoltovarmuus.fi/static/pdf/877.pdf

ISO27k TOOLKIT 2016. Controls cross check 2013 [Verkkoaineisto]. Saatavissa: http://iso27001security.com

ISO27k TOOLKIT 2016. Statement of Applicability (SOA) [Verkkoaineisto]. Saatavissa: http://iso27001security.com

LIIKENNE JA VIESTINTÄMINISTERIÖ 2017, Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti. [Viitattu 2017-05-28]. Saatavilla: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79770/LVM_09_2017_Verkko_%20ja_tietoturvadirektiivi.pdf?sequence=1

NISKANEN Vesa, 1994. Tieteellisten menetelmien perusteita ihmistieteissä. Helsingin yliopisto Lahden tutkimus- ja koulutuskeskus: Yliopistopaino.

SAARANEN-KAUPPINEN, Anita, PUUSNIEKKA, Anna, KUULA, Arja ja RISSANEN Riitta 2009. Menetelmäopetuksen tietovaranto KvaliMOTV. Kvalitatiivisten menetelmien verkko-oppikirja [Viitattu 2016-10-22.] Saatavissa: http://www.fsd.uta.fi/fi/julkaisut/motv_pdf/KvaliMOTV.pdf

SAVON VOIMA 2016, Savon Voima Konserni 2016. [Viitattu 2016-10-22] Saatavissa: http://www.savonvoima.fi/konserni/

SFS-EN ISO 9001, 2015. Laadunhallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto SFS. [Viitattu 2016-10-15]

SFS-ISO/IEC 27000, 2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Suomen Standardisoimisliitto SFS. [Viitattu 2016-10-15]

SFS-ISO/IEC 27001, 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto SFS. [Viitattu 2016-10-15]

SFS-ISO/IEC 27002, 2014. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Suomen Standardisoimisliitto SFS. [Viitattu 2016-10-15]

SFS-ISO/IEC 27003, 2011. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita. Suomen Standardisoimisliitto SFS. [Viitattu 2016-10-15]

SFS-ISO/IEC 27005, 2013 Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. Suomen Standardisoimisliitto SFS. [Viitattu: 2017-02-05]

SFS-ISO/IEC 27014, 2013. Governance of Information Security. Suomen Standardisoimisliitto SFS. [Viitattu 2017-5-12]

SFS Suomen Standardisoimisliitto 2015, ISO/IEC 27000 –standardiperhe. Kalvosarja. [Viitattu 2017-05-28]. Saatavissa: www.sfsedu.fi/files/121/ISO-27000_2015.ppt

STAF Jan 2016. CISSP bootcamp koulutusmateriaali. [Viitattu 2017-5-18]

THE ISO 27000 DIRECTORY 2017. The ISO Certification Process. [Viitattu: 2017-06-10.] Saatavissa: http://www.27000.org/ismsprocess.htm

VALTIONVARAINMINISTERIÖ, 2006. Tietoturvatavoitteiden asettaminen ja mittaaminen VAHTI 6/2006. [Viitattu 2016-10-21]. Saatavissa: https://www.vahtiohje.fi/web/guest/home

VALTIONVARAINMINISTERIÖ, 2010. Tietoturvatason arviointimalli. Excel-työkalu. [Viitattu 2016-10-24] Saatavissa: www.valtori.fi/download/noname/%7BB3B5A34B-83D2-4649-BB9C.../13010
VALTIONVARAINMINISTERIÖ 2013, Suomen kyberturvallisuusstrategia. [Viitattu 2016-10-15].

Saatavissa: http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit

VALTIONVARAINMINISTERIÖ 2014, Tietoturvallisuuden arviointiohje 2/2014. [Viitattu 2016-10-15].

Saatavissa: https://www.vahtiohje.fi/web/guest/home

VALTIONVARAINMINISTERIÖ 2016, Toiminnan jatkuvuuden hallinta 2/2016. [Viitattu 2016-10-15].

Saatavissa: https://www.vahtiohje.fi/web/guest/home

VALTIONVARAINMININISTERIÖ 2016, Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi [Viitattu 2017-03-10] Saatavissa:

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75412/OECD_julkaisu_NETTI.pdf?sequence=1

VILKKA, Hanna 2007. Tutki ja mittaa. Määrällisen tutkimuksen perusteet. Helsinki: Tammi. [Viitattu 2016-10-22.]

LIITE 1: ISO/IEC 27002 KONTROLLIEN TYYPIT JA TAVOITTEET (ISO27K TOOLKIT 2016)

ISO/IEC 27002 section	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
5	**Information security policies**									
5,1	**Management direction for information security**									
5.1.1	Policies for information security	✓	✓	✓		✓	✓	✓	✓	✓
5.1.2	Review of the policies for information security	✓	✓	✓		✓	✓	✓	✓	✓
6	**Organization of information security**									
6,1	**Internal Organization**									
6.1.1	Information security roles and responsibilities	✓	✓	✓				✓	✓	
6.1.2	Segregation of duties	✓	✓	✓				✓	✓	✓
6.1.3	Contact with authorities		✓			✓		✓	✓	✓
6.1.4	Contact with special interest groups		✓	✓	✓			✓	✓	✓
6.1.5	Information security in project management		✓	✓				✓		
6,2	**Mobile devices and teleworking**									
6.2.1	Mobile device policy			✓				✓	✓	✓
6.2.2	Teleworking			✓				✓	✓	
7	**Human Resources Security**									
7,1	**Prior to employment**									
7.1.1	Screening	✓	✓					✓	✓	✓
7.1.2	Terms and conditions of employment	✓	✓					✓	✓	✓
7,2	**During employment**									
7.2.1	Management responsibilities	✓	✓	✓	✓			✓	✓	✓
7.2.2	Information security awareness, education and training	✓	✓	✓	✓	✓		✓	✓	✓
7.2.3	Disciplinary process	✓	✓	✓	✓	✓	✓	✓	✓	✓
7,3	**Termination and change of employment**									
7.3.1	Termination or change of employment responsibilities	✓	✓	✓				✓	✓	✓
8	**Asset Management**									
8,1	**Responsibility for Assets**									
8.1.1	Inventory of Assets		✓	✓			✓	✓	✓	✓
8.1.2	Ownership of assets		✓	✓	✓	✓	✓	✓	✓	✓
8.1.3	Acceptable use of assets		✓	✓				✓	✓	✓

8.1.4	Return of assets	✓	✓					✓	✓	✓
8,2	**Information classification**									
8.2.1	Classification of information		✓						✓	✓
8.2.2	Labelling of information	✓		✓	✓			✓	✓	✓
8.2.3	Handling of assets	✓		✓	✓			✓	✓	✓
8,3	**Media handling**									
8.3.1	Management of removeable media	✓	✓	✓				✓	✓	✓
8.3.2	Disposal of media		✓	✓				✓	✓	✓
8.3.3	Physical media transfer		✓	✓						✓
9	**Access Control**									
9,1	**Business requirements of access control**									
9.1.1	Access control policy	✓		✓				✓	✓	
9.1.2	Access to networks and network services		✓	✓				✓	✓	
9,2	**User access management**									
9.2.1	User registration and de-registration	✓	✓					✓	✓	
9.2.2	User access provisioning		✓	✓				✓	✓	
9.2.3	Management of privileged access rights		✓	✓				✓	✓	
9.2.4	Management of secret authentication information of users			✓				✓	✓	
9.2.5	Review of user access rights	✓		✓	✓			✓	✓	
9.2.6	Removal or adjustment of access rights		✓	✓				✓	✓	✓
9,3	**User responsibilities**									
9.3.1	Use of secret authentication information		✓	✓				✓	✓	
9,4	**System and application access control**									
9.4.1	Information access restriction	✓		✓				✓	✓	
9.4.2	Secure log-on procedures	✓	✓	✓				✓	✓	
9.4.3	Password management system	✓		✓				✓	✓	
9.4.4	Use of privileged utility programs			✓				✓	✓	✓
9.4.5	Access control to program source code		✓	✓					✓	
10	**Cryptography**									
10,1	**Cryptographic controls**									
10.1.1	Policy on the use of cryptographic controls		✓					✓	✓	
10.1.2	Key management		✓					✓	✓	
11	**Physical and Environmental Security**									
11,1	**Secure Areas**									

11.1.1	Physical security perimeter	✓	✓	✓				✓	✓	✓
11.1.2	Physical entry controls	✓	✓	✓	✓			✓	✓	✓
11.1.3	Securing offices, rooms and facilities	✓	✓	✓	✓			✓	✓	✓
11.1.4	Protecting against external and environmental attacks		✓	✓						✓
11.1.5	Working in secure areas	✓		✓				✓	✓	✓
11.1.6	Delivery and loading areas	✓	✓	✓				✓	✓	✓
11,2	**Equipment**									
11.2.1	Equipment siting and protection		✓	✓	✓			✓	✓	✓
11.2.2	Supporting utilities		✓	✓		✓	✓			✓
11.2.3	Cabling Security			✓				✓		✓
11.2.4	Equipment maintenance		✓	✓	✓				✓	✓
11.2.5	Removal of assets	✓	✓	✓	✓			✓	✓	✓
11.2.6	Security of equipment and assets off-premises		✓					✓	✓	✓
11.2.7	Secure disposal or re-use of equipment	✓	✓	✓				✓		
11.2.8	Unattended user equipment	✓		✓				✓	✓	
11.2.9	Clear desk and clear screen policy		✓					✓		
12	**Operations security**									
12,1	**Operational procedures and responsibilities**									
12.1.1	Documented operating procedures		✓	✓		✓	✓	✓	✓	✓
12.1.2	Change management	✓	✓	✓				✓	✓	✓
12.1.3	Capacity management		✓							✓
12.1.4	Separation of development, testing and operational environments	✓	✓	✓				✓	✓	✓
12,2	**Protection from malware**									
12.2.1	Controls against malware	✓		✓	✓	✓	✓		✓	✓
12,3	**Backup**									
12.3.1	Information backup		✓	✓			✓		✓	✓
12,4	**Logging and monitoring**									
12.4.1	Event logging	✓			✓	✓		✓	✓	✓
12.4.2	Protection of log information	✓	✓	✓				✓	✓	✓
12.4.3	Administrator and operator logs	✓			✓			✓	✓	✓
12.4.4	Clock synchronisation		✓	✓					✓	
12,5	**Control of operational software**									
12.5.1	Installation of software on operational systems		✓					✓	✓	✓
12,6	**Technical Vulnerability Management**									
12.6.1	Control of technical vulnerabilities		✓						✓	

12.6.2	Restrictions on software installation		✓	✓					✓	
12,7	**Information systems audit controls**									
12.7.1	Information systems audit controls	✓			✓					✓
13	**Communications security**									
13,1	**Network security management**									
13.1.1	Network controls			✓				✓	✓	✓
13.1.2	Security of network services		✓	✓	✓			✓	✓	✓
13.1.3	Segregation in networks	✓		✓				✓	✓	
13,2	**Information transfer**									
13.2.1	Information transfer policies and procedures		✓	✓				✓	✓	✓
13.2.2	Agreements on information transfer		✓	✓				✓	✓	
13.2.3	Electronic messaging	✓		✓				✓	✓	✓
13.2.4	Confidentiality or non-disclosure agreements		✓	✓				✓		
14	**System acquisition, development and maintenance**									
14,1	**Security requirements of information systems**									
14.1.1	Information security requirements analysis and specification		✓					✓	✓	✓
14.1.2	Securing application services on public networks	✓	✓	✓				✓	✓	
14.1.3	Protecting application services transactions	✓	✓	✓				✓	✓	
14,2	**Security in development and support processes**									
14.2.1	Secure development policy	✓		✓				✓	✓	
14.2.2	System change control procedures		✓						✓	✓
14.2.3	Technical review of applications after operating platform changes				✓				✓	
14.2.4	Restrictions on changes to software packages		✓	✓					✓	
14.2.5	Secure system engineering principles		✓	✓				✓	✓	
14.2.6	Secure development environment		✓	✓				✓	✓	
14.2.7	Outsourced software development	✓	✓	✓				✓	✓	
14.2.8	System security testing		✓	✓					✓	
14.2.9	System acceptance testing			✓	✓					✓
14,3	**Test data**									
14.3.1	Protection of system test data			✓					✓	
15	**Supplier relationships**									

15,1	**Information security in supplier relationships**									
15.1.1	Information security in supplier relationships	✓	✓	✓				✓	✓	✓
15.1.2	Addressing security within supplier agreements	✓	✓	✓	✓	✓	✓	✓	✓	✓
15.1.3	Information and communication technology supply chain	✓	✓	✓				✓	✓	✓
15,2	**Supplier service delivery management**									
15.2.1	Monitoring and review of supplier services				✓			✓	✓	✓
15.2.2	Managing changes to supplier services		✓	✓				✓	✓	✓
16	**Information security incident management**									
16,1	**Management of information security incidents and improvements**									
16.1.1	Responsibilities and procedures					✓	✓	✓	✓	✓
16.1.2	Reporting information security events				✓	✓		✓	✓	✓
16.1.3	Reporting information security weaknesses	✓			✓			✓	✓	✓
16.1.4	Assessment of and decision on information security events				✓	✓		✓	✓	✓
16.1.5	Response to information security incidents					✓	✓	✓	✓	✓
16.1.6	Learning from information security incidents		✓				✓	✓	✓	✓
16.1.7	Collection of evidence	✓		✓		✓		✓	✓	✓
17	**Information security aspects of business continuity management**									
17,1	**Information security continuity**									
17.1.1	Planning information security continuity					✓	✓			✓
17.1.2	Implementing information security continuity						✓			✓
17.1.3	Verify, review and evaluate information security continuity					✓	✓			✓
17,2	**Redundancies**									
17.2.1	Availability of information processing facilities		✓	✓		✓	✓			✓
18	**Compliance**									
18,1	**Compliance with legal and contractual requirements**									
18.1.1	Identification of applicable legislation and contractual requirements			✓				✓	✓	✓
18.1.2	Intellectual property rights			✓				✓		
18.1.3	Protection of records			✓		✓	✓	✓	✓	✓
18.1.4	Privacy and protection of personally identifiable			✓				✓		

	information									
18.1.5	Regulation of cryptographic controls			✓				✓		
18,2	**Information security reviews**									
18.2.1	Independent review of information security		✓	✓		✓	✓	✓	✓	✓
18.2.2	Compliance with security policies and standards	✓			✓			✓	✓	✓
18.2.3	Technical compliance review					✓		✓	✓	

LIITE 2: STATEMENT OF APPLICABILITY (ISO27K TOOLKIT 2016)

Current as of:
DD/MM/YYYY

Statement of Applicability
Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection				Remarks (overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
5 Security Policies	5,1	Management direction for information security							
	5.1.1	Policies for information							
	5.1.2	Review of the policies for information security							
6 Organisation of information security	6,1	Internal organisation							
	6.1.1	Information security roles and responsibilities							
	6.1.2	Segregation of duties							
	6.1.3	Contact with authorities							
	6.1.4	Contact with special interest groups							
	6.1.5	Information security in project management							
	6,2	Mobile devices and teleworking							
	6.2.1	Mobile device policy							
	6.2.2	Teleworking							
7 Human resource security	7,1	Prior to employment							
	7.1.1	Screening							
	7.1.2	Terms and conditions of employment							
	7,2	During employment							
	7.2.1	Management responsibilities							
	7.2.2	Information security awareness, education and training							
	7.2.3	Disciplinary process							
	7,3	Termination and change of employment							

	7.3.1	Termination or change of employment responsibilities							
8 Asset management	8,1	Responsibility for assets							
	8.1.1	Inventory of assets							
	8.1.2	Ownership of assets							
	8.1.3	Acceptable use of assets							
	8.1.4	Return of assets							
	8,2	Information classification							
	8.2.1	Classification of information							
	8.2.2	Labeling of information							
	8.2.3	Handling of assets							
	8,3	Media handling							
	8.3.1	Management of removable media							
	8.3.2	Disposal of media							
	8.3.3	Physical media transfer							
9 Access control	9,1	Business requirements of access control							
	9.1.1	Access control policy							
	9.1.2	Access to networks and network services							
	9,2	User access management							
	9.2.1	User registration and de-registration							
	9.2.2	User access provisioning							
	9.2.3	Management of privileged access rights							
	9.2.4	Management of secret authentication information of users							
	9.2.5	Review of user access rights							
	9.2.6	Removal or adjustment of access rights							
	9,3	User responsibilities							
	9.3.1	Use of secret authentication information							
	9,4	System and application access control							
	9.4.1	Information access restriction							
	9.4.2	Secure log-on procedures							
	9.4.3	Password management system							
	9.4.4	Use of privileged utility programs							
	9.4.5	Access control to program source code							
10 Cryptography	10,1	Cryptographic controls							
	10.1.1	Policy on the use of cryptographic controls							
	10.1.2	Key management							
11 Physical and	11,1	Secure areas							

environmental security	11.1.1	Physical security perimeter							
	11.1.2	Physical entry controls							
	11.1.3	Securing office, room and facilities							
	11.1.4	Protecting against external end environmental threats							
	11.1.5	Working in secure areas							
	11.1.6	Delivery and loading areas							
	11,2	Equipment							
	11.2.1	Equipment siting and protection							
	11.2.2	Supporting utilities							
	11.2.3	Cabling security							
	11.2.4	Equipment maintenance							
	11.2.5	Removal of assets							
	11.2.6	Security of equipment and assets off-premises							
	11.2.7	Secure disposal or re-use of equipment							
	11.2.8	Unattended user equipment							
	11.2.9	Clear desk and clear screen policy							
12 Operations security	12,1	Operational procedures and responsibilities							
	12.1.1	Documented operating procedures							
	12.1.2	Change management							
	12.1.3	Capacity management							
	12.1.4	Separation of development, testing and operational environments							
	12,2	Protection from malware							
	12.2.1	Controls against malware							
	12,3	Backup							
	12.3.1	Information backup							
	12,4	Logging and monitoring							
	12.4.1	Event logging							
	12.4.2	Protection of log information							
	12.4.3	Administrator and operator logs							
	12.4.4	Clock synchronisaton							
	12,5	Control of operational software							
	12.5.1	Installation of software on operational systems							
	12,6	Technical vulnerability management							
	12.6.1	Management of technical vulnerabilities							
	12.6.2	Restrictions on software installation							
	12,7	Information systems audit considerations							

	12.7.1	Information systems audit controls							
13 Communications security	13,1	Network security management							
	13.1.1	Network controls							
	13.1.2	Security of network services							
	13.1.3	Segregation in networks							
	13,2	Information transfer							
	13.2.1	Information transfer policies and procedures							
	13.2.2	Agreements on information transfer							
	13.2.3	Electronic messaging							
	13.2.4	Confidentiality or non-disclosure agreements							
14 System acquisition, development and maintenance	14,1	Security requirements of information systems							
	14.1.1	Information security requirements analysis and specification							
	14.1.2	Securing applications services on public networks							
	14.1.3	Protecting application services transactions							
	14,2	Security in development and support processes							
	14.2.1	Secure development policy							
	14.2.2	System change control procedures							
	14.2.3	Technical review of applications after operating platform changes							
	14.2.4	Restrictions on changes to software packages							
	14.2.5	Secure system engineering principles							
	14.2.6	Secure development environment							
	14.2.7	Outsourced development							
	14.2.8	System security testing							
	14.2.9	System acceptance testing							
	14,3	Test data							
	14.3.1	Protection of test data							
15 Supplier relationships	15,1	Information security in supplier relationships							
	15.1.1	Information security policy for supplier relationships							
	15.1.2	Addressing security within supplier agreements							
	15.1.3	Information and communication technology supply chain							
	15,2	Supplier service delivery management							
	15.2.1	Monitoring and review of supplier services							

	15.2.2	Managing changes to supplier services							
16 Information security incident management	16,1	Management of information security incidents and improvements							
	16.1.1	Responsibilities and procedures							
	16.1.2	Reporting information security events							
	16.1.3	Reporting information security weaknesses							
	16.1.4	Assessment of and decision on information security events							
	16.1.5	Response to information security incidents							
	16.1.6	Learning from information security incidents							
	16.1.7	Collection of evidence							
17 Information security aspects of business continuity management	17,1	Information security continuity							
	17.1.1	Planning information security continuity							
	17.1.2	Implementing information security continuity							
	17.1.3	Verify, review and evaluate information security continuity							
	17,2	Redundancies							
	17.2.1	Availability of information processing facilities							
18 Compliance	18,1	Compliance with legal and contractual requirements							
	18.1.1	Identification of applicable legislation and contractual requirements							
	18.1.2	Intellectual property rights							
	18.1.3	Protection of records							
	18.1.4	Privacy and protection of personally identifiable information							
	18.1.5	Regulation of cryptographic controls							
	18,2	Information security reviews							
	18.2.1	Independent review of information security							
	18.2.2	Compliance with security policies and standards							
	18.2.3	Technical compliance review							

LIITE 3: EFQM/CAF ARVIONTILOMAKE (VAHTI 2/2010):

Otsikko EFQM/CAFin mukaan	Vaatimus	Taso	Toteutuuko vaatimus (kyllä/ei/ei koske meitä)
1. Johtajuudelle asetettavat vaatimukset			
1.1.	**Strateginen ohjaus: Organisaatio on tunnistanut ydintoimintoihinsa liittyvät jatkuvuuden ja erityistilanteiden hallintaa sekä tiedon turvaamista ohjaavat tekijät ja velvoitteet. Toiminnan jatkuvuuden hallinnan ja tiedon turvaamisen toimenpiteet tukevat organisaation ydintoiminnan tavoitteita.**		**0**
	1. Organisaation toimintaa koskevan lainsäädännön asettamien vaatimusten tunnistaminen ja niistä henkilöstölle tiedottaminen on organisoitu ja vastuutettu.	Perus (2)	
	2. Organisaation ydintoiminnot ja -prosessit on tunnistettu sekä organisoitu ja vastuutettu.	Perus (2)	
	3. Organisaatiolla on kirjallinen johdon hyväksymä tietoturvapolitiikka.	Perus (2)	
	4. Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi.	Korotettu (3)	
	5. Organisaatiolla on vuosittainen tietoturvallisuuden kehittämissuunnitelma.	Korkea (4)	
	6. Tulosohjauksessa käytetään myös tietoturvallisuuteen liittyviä osuuksia.	Korkea (4)	
1.2.	**Resursointi ja organisointi: Jatkuvuuden hallinnalle ja tiedon turvaamiselle on asetettu tavoitteisiin nähden riittävät resurssit.**		**0**
	1. Organisaatioon on nimitetty tietoturvavastaava, jonka työnkuvassa on mainittu tietoturvavastuut.	Perus (2)	
	2. Tietoturvavastaavalla on aikaa tietoturvavastuidensa suorittamiseen.	Perus (2)	
	3. Kaikkien tietoturvavastuita omaavien työnkuvissa vastuu on mainittu.	Korotettu (3)	
	4. Organisaatiossa on sen kokoon ja tavoitteisiin nähden riittävästi tietoturvahenkilöstöä.	Korotettu (3)	
	5. Tietoturvallisuuden resursointi on huomioitu organisaation toiminta- ja taloussuunnittelussa tai budjetissa ja toteutumista seurataan.	Korotettu (3)	
	6. Tietoturvavastaava on päätoiminen.	Korkea (4)	
1.3.	**Yhteistyön koordinointi: Jatkuvuuden hallinnan ja tiedon turvaamisen suunnittelu toteutetaan ydin- ja tukitoimintojen yhteistyönä.**		**0**
	1. Organisaation johto ja tietoturvallisuuden eri osa-alueiden vastuuhenkilöt keskustelevat säännöllisesti.	Perus (2)	
	2. Organisaatiossa on säännöllisesti kokoontuva tietoturva-asioita käsittelevä yhteistyöryhmä.	Perus (2)	
	3. Johdon tapaamiset ovat vähintään kerran vuodessa.	Korotettu (3)	
	4. Tietoturva-asioita käsittelevä yhteistyöryhmä kokoontuu vähintään kaksi kertaa vuodessa.	Korotettu (3)	
	5. Tapaamisissa käsitellään mm. havaittuja riskejä, asetettuja tietoturvatavoitteita, niiden saavuttamista ja tulevaisuuden tarpeista aiheutuvia muutoksia.	Korkea (4)	
	6. Tapaamisista pidetään pöytäkirjaa ja sovittujen toimenpiteiden toteutumista seurataan.	Korkea (4)	

1.4.	**Raportointi ja viestintä sidosryhmille: Viestinnän ja raportoinnin vastuut ja toimintamalli sidosryhmien kanssa on määritetty siten, että osapuolilla on toimintaan, sen kehittämiseen ja päätöksentekoon tarvittavat tiedot.**		**0**
	1. Sidosryhmät, joille organisaatio on vastuussa tietoturvallisuudesta, ja niiden kontaktipisteet on tunnistettu.	Perus (2)	
	2. Johto on organisoinut ja vastuuttanut sidosryhmiin vaikuttavista tietoturva-asioista raportoinnin sekä tietoturvapoikkeamista tiedottamisen.	Perus (2)	
	3. Sidosryhmille raportoidaan tietoturvallisuudesta vuosittain tai johdon määrittelemällä tavalla.	Korotettu (3)	
	4. Sidosryhmäraportilla on mallipohja.	Korotettu (3)	
	5. Jos muuta ei sovita, raportin sisältöön kuuluu mittaustietoa vaatimuksenmukaisuudesta, tietoturvatavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyt toimenpiteet sekä muut merkittävimmät tietoturvamuutokset.	Korkea (4)	
	6. Raportointia kehitetään sidosryhmien palautteen perusteella.	Korkea (4)	
1.5.	**Johtaminen erityistilanteessa: Erityistilanteiden hallinta on organisoitu ja huomioitu toimintamalleissa.**		**0**
	1. Tietoturvapoikkeamien käsittely on organisoitu ja vastuutettu.	Perus (2)	
	2. Vakavista tietoturvapoikkeamista kerrotaan johdolle viivytyksettä ja niistä pidetään kirjaa.	Perus (2)	
	3. Organisaatiossa on kirjallinen malli tietoturvapoikkeamien käsittelyyn. Ohjeessa on määritelty roolitasolla kuka selvittää tapahtunutta kenen määräyksestä ja kuka päättää viranomaiskontakteista (esim. esitutkintapyynnön teosta) ja tiedottamisesta.	Korotettu (3)	
	4. Tietoturvapoikkeamista tehdään jälkikäteisanalyysi ja käynnistetään tarvittavat korjaavat toimenpiteet tapahtuman uusiutumisen ehkäisemiseksi.	Korotettu (3)	
	5. Havaituista tietoturvapoikkeamista tehdään vuosittain yhteenveto.	Korkea (4)	
	6. Tietoturvapoikkeamista vaihdetaan tietoja kumppanien kanssa ja kumppanien kokemuksia käytetään hyväksi.	Korkea (4)	
1.6.	**Raportointi Johdolle: Tiedot kehittämistoimenpiteiden toteutumisesta ja kustannuksista välittyvät organisaation johdolle.**		**0**
	1. Tietoturvallisuudesta raportointi on vastuutettu ja organisoitu.	Perus (2)	
	2. Tietoturva-asioista raportoidaan organisaation johdolle säännöllisesti.	Perus (2)	
	3. Raportointimenettely on kuvattu kirjallisesti.	Korotettu (3)	
	4. Tietoturva-asioista raportoidaan organisaation johdolle vähintään vuosittain.	Korotettu (3)	
	5. Jatkuva raportointi perustuu päätettyihin toiminnan mittareihin.	Korkea (4)	
	6. Raportin sisältöön kuuluu mittaustietoa resurssien käytöstä, tietoturvatavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyt toimenpiteet sekä muut merkittävimmät tietoturvamuutokset.	Korkea (4)	
2. Toiminnan suunnittelulle asetettavat vaatimukset			
2.1.	**Toimintaympäristön vaikutus: Toimintaympäristö ja sen vaikutus toimintaan tunnetaan.**		**0**
	1. Erilliset tietojen käsittelyn toimintaympäristöt ja niihin kuuluvat järjestelmät ja toiminnot on tunnistettu.	Perus (2)	
	2. Kunkin toimintaympäristön erityisvaatimukset ja tavoitteet tietoturvallisuuden osalta on tunnistettu.	Perus (2)	
	3. Toimintaympäristöt ja niihin kuuluvat järjestelmät on dokumentoitu.	Korotettu (3)	
	4. Ympäristö- ja järjestelmälistaukset katselmoidaan ja tarvittaessa päivitetään vähintään vuosittain	Korotettu (3)	
	5. Ympäristöjen elinkaaren vaiheet on dokumentoitu ja dokumentissa on kriteerit milloin ja miten ympäristö siirtyy vaiheesta toiseen.	Korkea (4)	

	6. Kunkin elinkaaren vaiheen erityisvaatimukset tietoturvallisuuden osalta on määritelty ja dokumentoitu.	Korkea (4)	
2.2.	**Tavoitteiden määrittely: Ydintoiminnasta on johdettu sen edellyttämien palvelujen jatkuvuuden hallinnan, erityistilanteiden ja tiedon turvaamisen vaatimukset.**		**0**
	1. Kunkin ydintoiminnon ja -prosessin tietoturvallisuuden kannalta suojattavat kohteet on tunnistettu ja luokiteltu vaadittavan tietoturvallisuuden tason mukaisesti.	Perus (2)	
	2. Ydintoimintojen tai -prosessien tavoitteisiin on liitetty myös tietoturvatavoitteita.	Perus (2)	
	3. Tietoturvatavoitteiden määrittelyssä on otettu huomioon sekä luottamuksellisuus, eheys että saatavuus.	Korotettu (3)	
	4. Ydintoiminnoista ja -prosesseista on karkean tason toiminto- tai prosessikuvaukset.	Korotettu (3)	
	5. Toiminto- tai prosessikuvauksiin on liitetty tietoturvallisuuden kannalta oleelliset tietoturvaprosessit tai toimet tai ne on dokumentoitu erikseen.	Korkea (4)	
	6. Toimintojen tietoturvatavoitteisiin on liitetty suoriutumista kuvaavia mittareita.	Korkea (4)	
2.3.	**Toiminnan kehittäminen riskien arvioinnilla: Organisaatio varmistaa, että tietoturvallisuuden taso vastaa organisaation strategisia tavoitteita. Tietoturvallisuuden kehittäminen ottaa huomioon organisaatiota kohtaavat tietoturvauhat ja riskit. Säännöllinen riskienhallintamenettely on käytössä.**		**0**
	1. Organisaatiossa tehdään säännöllisesti tietoturvallisuuteen liittyvien riskien arviointia.	Perus (2)	
	2. Riskien arvioinnin perusteella parannetaan tietoturvallisuutta liian suurten riskien osalta johdon päättämillä toimenpiteillä.	Perus (2)	
	3. Organisaatiossa tehdään ydintoimintojen tietoturvariskien arviointia vähintään vuosittain.	Korotettu (3)	
	4. Organisaatiolla on riskien arvioinnin menetelmä ja ohjeistus.	Korotettu (3)	
	5. Organisaatiolla on kirjallinen tietoturvasuunnitelma, joka määrittelee mitä teknisiä ja hallinnollisia toimia ja prosesseja organisaatiossa käytetään havaittujen tietoturvariskien hallitsemiseksi.	Korotettu (3)	
	6. Organisaatiossa tehdään tietoturvariskien arviointia myös suurten muutosten yhteydessä.	Korkea (4)	
	7. Organisaatiolla on riskienhallintapolitiikka.	Korkea (4)	
	8. Suurimmista riskeistä pidetään koko organisaation tasolla kirjaa ja riskienhallintatoimenpiteiden toteutumista seurataan.	Korkea (4)	
2.4.	**Toimintaverkoston hallinta: Palvelujen jatkuvuus ja tiedon turvaaminen kumppaniverkostossa on suunniteltu ja sovittu.**		**0**
	1. Organisaatiossa on tiedossa, missä toimintaverkostoissa organisaatio on mukana sekä mitä alihankkijoita ja yhteistyökumppaneita sen tietojen kanssa toimii missäkin roolissa.	Perus (2)	
	2. Organisaatiolla on kirjallinen dokumentti, jossa kuvataan sen osallistumista ja roolia erilaisissa alihankinta- ja yhteistyöverkostoissa sekä osallistumisen yleisiä tietoturvavaatimuksia.	Korotettu (3)	
	3. Toimintoverkostot on luokiteltu tietoturvatason mukaan ja kullakin luokalla on omat tietoturvavaatimuksensa.	Korkea (4)	
	4. Palveluntarjoajaksi voidaan valita vain sellainen palveluntarjoaja, jolla on mahdollisuus suojata asiakirjojen luottamuksellisuus ja tarvittaessa selvittää luottamuksellisuuden loukkaukset sähköisen viestinnän tietosuojalain (516/2004) 13 a - 13k §.ssä tarkoitetulla tavalla.	Korkea (4)	
2.5.	**Erityistilanteiden hallinta: Erityistilanteiden hallinnan menettelyt on suunniteltu, koulutettu ja harjoiteltu.**		**0**
	1. Organisaation johto on tiedostanut mitä yhteiskunnan elintärkeiden toimintojen turvaamiseen (YETT) liittyviä vastuita organisaatiolla on.	Suomen erityisvaatimus	
	2. Organisaatiolla on jatkuvuussuunnitelma tai -suunnitelmia.	Perus (2)	
	3. Jatkuvuussuunnitelmien päivitys ja katselmointi on vastuutettu ja organisoitu.	Korotettu (3)	
	4. Jatkuvuussuunnitelmien toimivuutta testataan, harjoitellaan ja arvioidaan säännöllisesti.	Korotettu (3)	
	5. Jatkuvuussuunnitelmien toimivuutta harjoitellaan keskeisten yhteistyökumppanien kanssa.	Korkea (4)	

3. Henkilöstölle asetettavat vaatimukset			
3.1.	**Osaamisen ja tietoisuuden kehittäminen sekä sanktiot: Jatkuvuuden hallinnan ja tiedon turvaamisen osaamiselle on asetettu rooli- tai tehtäväkohtaiset vaatimukset, osaamistaso tunnetaan ja osaamista kehitetään. Organisaatio kannustaa henkilöstöä noudattamaan ja kehittämään hyvää jatkuvuuden hallinnan ja tiedon turvaamisen toimintamallia. Organisaatiossa on sovittu tapa toimia turvallisuuspoikkeamissa ja väärinkäytöstilanteissa.**		**0**
	1. Työntekijöiden tekninen valvonta on käsitelty YT-menettelyn mukaisesti (Laki yksityisyyden suojasta työelämässä, 21§).	Suomen erityisvaatimus	
	2. Organisaatiossa järjestetään säännöllisesti tietoturvakoulutusta henkilöstölle ja muille avainryhmille. Tietoturvahenkilöstön osaamista kehitetään ja ylläpidetään.	Perus (2)	
	3. Perehdyttämistilanteessa käsitellään myös tietoturva-asioita.	Perus (2)	
	4. Muuttuneista tietoturvaohjeista ja -käytännöistä tiedotetaan kaikille organisaatiossa toimiville.	Perus (2)	
	5. Sääntöjen noudattamista seurataan ja poikkeamiin puututaan.	Perus (2)	
	6. Organisaatiossa on kirjallinen tietoturvallisuuden koulutussuunnitelma.	Korotettu (3)	
	7. Perehdyttäjällä on kirjallinen lista käsiteltävistä tietoturva-asioista.	Korotettu (3)	
	8. Henkilöstön osallistumista koulutuksiin seurataan.	Korotettu (3)	
	9. Tietoturvamääräysten ja -ohjeiden rikkomisen seuraukset on kuvattu organisaatiossa ja tiedotettu kaikille organisaatiossa työskenteleville.	Korotettu (3)	
	10. Esimies ja alainen käyvät vuosittain keskustelun työn tietoturvavastuista ja osaamisen kehittämisen tarpeista.	Korotettu (3)	
	11. Henkilöstön tietoturvaosaamisesta varmistutaan.	Korotettu (3)	
	12. Tietoturvakoulutuksessa otetaan huomioon organisaatiossa ja lähiympäristössä tapahtuneet muutokset ja tietoturvapoikkeamat.	Korkea (4)	
	13. Hyvistä tietoturvateoista annetaan positiivista huomiota.	Korkea (4)	
3.2.	**Henkilöresurssien ja tehtävien hallinta: Henkilöstö ja sen käyttö on suunniteltu ja mitoitettu ydintoimintojen jatkuvuuden hallinnan ja tiedon turvaamisen edellyttämällä tavalla. Avainroolit ja -henkilöt on tunnistettu ja varajärjestelyt on suunniteltu.**		**0**
	1. Toteutettavaksi valitut tietoturvatoimenpiteet ja -prosessit on organisoitu ja vastuutettu.	Perus (2)	
	2. Tietoturvallisuuden avainroolit on tunnistettu ja niille on nimetty varahenkilö tai -henkilöt.	Perus (2)	
	3. Toteutettavaksi valituista tietoturvaprosesseista tai -toimenpiteistä ja niiden vastuuhenkilöistä on luettelo.	Korotettu (3)	
	4. Tietoturvallisuuden varahenkilöt on koulutettu tehtäväänsä	Korotettu (3)	
	5. Organisaatiossa on määritelty tehtävät tai roolit, joiden hakijasta tehdään turvallisuusselvitys, ja selvityksen hakuprosessi on dokumentoitu.	Korkea (4)	
	6. Organisaatiossa on tehty tietoturvallisuuden osaamiskartoitus.	Korkea (4)	
3.3.	**Erityistilanteissa toimiminen: Kriittisten toimintojen häiriöiden hallintaohjeet on laadittu, koulutettu ja toiminta harjoiteltu.**		**0**
	1. Sähköisten viestien, sähköpostien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan myös tietoturvapoikkeamatilanteita selvitettäessä (Sähköisen viestinnän tietosuojalaki 4§ ja 5§ sekä Laki yksityisyyden suojasta työelämässä 6. luku).	Suomen erityisvaatimus	
	2. Henkilöstö tietää, kenelle tietoturvapoikkeamista ja -tapauksista tai niiden uhkista tulee ilmoittaa.	Perus (2)	
	3. Tietoturvapoikkeamia selvittävät henkilöt on koulutettu tehtäväänsä.	Korotettu (3)	
	4. Organisaatiossa on tietoturvapoikkeamien selvittämiseen koulutettu ryhmä, joka harjoittelee säännöllisesti.	Korkea (4)	

4. Kumppanuuksille ja resurssien hallinnalle asetettavat vaatimukset			
4.1.	**Sopimusten hallinta: Sopimuksissa kirjataan liiketoiminnan jatkuvuuden hallinnan, erityistilanteiden hallinnan ja tiedon turvaamisen vaatimukset sekä niiden toteuttaminen. Kriittisen toiminnan jatkuvuuden ja tiedon turvaamisen hallintavelvoite on ulotettu koko toimittajaverkostoon.**		**0**
	1. Kumppanuus- ja hankintatoiminta on vastuutettu ja organisoitu.	Perus (2)	
	2. Kumppanin kanssa tehdään kirjallinen sopimus, jossa määritellään yhteistyön tai hankinnan kohteen tietoturvavaatimukset sekä miten tietoturvallisuuden valvonta, seuranta, auditointi ja raportointi tapahtuu.	Perus (2)	
	3. Kumppanille asetetaan tarvittavat tietoturvavaatimukset jo tarjouspyyntö- tai kumppanuusneuvotteluvaiheessa.	Korotettu (3)	
	4. Kumppanuussopimuksessa määritellään mitä tietoturvallisuustasoa kumppanin ja mahdollisen kumppanin alihankintaverkoston on kohteen luonteen huomioon ottaen noudatettava.	Korotettu (3)	
	5. Ennen sopimuksen solmimista organisaatio auditoi tai pyytää kirjallisen selvityksen kumppanin yhteistyön kohteeseen liittyvistä tietoturvamenettelyistä.	Korkea (4)	
	6. Sopimuksessa on määritelty sanktiot tietoturvapoikkeamista ja -loukkauksista.	Korkea (4)	
4.2.	**Toiminnan varmistaminen erityistilanteissa: Kumppanin häiriöiden ja erityistilanteiden hallintakyky on määritelty ja todennettu.**		**0**
	1. Tietoturvallisuuden valvonta sekä poikkeamien kirjaaminen ja raportointi on organisoitu ja vastuutettu yhteistyön kohteeseen liittyen.	Perus (2)	
	2. Havaituista kumppania koskevista tietoturvapoikkeamista tiedotetaan kumppanille välittömästi ja poikkeaman korjaustoimet aloitetaan sovitusti.	Perus (2)	
	3. Tietoturvapoikkeaman käsittelystä yhteistyössä on kirjalliset ohjeet.	Korotettu (3)	
	4. Poikkeamasta ja sen syystä valmistuu kirjallinen raportti.	Korotettu (3)	
	5. Organisaatiokohtaisia jatkuvuusharjoituksia toteutetaan säännöllisesti.	Korotettu (3)	
	5. Yhteistoimintaa erityistilanteessa harjoitellaan kumppanin kanssa.	Korkea (4)	
	6. Tietoa poikkeamien syistä käytetään sopimusten ja toiminnan parantamiseen.	Korkea (4)	
5. Toiminnan prosesseille asetettavat vaatimukset			
5.1.	**Tietoaineistojen hallinta: Asiakirjallisen ja muun tietoaineiston turvallisuus varmistetaan sen koko elinkaaren aikana. Organisaatiossa käsitellään tietoaineistoja lakien ja hyvän hallintotavan mukaisesti.**		**0**
	1. Organisaatiolla on arkistonmuodostussuunnitelma (Arkistolaki 8§), josta käytetään usein myös nimitystä tiedonhallinta- tai tiedonohjaussuunnitelma.	Suomen erityisvaatimus	
	2. Organisaatio pitää luetteloa organisaatioon käsiteltäviksi tulleista ja käsitellyistä asioista (Julkisuuslaki 18§).	Suomen erityisvaatimus	
	3. Työntekijät tietävät miten tietoaineistoja organisaatiossa käsitellään.	Perus (2)	
	4. Organisaation tuottamasta kirjallisesta asiakirjasta käy ilmi kuka sen on laatinut ja milloin sekä sen hyväksymisen tila.	Perus (2)	
	5. Hävitettäväksi tarkoitetut asiakirjat tuhotaan niin, että luottamuksellisuus ja tietosuoja on varmistettu.	Perus (2)	
	6. Organisaatiolla on tietoaineistojen käsittelyn kirjallinen ohje, jossa kerrotaan, miten asiakirjat hyväksytään, katselmoidaan ja mikä organisaation aineisto on salassa pidettävää tai muun vaitiolovelvollisuuden alaista.	Korotettu (3)	
	7. Organisaatiossa käytössä olevat tietoaineistojen hallinnan välineet tukevat aineistojen luokittelua ja arkistointia.	Korkea (4)	

6. Toiminnan arvioinnille ja todentamiselle asetettavat vaatimukset			
6.1.	**Toiminnan arviointi ja todentaminen: Tietoturvallisuuden hallinnan tilaa organisaatiossa seurataan jotta voidaan varmistua, että se palvelee ydintoimintaa.**		**0**
	1. Organisaatiossa tehdään säännöllisesti tietoturvallisuuden auditointeja tai arviointeja.	Perus (2)	
	2. Auditoinnit tai arvioinnit ovat suunniteltuja ja johdon hyväksymiä.	Perus (2)	
	3. Auditoinnin tai arvioinnin tulokset raportoidaan toiminnon tai kohteen omistajalle.	Perus (2)	
	4. Auditointien tai arviointien suosituksista pidetään koko organisaation tasolla kirjaa ja parannustoimenpiteiden toteutumista seurataan.	Perus (2)	
	5. Tietoturva-auditointeja tai arviointeja tehdään joka vuosi.	Korotettu (3)	
	6. Organisaatiossa on kirjallinen johdon hyväksymä auditointi- tai arviointiprosessi, jossa on mm. määritelty auditoijien tai arvioijien pätevyysvaatimukset.	Korotettu (3)	
	7. Raportin pohjalta toiminnon tai kohteen omistaja määrittelee ja vastuuttaa parannustoimenpiteet, joilla havaitut riskit saadaan hyväksyttävälle tasolle.	Korotettu (3)	
	8. Auditoinnit tai arvioinnit käyvät läpi organisaation ydintoiminnot 5 vuoden aikajaksolla.	Korkea (4)	
	9. Tietoturva-auditoinneissa tai -arvioinneissa käytetään myös ulkopuolisia resursseja.	Korkea (4)	