Tietoturvallisuuden hallintajärjestelmän käyttöönotto organisaatiossa

Janne Salonen

2020 Laurea

Laurea-ammattikorkeakoulu

Tietoturvallisuuden hallintajärjestelmän käyttöönotto organisaatiossa

Janne Salonen

Turvallisuus ja riskienhallinta

Opinnäytetyö

Toukokuu 2020

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuus ja riskienhallinta
Tradenomi amk

Janne Salonen
Tietoturvallisuuden hallintajärjestelmän käyttöönotto organisaatiossa
Vuosi 2020 Sivumäärä 46

Tässä opinnäytetyössä tutkitaan tapaustutkimuksen ja konstruktiivisen menetelmän keinoin, miten ISO/IEC 27001 -standardin mukainen tietoturvallisuuden hallintajärjestelmä luodaan, toteutetaan ja ylläpidetään organisaatiossa jatkuvan parantamisen periaatteen mukaisesti, jotta prosessin osalta voidaan ymmärtää, mitä odottaa, vaatia ja välttää. Näistä tiedoista hyötyvät erityisesti tietoturvapäälliköt ja –asiantuntijat, jotka ovat kiinnostuneita edistämään standardin mukaisen hallintajärjestelmän käyttöä organisaatioissaan.

Tietoturvallisuuden hallintajärjestelmän käyttöönotto on mielekkäintä nähdä organisaation strategisena päätöksenä, koska se vaikuttaa perinpohjaisesti tietoturvallisuustoimintaan ja -toimintoihin sen jälkeen, kun se toteutetaan organisaation tarpeiden mukaisena. Standardin vaatimukset, teoreettiset mallit ja tapaustutkimuksen tutkimusmenetelmät muodostavat kokonaisuuden, jota analysoidaan systemaattisesti ja sovelletaan konstruktiivisesti. Kolme tässä opinnäytetyössä esiteltävää tapausta ovat keksittyjä ja niiden on tarkoitus osoittaa, millaisia todelliset esteet ja hidasteet voivat olla, kun siirrytään aiemmista tietoturvallisuuden hallinnoinnin tavoista käyttämään standardin mukaista hallintajärjestelmää.

Teoreettinen viitekehys on Socio-technical Systems –malli, koska se soveltuu projekteihin, joiden tarkoituksena ovat organisaatiota kehittävät tehtävät kuten tietojärjestelmäkehitys tai tietoturvan järjestelmän parantaminen. On suositeltavaa hyödyntää teoreettisia viitekehyksiä, joiden avulla prosessia voidaan edistää. Opinnäytetyön tulokset osoittavat, että kolmen mahdollisen tapauksen ongelmien syyt pyrittäessä standardin mukaiseen hallintajärjestelmään johtuivat puutteellisesta ja epäselvästä tietoturvapolitiikasta, viestinnän vaikeuksista ja epäorganisoidusta tavasta tallentaa ja dokumentoida tietoa organisaatiossa. Opinnäytetyön tulosten perusteella on suositeltavaa, että standardi luetaan ja sisäistetään huolellisesti ja että ongelmien ilmetessä hyödynnetään teoreettisia menetelmiä, jotka nimetään tuonnempana, mikäli ne sopivat organisaation luonteeseen ja rakenteeseen. On tärkeää, että ISO/IEC 27001 –standardia toteutetaan asiantuntijoiden johdolla, jotka osaavat edistää prosessia ammattimaisesti ja käytännöllisen tietotaitonsa avulla.

Asiasanat: ISO/IEC 27001:2017, riskienhallinta, tietoturva

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Bachelor's Thesis

Janne Salonen

The Adoption of an Information Security Management System in an Organization

Year 2020 Pages 46

The purpose of this thesis is to offer insights into how to establish, implement, maintain and improve an information security management system (ISMS) called ISO/IEC 27001 in an organization. The thesis employs case studies as the research method, which involves systematic analyses and constructive implications. This thesis provides guidelines for information security managers and experts on how to introduce this ISMS in an organization. The guidelines enable one to know what to expect, demand and avoid during the establishment of the ISMS.

The adaptation of the ISMS should be seen as a strategic decision for an organization, since it would profoundly affect all operations. The three cases used in this thesis are fictitious and are intended to illustrate the real obstacles and hindrances that may be encountered in migrating from previous information security solutions to the ISO/IEC 27001 standard for information security management.

The findings from this thesis show three potential problems concerning the implementation of the standard due to the context of the organization. The problems include a lack of clear and systematic security information policies in the organization, lack of efficient communications within the organization, and disorganized information storage and documenting systems for staff members.

The Socio-technical Systems model is the theoretical framework in this thesis because it is suitable for projects aimed at organizational development tasks, such as information system development or security system enhancement. Based on the results, it is recommended that a thorough reading and understanding of the standard should be conducted, and some suitable theoretical frameworks used to support the process upon the emergence of problems. It is also recommended to choose approaches in accordance with the nature and the structure of the organization. It is very important to have experts, who know how to use the standard, to efficiently manage the implementation process with professionalism and practical know-how.

Keywords: ISO/IEC 27001:2017, Information Security, Risk Management

Sisällys

1 Johdanto 7
1.1 Tutkimusongelman määritys 8
1.2 Tutkimusmenetelmät sekä tietoperustan teoreettinen viitekehys 10
1.3 Miksi kehittämistyö on tärkeää 12
1.4 Aiheen rajaaminen ja tutkimuskysymykset 17
2 Standardi ISO/IEC 27001:2017 18
2.1 ISO/IEC 27001:2017 – mikä se on 20
2.2 Vaatimusosan kuvailua 17
2.3 ISO/IEC 27001 -vaatimusosat 18
2.3.1 Organisaation toimintaympäristö 19
2.3.2 Johtajuus: sitoutuminen, tietoturvapolitiikka sekä roolit vastuut ja valtuudet ...20
2.3.3 Riskien ja mahdollisuuksien käsittely 22
2.3.4 Tietoturvatavoitteet ja suunnitelmat niihin pääsemiseksi 23
2.3.5 Standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomisen yhteydessä määritettävät tukitoiminnot: pätevyys, tietoisuus, viestintä ja dokumentointi 25
2.3.6 Toiminnasta eli toiminnan suunnittelusta ja ohjauksesta sekä tietoturvariskien arvioinnista ja käsittelystä 26
2.3.7 Suorituskyvyn arviointi – seuranta, mittaus, analysointi ja arviointi sekä sisäinen auditointi ja johdon katselmus 27
2.3.8 Parantaminen: Poikkeamat ja korjaavat toimenpiteet sekä jatkuva parantaminen 28
3 Ongelmaesimerkkejä, syiden arviointia ja ratkaisuehdotuksia 28
3.1 Mahdollisia ongelmakohtia standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomisessa organisaatiolle 29
3.1.1 Yhtenäisyyden, selkeän linjan ja tietoturvapolitiikan puutteet organisaatiossa 29
3.1.2 Johdon tehtävät, muutoksesta viestiminen ja epätietoisuus rooleista 31
3.1.3 Ongelmat dokumentoidun tiedon tallentamisessa ja löytämisessä organisaatiossa 33
4 Tulokset 36
4.1 Opinnäytetyön tulokset 37
4.2 Johtopäätökset opinnäytetyön tuloksista 39
Lähteet 42
Kuviot 44
Taulukot 44
Liitteet 45

1 Johdanto

Tässä opinnäytetyössä esitellään standardin ISO/IEC 27001:2017 mukaisen tietoturvallisuuden hallintajärjestelmää, sen käyttöönottoa ja sen hyödyntämistä organisaation ongelmanratkaisussa. Syy tämän työn tekemiseen on siinä, että ISO/IEC 27001:2017 –standardia on vaikeaa hahmottaa, mikäli ei perehdy siihen huolellisesti ja käytä aikaa sen ymmärtämiseen. Toinen keskeinen hankaluus on siinä, että vaikka perehtyisikin standardiin mahdollisimman huolellisesti, sen vaatimusosat eivät aukea, ellei osaa soveltaa sen osia organisaation toimintaympäristöön. Tästä syystä standardin pintapuolinen opiskelu ei välttämättä auta sen ymmärtämisessä käytännössä lainkaan. Nämä mainitut ongelmat ratkeavat tutkimuskysymysten vastausten ja johtopäätösten myötä, koska esimerkkien avulla etäisiksi jäävät vaatimusosat tulevat ymmärrettäviksi käytännössä. Hankalissa kysymyksissä ISO/IEC 27001:2017 –periaatteita verrataan paremmin tunnettuihin fyysisen turvallisuuden perusajatuksiin, jotta lukija voi havaita eri käytäntöjen välillä vallitsevia samankaltaisuuksia.

ISO/IEC 27001:2017 –standardin käyttöönoton tavoitteena on **luoda turvallisuutta** ja **lisätä toiminnan hallintaa** kohdeorganisaatiossa, oli kyseessä sitten valtionhallinnon toimija, yritys tai vaikka yhdistys. Korostettakoon tässä yhteydessä, että standardit ISO/IEC 27001:2013 ja ISO/IEC 27001:2017 ovat sisällöllisesti lähes täysin identtisiä, ja molemmat standardit ovat käytössä tässä opinnäytetyössä. Opinnäytetyössä kuvaillaan ensin yleisellä tasolla standardia ISO/IEC 27001, sen ominaisuuksia, piirteitä ja erityistä huomiota kiinnitetään vaatimusosaan ja sen soveltamiseen. Lisäksi esitellään ISO/IEC 27001 -standardia tukevia menetelmiä, ohjeistuksia ja käsitteenmäärittelyjä. Keskeiset osat työtä ovat tapausesimerkit, jotka esitellään siten, että ensin esitetään kuvitteellinen (mutta täysin mahdollinen) ongelma, etsitään juurisyitä sille ja lopuksi ratkaistaan ongelma (tai hahmotellaan konstruktiivisia ratkaisumahdollisuuksia) standardin vaatimusten valossa. Myös standardin hallintakeinoja eli kontrolleja esitellään lyhyesti ja viittauksenomaisesti ongelmanratkaisuluvuissa. Nämä kontrollit ovat käytännön keinoja toteuttaa hallintajärjestelmän vaatimusosia.

Tietoturvallisuuden tulisi ylipäänsä olla luonnollinen osa organisaation toimintaa ja ennen kaikkea osana kokonaisvaltaisempaa riskienhallintaa. Sen tulee muodostaa perustaa toiminnan jatkuvuuden suunnittelulle ja toiminnan varmuudelle. Keskeisten toimintaa sekä päätöksiä tukevien tietoaineistojen täytyy olla saavutettavissa tarpeen mukaan, jotta organisaation toiminta ei vaarantuisi. Virheellinen tai luvattomasti muutettu tieto voi saada aikaan vakavia vahinkotilanteita organisaatiolle, julkikuvalle tai pahimmassa tapauksessa jopa yhteiskunnan turvallisuudelle, mikäli päätöksiä tehdään tuon vääristyneen tiedon pohjalta. (Andreasson & Koivisto 2013, 32.)

ISO/IEC 27001:2017 –standardi saatetaan mieltää liian suppeassa mielessä tietoturvallisuuden hallintajärjestelmäksi siinä mielessä, että ei riittävän hyvin ymmärretä, että mikä tahansa kokonaisturvallisuuden osa-alueen ongelma saattaa luoda tietoturvallisuuden kannalta riskialttiin tilanteen. Näin ollen on alusta alkaen tärkeää tarkastella standardia myös kokonaisturvallisuuden edistämisen työvälineenä. Käytännössä ISO/IEC 27001:2017 –standardin mukainen hallintajärjestelmä ei jätä merkittäviä jäännösriskejä myöskään fyysisen turvallisuuden osalta, kun vaatimuksenmukaisuus on kunnossa ja hallintakeinot ovat vaikuttavia. Tarvittavat hallintakeinot muodostavat fyysisen turvallisuuden periaatteiden mukaisesti yhtenäisen järjestelmän (ISO/IEC 27003:2017, 24; Garcia 2008, 9).

1.1 Tutkimusongelman määritys

Mikäli organisaatio päättää ryhtyä toteuttamaan ISO/IEC 27001:2017 –standardin mukaista tietoturvallisuuden hallintajärjestelmää, useita käytännön kysymyksiä nousee esiin: onko resursseja, onko aikaa, onko asiantuntijoita omassa organisaatiossa, voidaanko saada apua ulkopuolisilta standardin tuntijoilta, saadaanko vastuut määriteltyä ja niin edelleen. Itse standardi on alle 50-sivuinen teksti, mutta koska siinä on useita vaatimusosia ja velvoittavia määrityksiä, sen sisäistäminen voi olla hyvinkin haastavaa. Jopa kokonaiskuvaa voi olla vaikea saada, koska usein saattaa käydä niin, ettei standardin laajuutta täysin alussa ymmärretä. Vaikka kyseessä onkin tietoturvallisuuden hallintajärjestelmä, standardin voisi periaatteiltaan mieltää myös organisaation yleisen ja järjestelmällisen hallinnoinnin tukena, ainakin siinä mielessä, että ISO/IEC 27001:2017 –standardin vaatimusosan tarkastelun myötä tutustutaan keskeisiin osa-alueisiin organisaatiossa, prosesseissa ja sen turvallisuutta edistävässä toiminnassa. Tutkimusongelmana on avata havainnollistavien ongelmien ratkaisujen myötä aiheen peruskysymyksiä, jotta menetelmän sisäistämisen avulla saavutetaan uutta ymmärrystä standardoinnin käyttöönoton käytännön haasteista.

ISO/IEC 27001:2017 –standardissa on käytännössä pääpiirteittäin samat käyttöönoton esivaiheet kuin useissa fyysisen turvallisuuden järjestelmissä, kun halutaan ymmärtää organisaation sisäisiä ja ulkoisia seikkoja: tavoitteiden määrittäminen, alkusuunnittelu tai kartoitus, suunnittelun arviointi ja monissa tapauksissa uudelleensuunnittelu tai järjestelmän tarkentaminen (Garcia 2008, 3; ISO/IEC 27003:2017, 7-9).

Standardin ISO/IEC 27001:2017 mukaisesta tietoturvallisuuden hallintajärjestelmästä kiinnostunut taho voi opinnäytetyön perusteella saada hyödyllisen kuvan siitä, millaisista seikoista kokonaisuus koostuu ja miten hallintajärjestelmä mukautuu olomassaoleviin tietoturvallisuuden ratkaisuihin ja turvallisuuskulttuuriin. Ensimmäisten vaiheiden joukossa on tutustua organisaation toimintaan ja tarpeisiin tietoturvallisuuden osalta, jotta hallintajärjestelmä saadaan

osaksi prosesseja ja yleisiä johtamis- ja hallintarakenteita ja että se on kiinnittyneenä niihin (ISO/IEC 27003:2017,13).

Opinnäytetyön teoreettinen tausta muotoutuu käytettyjen tietoturvallisuuden käsitteiden määrittelystä ja tapaustutkimuksen havainnollisten esimerkkien peilaamisesta standardin vaatimuksiin. Tutkin, millaisia prosesseja käynnistyy, kun organisaation turvallisuuskulttuurin käytännöt kytketään standardin edellyttämiin jatkuvan parantamisen periaatteisiin. Työn tarkoituksena on siis käytännön esimerkkien avulla osoittaa, minkälaisia tekijöitä ja mahdollisia ongelmakohtia voi esiintyä, kun organisaatiossa halutaan toteuttaa ISO/IEC 27001 –standardin mukaista tietoturvan hallintajärjestelmää. Tietotausta ja -perusta on syntynyt käytännön työtehtävieni myötä työskennellessäni tietoturvakonsulttina ulkoministeriön ISO/IEC 27001 –standardin käyttöönottoprojektin parissa ja sen luomisen eri vaiheissa. Tuona aikana aloin pohtia havainnollista tapaa kuvata selkeästi paitsi itse standardia myös mahdollisia ongelmakohtia sen käyttöönoton eri työvaiheissa. Ulkoministeriössä pyritään siihen, että ISO/IEC 27001 –standardin mukainen tietoturvallisuuden hallintajärjestelmä saadaan sertifioitua.

Opinnäytetyössä tarkastellaan käytännön havainnollistavien esimerkkien avulla tapoja, joilla organisaatio saavuttaa vaatimuksenmukaisuuden osa-alueilla, jotka vaativat toimenpiteitä. Tavoitteena on havainnollistaa, että ISO/IEC 27001 –standardia voi tarvittaessa tarkastella myös eräänlaisena menetelmänä, jonka avulla voidaan toteuttaa organisaation sisäistä ongelmanratkaisua aiheissa, joissa kehitystyö on välttämätöntä, jotta vaatimuksenmukaisuus mahdollistuu. Tästä käytännönläheisyydestä johtuen myös standardin vaatimusosat tulevat helpommin ymmärrettäviksi. Alussa keskeinen vaihe on tutustua organisaation sisäiseen ja ulkoiseen toimintaympäristöön, koska sen jälkeen standardin vaatimukset voidaan sovittaa asianmukaisesti, jolloin tietoturvallisuuden kokonaisuudesta tulee hallittu (ISO/IEC 27003:2017, 47).

1.2 Tutkimusmenetelmät sekä tietoperustan teoreettinen viitekehys

Tutkimustyön luonteen mukaan tulee valita aiheen käsittelyyn soveltuva menetelmä tutkia aiheen tutkimuskysymyksiä. (Aaltola & Valli 2007, 19). Opinnäytetyössä tarkoitus on tuoda yleistä ymmärrystä esitellystä standardista ja tarkastella tietoturvan järjestelmän hallintaa standardin vaatimusten valossa. Painotus on vahvasti menetelmän esittelyssä, ongelmanratkaisussa, standardin sovittamisessa organisaation tavoitteisiin sekä yleisen turvallisuuskulttuurin edistämisen muistamisessa.

Tapaustutkimuksessa tutkittavana kohteena on yksittäinen tapahtuma tai esimerkiksi rajattu kokonaisuus, jolloin käytetään monipuolisesti hankittuja ja erilaisilla tavoilla saatuja tietoaineistoja. Tapaustutkimuksen avulla tavoitteena on tutkia, kuvata ja selittää tapauksia pääosin kysymällä *miksi*- sekä *miten*-kysymyksiä (Yin 1994, 5-13). Tutkimusmenetelmät tässä opinnäytetyössä ovat tapaustutkimuksia, mutta mukana on myös piirteitä konstruktiivisen tutkimuksen keinoista, erityisesti, kun esitettyjen ongelmien seurauksena pyritään esittämään uusia ratkaisumalleja standardin vaatimuksien täyttämiseksi analyysi- ja kehittämisvaiheiden päätteeksi.

Menetelmällisenä ratkaisuna on käytetty myös erilaisia soveltamiskäytäntöjä, joissa yhdistyvät ongelmanratkaisukeskeisyys, havainnollistavat tapaukset, uuteen ymmärrykseen pyrkiminen ja toimet, jotka johtavat vaatimusten mukaisiin ratkaisuihin. (Vrt. esim. Hirsjärvi, Remes & Sajavaara 2002, 121-122). Lisäksi tarkastellaan erilaisia ongelmanratkaisumalleja (DSR-, CWA- ja STS-menetelmiä), joiden avulla pyritään saamaan uusia virikkeitä ja näkökulmia hankaliin ja aikaa vieviin ongelmiin ISO 27001 –standardin käyttöönotossa.

Kun ISO/IEC 27001 –standardin asiantuntija tutustuu organisaatioon saadakseen tarkan kuvan sen toimintaympäristöstä ja toiminnasta, hän on tekemisissä erilaisten ja eritasoisten narratiivien kanssa kuunnellessaan selostuksia, esityksiä ja arvioita. Myös kirjallisissa materiaaleissa, raporteissa ja dokumentaatioissa on narratiivisia aineksia. Tässä yhteydessä onkin hyvä tiedostaa, että kun asiantuntija tutustuu itselleen vieraaseen organisaatioon, häneltä vaaditaan riittävää kykyä narratiivien analyysiin. Tätä ei tule kuitenkaan sekoittaa narratiiviseen analyysiin, mikä on ennen kaikkea tutkimuksellinen menetelmä. (Aaltola & Valli 2010, 149)

Tutkimusmenetelminä käytetään havainnollistavaa tapaustutkimusta ja lähinnä konstruktiivista tutkimusmetodia, jossa esitetyn ongelmakysymyksen analyysin ja juurisyiden kartoittamisen myötä siirrytään kehittämisen vaiheisiin, minkä jälkeen luodaan uusi asetelma tai tietoturvallisuuden rakenne standardin vaatimukset huomioiden tai vaihtoehtoisesti mikäli kysymyksen kompleksisuudesta johtuen selkeää suljettua ratkaisua ei tule antaa, ongelma jäte-

tään tietyiltä osin avoimeksi. Tarkoitus ei siis ole antaa kiistattomia vastauksia esimerkkiongelmiin, vaan tutustuttaa lukija yksittäisten tietoturvallisuustekniikoiden sijaan tietoturvallisuuden hallintajärjestelmän menetelmiin käymällä läpi mahdollisia ratkaisumalleja ISO/IEC 27001:2017 –standardista.

Ote opinnäytetyössä on ensi sijassa havainnollistava, esimerkkeihin pohjaava, konstruktiivinen ja ratkaisuhakuinen. Usein kokonaisturvallisuuden ja tietoturvallisuuden hallinnan järjestelmät tukevat toisiaan niissä tapauksissa, joissa toimijatahot ovat yhtä mieltä siitä, että standardien avulla on mahdollista saavuttaa laajempaa johdonmukaisuutta, yhtenäisyyttä ja vertailtavuutta turvallisuusratkaisuissa. Kokonaisturvallisuuteen pyrkiminen on eräänlaisena johtoajatuksena myös tässä opinnäytetyössä, ja sen vuoksi tutkimuksessa esitetään myös vaihtoehtoisia tai pikemminkin täydentäviä hallintajärjestelmän analyysin ja kehittämisen keinoja niiltä osin, kuin ne tukevat ISO/IEC 27001 –standardin edellyttämää riskienhallintaa. Näitä tapoja ovat esimerkiksi riskien käsittelytoiminta, tietoturvariskien hallintaprosessi ja ISMS-järjestelmän vaikuttavuuden mittaaminen.

Vertailukohtia erilaisiin turvallisuutta käsitteellistäviin jäsentelyihin tavoitellaan muun muassa EK:n turvallisuusmallin esittelyllä. Kyseinen malli ei suoranaisesti liity ISO/IEC 27001 –standardiin, mutta sitä voidaan käyttää turvallisuuskokonaisuuden ymmärtämisen apuna eikä se ole ristiriitainen suhteessa standardiin. Lisäksi käytössä oleva sanasto on valittu sillä periaatteella, että se kestää aikaa ja muuttuvia (tieto)turvallisuusolosuhteita, joten vaikka käytössä olevan tietoturvakäsitteistön julkaisusta onkin kulunut jo aikaa, on perustermit valittu siten, että ne ovat edelleen ajankohtaisia. Huomioitavaa on, että standardia ei varsinaisesti pyritä esittämään kokonaisuudessaan, sillä opinnäytetyön ei ole tarkoitus olla tässä mielessä kattava. Havainnollistavan otteen tarkoitus on ensisijaisesti johdattamaan aiheeseen tutustuminen yleisen menetelmän ymmärtämiseen.

Rakenteellisesti teoreettinen tausta ilmenee seuraavasti: ISO/IEC 27001 –standardia esitellään ensin luvussa kaksi yleisesti ja sen jälkeen vaatimuksien osalta siten, että apuna käytetään standardia, tämän jälkeen seuraavassa luvussa esitetään kuvitteellisia esimerkkiongelmia, jonka jälkeen niiden analyysissä etsitään juurisyitä ja lopuksi ongelmille etsitään ratkaisuja ensisijaisesti standardista tai standardin ohjeistuksista sekä edellä kuvatuista ongelmanratkaisumenetelmistä. Lopulta opinnäytetyön loppupuolella käsitellään johtopäätöksiä ja tuloksia. Kuvioiden ja tietoturvallisuuden vaihtoehtoisten mallien esittelyllä pyritään paitsi saamaan hyödyllisiä näkökulmia standardin ratkaisumalleille, myös ilmaisemaan, että erilaisille riskienhallintamenettelyille on tilaa ISO/IEC 27001 –standardissa, jolloin ne omilta osiltaan tukevat vaatimuksenmukaisen tietoturvallisuuden hallintajärjestelmän jatkuvaa parantamista. Tieteellisessä tutkimuksessa empiirisen tutkimuksen *havaintoja* ei koskaan itsessään pidetä tuloksina, eli asioita ei oteta sellaisina kuin miltä ne näyttävät. Havaintoja pidetään vain johtolankoina, joita jollain tavalla tulkiten pyritään pääsemään havaintojen ”taakse”. (Alasuutari

2011, 78.) Tämä ymmärrys toteutuu myös tässä opinnäytetyössä, erityisesti, kun analyysi kohdistuu ongelmien juurisyihin.

Käytän tässä opinnäytetyössä ISO/IEC 27003:2017 –ohjeistusta ja kolmea ongelmanratkaisumallia, jotka ovat: 1) DSR - Design Science Research framework; 2) STS - Socio-technical Systems ja 3) CWA - Cognitive Work Analysis, joiden ominaisuuksia ja soveltuvuutta avataan suhteessa ongelmien luonteeseen. Näitä ongelmanratkaisumalleja ja niiden ominaisuuksia esitellään lyhyesti, minkä jälkeen luvussa 4.2. arvioidaan, miten standardi voidaan ottaa käyttöön ja minkälaiset perusehdot tätä käyttöönottoa edeltävät.

1.3 Miksi kehittämistyö on tärkeää

ISO/IEC 27001 –standardi on suunnattu tietoturvariskien hallinnasta vastaaville johtajille ja henkilöstölle organisaatiossa – lisäksi joissain tapauksissa myös tätä toimintaa tukeville tahoille ulkopuolelta (SFS-käsikirja 327: 2012, 309). ISO/IEC 27001 –standardin mukaisella tietoturvan hallintajärjestelmällä haetaan useita hyötyjä. Ensinnäkin ISO:n ja IEC: sääntöjen mukaan standardien on oltava yhteensopivia SL:n mukaisten hallintajärjestelmästandardien kanssa (ISO/IEC 27001: 2017, 5). Tämän johdosta yhtenäisistä käytännöistä saadaan hyötyä johtamistasosta lähtien, koska toiminnan rakennetta ohjaavat käytännöt yhtenäistyvät ja tehostuvat organisaatioissa, joissa useampia standardeja on käytössä. Lisäksi ISO/IEC 27001 –standardi perustuu siis siihen, että se yhtenäistyy saumattomasti organisaation hallintarakenteisiin. (ISO/IEC 27001: 2017, 5.) Näin standardin ulkopuolisista käytännöistä on mielekkäintä jopa luopua niissä tilanteissa, joissa pyritään purkamaan tarpeettomia tai päällekkäisiä rakenteita organisaation tietoturvallisuuden hallinnassa.

Kehittämistyö on eräs esimerkki siitä, miten organisaatiossa ei pelkästään enää sitouduta yksittäisen kehittämisprosessin myötä saavutettavaan tulokseen, koska standardin jatkuvan parantamisen periaatteen mukainen kehittäminen yhtenäistää muutoin irrallisia prosesseja seuratusti, mitattavasti ja arvioidusti (ISO/IEC 27001: 2017, 12-13). Tämä ei kuitenkaan tarkoita, että organisaation johtamisen tai hallinnoinnin järjestelmiä pyrittäisiin muuttamaan, koska standardin vaatimusosassa todetaan, että hallintajärjestelmän vaatimukset yhdistetään organisaation prosesseihin (ISO/IEC 27001: 2017, 7). Kyse on vain lähinnä siitä, *miten* prosesseja toteutetaan jatkossa, jotta standardin vaatimuksenmukaisuus saavutetaan. Mitattavuustestausten avulla voidaan arvioida, miten suuri prosentuaalinen osa organisaation toiminnasta täyttää ISO/IEC 27001 –standardin vaatimukset. Arvioinnissa keskeisessä osassa on sen tutkiminen, toimiiko kokonaisuus vaatimusten edellyttämällä tavalla. On huomattava, että saattaa ilmetä tilanteita, joissa yksittäinen hallintakeino ei vaikuta riittävältä, mutta kokonaisuutta tarkasteltaessa havaitaan, että vaatimuksenmukaisuus täyttyy silti erinomaisesti. Näissä tilanteissa erillistä tai yksittäistä kontrollia ei ole syytä painottaa kokonaisuuden kustannuksella.

(Garcia 2008, 9.) Standardin keskeisellä käsitteellä, jatkuvalla parantamisella, tarkoitetaan, että organisaatio sitoutuu kehittämään tietoturvallisuuden hallintajärjestelmän soveltuvuutta, tarkoituksenmukaisuutta ja vaikuttavuutta (ISO/IEC 27003:2017, 46). Jatkuvassa parantamisessa huomioidaan se, että organisaatiot eivätkä niiden toimintaympäristöt ole ikinä muuttumattomia. Tämän lisäksi tietojärjestelmiin kohdentuvat riskit muuttuvat nopeasti, joten aina on oltava keinoja hallintajärjestelmän kehittämiseen, vaikka toimintaympäristö ei olisikaan muuttumassa. (ISO/IEC 27003:2017, 47.)

Jatkuva parantaminen ei ole ainoastaan ISO/IEC 27001:2017 -standardin ominaispiirre, sillä useissa fyysisen turvallisuuden järjestelmissä on käytössä vastaavia prinsiippejä. On tyypillistä, että eri käyttöönoton vaiheiden lopuksi suoritetaan analyysiprosessi, jossa arvioidaan järjestelmän haavoittuvuuksia ja tarkastellaan ovatko suojelutavoitteet saavutettu. Tämän jälkeen analysoidaan määräajoin, onko alkuperäiset suojaustavoitteet syytä pitää ennallaan ja että järjestelmä on edelleen vaikuttava (Garcia 2008, 5-6). Standardoidun hallintajärjestelmän etuina on myös se, että tietoturvavastuut ja -valtuudet jakautuvat tasaisemmin kaikkien organisaation työntekijöiden roolin mukaisesti, jolloin on mahdollista keskittyä työn sisältöön ja laadulliseen kehittämiseen (ISO/IEC 27001: 2017, 7).

1.4 Aiheen rajaaminen ja tutkimuskysymykset

Tässä työssä ei ensi sijassa juurikaan oteta kantaa siihen, **miksi** standardeja tulisi hyödyntää eikä siihen, että tarkasteltaisiin kriittisesti ISO/IEC 27001 -standardia. Syy tähän on ennen kaikkea käytännöllinen: standardit ovat maailmanlaajuisesti käytössä ja niiden katsotaan yleisesti ottaen tehostavan toimintaa. Tämä opinnäytetyö on koostettu siten, että siitä on hyötyä organisaation ylimmälle johdolle, (tieto)turvallisuusjohdolle ja hallinnasta vastaaville tahoille, jotka ovat kiinnostuneita ISO/IEC 27001 -standardin ominaisuuksista. Kattavaa aiheenkäsittelyä ei harjoiteta, koska organisaatioiden tietoturvallisuuskokonaisuudet ovat laajoja ja jokaisella toimijalla on käytössä omanlaisia ratkaisuja. Sen vuoksi näkökulman valinnassakin huomioidaan, että nopeasti omaksuttava tapa ymmärtää ISO/IEC 27001 -standardin erityispiirteitä on havainnollistusten avulla. Toinen tehokas keino on perehtyä standardin vaatimusosaan ja jokaisen kohdan osalta miettiä erikseen, mitä tämän vaatimuksen toteuttaminen vaatisi organisaatiossa. Todettakoon tässä yhteydessä, että kyseisiä vaatimuskohtia standardissa ovat kohdat 4-10, jotka ovat:

4. Organisaation toimintaympäristö

5. Johtajuus

6. Suunnittelu

7. Tukitoiminnot

8. Toiminto

9. Suorituskyvyn arviointi

10. Parantaminen

Aiheen käsittely rajautuu siis enimmäkseen näihin vaatimusosiin, vaikka yksittäisissä tapauksissa käsitellään myös hallintakeinoja, joihin kuuluvat myös muun muassa tietoturvapolitiikat ja viestintäturvallisuus. Tässä työssä esitetään siis ensisijaisesti standardin vaatimusosat, jotta tulee ymmärrettäväksi, mitä niillä tarkoitetaan. Aiheen rajauksen ja esimerkinomaisten havainnollisten ongelmien ansiosta, tähän opinnäytetyöhön ei tarvitse liittää salassa pidettäviä tietoja.

Ensisijaisia tutkimuskysymyksiä ovat:

- **mikä** on ISO/IEC 27001 -standardi
- **mihin** ISO/IEC 27001 liittyy
- **miksi** ISO/IEC 27001 tulisi ottaa käyttöön
- **miten** ISO/IEC 27001 voidaan ottaa käyttöön

Toissijaisena tutkimuskysymyksenä on myös tarkastella **miten**, **millä tavoilla** ja **miksi** ISO/IEC 27001 -standardi yhdistyy organisaation prosesseihin ja yleisiin johtamis- ja hallintarakenteisiin. Tukea antavana tutkimuskysymyksenä arvioidaan keinoja, joiden avulla mahdollisia ongelmia ISO/IEC 27001 –standardin mukaisen tietoturvallisuuden hallintajärjestelmän käyttöönottoon liittyen voidaan ratkaista, joten opinnäytetyössä vastataan siihen, **miten** standardi voidaan ottaa käyttöön. Opinnäytetyössä käytettävät ongelmatapausesimerkit ovat kuvitteellisia ja niiden on tarkoitus havainnollistaa todellisia esteitä ja hidasteita, joita saattaa esiintyä siirryttäessä ISO/IEC 27001 –standardin mukaisen tietoturvallisuuden hallintajärjestelmän käyttöön. Miksi sitten käytetään kuvitteellisia esimerkkejä eikä eikä vaikkapa kyselytutkimuksen avulla selvitettyjä case-tyyppisiä ongelmia? Syy tähän on se, että standardia on vaikeaa ymmärtää ja mikäli esitetään todellisia ongelmatapauksia, lukijan huomio kohdistuu liiaksi yksittäisiin ratkaisukeinoihin, mikä ei ole hyödyllistä, koska yleisten ongelmanratkaisuja tukevien menetelmien ymmärtäminen on tämän opinnäytetyön päämääränä. Mikäli haluaa tutustua esitetyn kaltaiseen tutkimukseen, kannattaa lukea Joffre Velascon, Rodrigo Ullaurin, Luis Pilicitan, Bolívar Jácomen, Pablo Saan ja Oswaldo Moscoso-Zean case-tutkimus Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry vuodelta 2018.

2 Standardi ISO/IEC 27001:2017

Tässä opinnäytetyössä on keskeistä esitellä myös ISO/IEC 27001 –standardin sisältöjä. Työssä ei referoida vaatimuskohtia, mutta tavoitteena on selventää vaatimusten sisältöä ymmärrettävästi siten, etteivät tiedot vääristy. Järjestys, jossa vaatimuskohdat esitetään on kuitenkin kronologisesti yhteneväinen standardin suhteen. Tarkoituksena on tehdä ymmärrettäväksi, mitä tarkoitetaan sillä, että ISO/IEC 27001 –standardia kutsutaan tietoturvallisuuden hallintajärjestelmäksi. Syy, miksi vaatimusosat esitetään tässä työssä on se, että ne kiinnittyvät oleellisesti kysymykseen, **miten** ISO/IEC 27001 –standardin mukainen tietoturvallisuuden hallintajärjestelmä otetaan käyttöön organisaatiossa.

2.1 ISO/IEC 27001:2017 - mikä se on

Tässä luvussa esitellään ISO/IEC 27001:2017 –standardin vaatimusosien sisältöjä samassa kronologisessa järjestyksessä kuin ne esitetään itse standardissa. Vaatimusosien esittämisjärjestys ei sinällään ole kriittinen kysymys, koska lähtökohtana on joka tapauksessa, että kaikki näiden kohtien vaatimukset täyttyvät organisaatiossa. ISO (International Organization for Standardization) sekä IEC (International Electrotechnical Commission) muodostavat järjestelmän, joka erikoistuu maailmanlaajuiseen standardisointiin. ISO:n ja IEC:n teknilliset komiteat toimivat yhteistyössä kumpiakin osapuolia koskettavilla osa- ja aihealueilla. Kansainvälisiä standardeja laadittaessa ISO ja IEC noudattavat yhteisiä sääntöjä (ISO/IEC Directives). Kansainvälisten standardien julkaisemiseksi on saatava vähintään 75 % kannatus kansallisten jäsenjärjestöjen äänestäessä. (ISO/IEC 27001: 2017, 3.)

Tässä opinnäytetyössä käytettävä versio standardista on ISO/IEC 27001:2013 (“Information technology. Security techniques. Information security management systems, Requirements”). Tämä versio on sisällöllisesti täsmälleen sama kuin myös käytössäni oleva ISO/IEC 27001:2017 (“Information technology. Security techniques. Information security management systems, Requirements). Sovellusohjeet hallintakeinoista on standardissa ISO/IEC 27002:2017 (Information technology. Security techniques. Code of practice for information security controls – ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015). Mittauksen ja hallintajärjestelmän vaikuttavuuden testaamiseen suositellaan standardia ISO/IEC 27004:2016. Tietoturvallisuuden mittaustoiminnassa on toimintoja, joilla varmistetaan, että laaditut mittaustulokset tuottavat täsmällistä tietoa toteutetusta ISMS-järjestelmästä, turvamekanismeista tai turvamekanismiyhdistelmien vaikuttavuudesta ja sopivista parannustoimenpidetarpeista (SFS-käsikirja 327:

2012, 264). Syy tämän opinnäytetyön tekemiseen oli, että toimintakulttuurin sisäiset rakenteet voivat tuottaa ongelmia standardien käyttöönotossa.

ISO/IEC 27001:2017 -standardin perusperiaatteisiin kuuluu tietynlainen joustavuus, eli esimerkiksi mikäli kohdeorganisaatio muuttuu rakenteellisesti merkittävästi tai alkaa käyttää esimerkiksi pilvipalveluita tallentamiskeinona, standardi kykenee ulottamaan hallintajärjestelmäkontrolleja myös uusiin olosuhteisiin. Tässä merkittävänä apuna on se seikka, että ISO/IEC –standardit ovat täysin yhteensopivia muiden ISO –julkaisujen kanssa (esimerkiksi pilvitallennuksista on julkaistu omat ISO –ohjeistukset, vaikka niillä ei olekaan suoranaista yhteyttä ISO/IEC 27001:2017 -standardiin). (ISO/IEC 27001: 2017, 5.) Joustavuus näyttäytyy vahvasti myös hallintakeinojen mukautuvuutena, koska menettelyohjeiden mukaan hallintakeinoja ollaan velvoitettuja valitsemaan organisaation tarpeiden määrittämänä (ISO/IEC 27001: 2017, 5). Liite A:n luettelo hallintatavoitteista ja –keinoista ei ole täydellinen, sillä siinä esitettyjen lisäksi voi tietyissä tapauksissa olla tarpeen käyttää muita hallintatavoitteita ja –keinoja (ISO/IEC 27001: 2017, 8).

Standardissa todetaan myös, että organisaation tietoturvallisuuden hallintajärjestelmän luontiin ja toteuttamiseen vaikuttavia tekijöitä ovat muun muassa organisaation tarpeet ja tavoitteet, turvallisuusvaatimukset, käytettävät organisaatioprosessit sekä organisaation koko ja rakenne. Keskeistä standardin näkökulmasta on, että kaikkien näiden tekijöiden odotetaankin muuttuvan ajan saatossa. (ISO/IEC 27001: 2017, 5.) Edellä käsiteltyjen perusprinsiippien ja käsitteiden avaamisen jälkeen on kuitenkin mielekästä palata väliotsikon kysymykseen ja pyrkiä vastaamaan havainnollistavalla tavalla, mikä standardi on. Lyhyesti sanoen standardi on 46-sivuinen teksti, jossa esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset (ISO/IEC 27001: 2017, 5). Ydinteksti koostuu kahdesta osasta, joista ensimmäisen, eli kohtien 4-10, vaatimuksia on noudatettava, mikäli organisaatio haluaa sertifioida standardin (ISO/IEC 27001: 2017, 5). Toinen osa, liite A, on hallintatavoitteiden ja –keinojen viiteluettelo, joita ei sertifioida, vaikka ne käytännössä ovatkin merkittävässä osassa standardin käyttöönoton kaikissa vaiheissa.

Standardin kohdissa 4-10 esitetään vaatimuksia, joiden avulla voidaan määrittää jäsennellysti organisaation ulkoisia ja sisäisiä seikkoja. Kohta neljässä päämääränä on ymmärtää organisaation toimintaympäristöä, sidosryhmien tarpeita ja tietoturvallisuuden hallintajärjestelmää. Viidennessä kohdassa painotetaan johtajuutta ja sitoutuneisuutta, tietoturvapolitiikkaa sekä rooleja, vastuita ja valtuuksia organisaatiossa. Kuudennessa käsitellään riskejä ja mahdollisuuksia, tietoturvariskejä sekä tietoturvatavoitteita ja niiden saavuttamiseen vaadittavien toimenpiteiden suunnittelua. (ISO/IEC 27001: 2017, 6-10.)

Seitsemännessä kohdassa painotetaan tukitoimintoja, joita ovat resurssit, pätevyyteen liittyvät kysymykset organisaatiossa, organisaatiossa työskentelevien henkilöiden tietoisuus oleellisista hallintajärjestelmää koskevista vaatimuksista, viestintäkäytännöt sekä dokumentoituun tietoon liittyvät ohjeistukset ja hallinnat. Kahdeksannessa kohdassa esitetään toiminnan suunnitteluun ja ohjaukseen liittyviä käytäntöjä sekä tietoturvariskien arviointia ja käsittelyä organisaatiossa. Kohta yhdeksän on suorituskyvyn arviointi ja tähän kuuluvat osa-alueet ovat: seuranta, mittaukset, analyysit ja arvioinnit, sisäinen auditointi ja johdon katselmus. Viimeisessä eli kymmenennessä kohdassa ydinalueina ovat parantaminen, poikkeamat ja korjaavat toimenpiteet sekä jatkuvan parantamisen periaate. Hallintakeinoja eli kontrolleja on vuoden 2013 standardissa 114 kappaletta. Hallintakeinot kohdentuvat edellä esiteltyjen vaatimuskohtien 4-10 osa-alueisiin. (ISO/IEC 27001: 2017, 10-14.)

2.2 Vaatimusosan kuvailua

Kansainvälisessä standardissa ISO/IEC 27001:2017 esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset. Käytännössä hallintajärjestelmän luominen edellyttää tiivistä ja useimmissa tapauksissa aikaa vievää projektityötä, jossa asiantuntijat perehtyvät organisaatioon, selvittävät yksityiskohtia, tapaavat toimijoita ja vastuuhenkilöitä, pitävät palavereja, joissa keskitytään eri osa-alueisiin ja valvovat edistymistä aikataulujen puitteissa. Organisaation tarpeet ja tavoitteet, turvallisuusvaatimukset, käytettävät organisaatioprosessit sekä organisaation koko ja rakenne vaikuttavat useisiin asioihin. Tarvittavat resurssit mahdollistavat mahdollisimman nopean etenemisen ja mahdolliset esteet ja hidasteet on helpompi raivata tieltä, mutta isoissa organisaatioissa toimintaan perehtyminen on useissa hidasta, varsinkin jos aiemmin tietoturva- ja hallintajärjestelmäasiat on hoidettu mielivaltaisesti. Tulisi noudattaa kokonaisvaltaista ja koordinoitua lähestymistapaa. (ISO/IEC 27002:2017, 6.) Täsmällinen ja ajantasainen dokumentaatio on keskeinen seikka, jolla prosessia voidaan tehostaa, koska sertifiointivaiheeseen pääseminen edellyttää, että kaikista vaatimusosan toimista raportoidaan tarkasti määritetyllä tavalla (Vrt. ISO/IEC 27001:2017, 5).

Standardi on muodostettu sillä ajatuksella, että suojattavan tiedon luottamuksellisuus, eheys ja saatavuus eivät vaarannu, vaikka organisaation oleellisimmat rakenteet muuttuvatkin, mikä käytännössä tarkoittaa sitä, että standardin mukaisen ISO/IEC 27001 hallintajärjestelmän luominen organisaatiolle sitouttaa tahot pitkän tähtäimen kehitystyöhön, koska oleellinen osa hallintajärjestelmäkehitystä on jatkuvaan parantamiseen ryhtyminen. Näin ollen normaalit organisaatiota koskevat vaihtelut tai muutokset eivät horjuta standardin toimivuutta, mikä tarkoittaa sitä, että standardin avulla voidaan saavuttaa merkittävästi suurempi johdonmukai-

suuden ja vakauden taso kuin ilman sitä. (Vrt. ISO/IEC 27002:2017, 6.) Tämä on etu myös hieman pienemmissä organisaatioissa, joissa organisaation rakenteelliset seikat eivät välttämättä ole täysin loppuun asti mietittyjä, sillä standardin avulla on mahdollista luoda toimivia ja pitkän tähtäimen näkökulmasta katsottuna kestäviä reunaehtoja toiminnalle (Ks. ISO/IEC 27001: 2017, 5).

Hallintajärjestelmän on siis oltava osa organisaation prosesseja ja johtamis- ja hallintarakenteita ja on tärkeää, että se on yhdistetty niihin (ISO/IEC 27001: 2017, 5; ISO/IEC 27002:2017, 6).) Ei ole mahdollista luoda vaatimusten mukaista ISO/IEC 27001 hallintajärjestelmää kattavasti siten, että vaatimukset toteutuvat puutteellisina. Tästä syystä asiantuntijan pitää ymmärtää organisaation tavoitteiden yksityiskohdat ja päämäärien muodostamat kokonaisuudet ja niiden vaikutukset organisaation käytännön toiminnassa. Standardin mukaisessa toiminnassa tietoturvallisuus huomioidaan, kun suunnitellaan prosesseja, tietojärjestelmiä ja hallintakeinoja, mikä näyttäytyy muun muassa siinä, että toimintojen erilaiset vaiheet, siirtymät ja tietoturvakäytännöt analysoidaan ja kirjataan dokumentteihin, jotta mahdolliset heikkoudet tulevat tiedostetuiksi. Tässä yhteydessä tietoturvaan liittyvät toimenpiteet ja ratkaisut eivät ole ulkoapäin annettuja vaan tietoturvallisuus kytkeytyy täysin saumattomasti kaikkiin organisaation tekemiin päätöksiin ja toimintoihin – näin siis vaatimusten mukaisessa hallintajärjestelmässä. Käänteisesti voidaan esittää arvio, että tietoturvallisuus ei välttämättä käytännössä muodosta lähimainkaan riittävää kattavuutta ja aukottomuutta, mikäli asian tärkeyttä ei tiedosteta organisaatioissa, jolloin vaikuttavuus ei ole riittävää. (Vrt. ISO/IEC 27002:2017, 6.)

Keskeinen oletus on, että hallintajärjestelmä on organisaation tarpeiden mukainen ja että sisäiset ja ulkoiset sidosryhmät voivat standardia hyödyntämällä arvioida organisaation kykyä täyttää tietoturvavaatimuksia. (ISO/IEC 27001:2017, 5) Standardin mukaisella ISO/IEC 27001 -hallintajärjestelmällä on siis mainehyötyjä liittyen muun muassa ulkoisiin sidosryhmiin ja muihin tavoitteiden mukaisiin ratkaisuihin yhteistyötahoihin liittyen, koska esimerkiksi tilanteessa, jossa kaksi ISO/IEC 27001 –sertifioitua toimijaa ryhtyvät yhteistyöhön, kumppanin luotettavuus on tavallista nopeammin ja vähäisemmillä varmistuskeinoilla todennettavissa (Vrt. SFS-käsikirja 327: 2012, 85).

2.3 ISO/IEC 27001 –vaatimusosat

Seuraavassa alaluvussa esitellään ISO/IEC 27001 –vaatimusosat siinä järjestyksessä kuin ne standardissakin kuvataan. Tarkoituksena on, että lukija saa nopeasti ja selkeästi käsityksen siitä, mitä vaatimusosat ovat ja mihin niillä pyritään, koska mikäli itse standardin sisältöä ei käsiteltäisi millään tavalla, lukijan olisi hyvin haasteellista ymmärtää, mitä ISO/IEC 27001 –standardilla tarkoitetaan. Standardivaatimuksia ei ole luvallista sellaisenaan toistaa eikä varsinkaan muokata, mutta asiantuntija voi silti kuvata määrityksiä, mikäli on aidosti sisäistänyt

sisällöt ja noudattaa huolellisuutta. Tästä syystä vaatimusosien kuvailussa ei käytetä ulkopuolisia lähteitä itse standardin lisäksi, jotta keskeinen viesti eli vaatimuksien sisältö ei vääristyisi.

2.3.1 Organisaation toimintaympäristö

Organisaatio määrittää omien päämääriensä kannalta oleellisimmat ulkoiset ja sisäiset seikat, koska nämä vaikuttavat sen mahdollisuuksiin saada toivotut hyödyt tietoturvallisuuden hallintajärjestelmältä. Ulkoiset ja sisäiset seikat organisaatiossa viittaavat esimerkiksi tietojärjestelmiin tai toimintoihin sekä näihin liittyviin vaatimuksiin. On todennäköistä, että mikäli organisaatio määrittää, analysoi ja dokumentoi tavoitteensa ja toivomansa hyödyt tietoturvallisuuden hallintajärjestelmältä, toiminta tehostuu, kevenee ja virtaviivaistuu kokonaisuudessaankin, mikä lisää tietoturvallisuuden hallintaa. (Ks. ISO/IEC 27003, 7.) Keskittymällä ulkoisiin ja sisäisiin asioihin ja näihin kytkeytyviin vaatimuksiin, oma organisaatio ja sen toiminnot tulevat tutuksi, jolloin tarpeettomiin toimenpiteisiin ei tarvitse ryhtyä, tyhjäkäynti vähenee ja resurssit ovat kohdennettavissa tarkemmin. (ISO/IEC 27001: 2017, 5-6; Vrt. SFS-käsikirja 327: 2012, 4.)

Organisaatio määrittelee keskeiset sidosryhmänsä (esimerkiksi asiakkaat, yhteisöt, alihankkijat, kumppanit) sekä vaatimukset, jotka nämä sidosryhmät asettavat tietoturvallisuuden kannalta. Näin toimimalla on mahdollista saavuttaa jopa kilpailuetuja, koska sisäisen ja ulkoisen toiminnan välinen rajapinta täsmentyy, jolloin organisaatiossa voidaan arvioida, mihin toimiin kannattaa ryhtyä, mihin on välttämätöntä ryhtyä ja milloin on syytä välttää tiettyjä asioita. Näin havaitaan, että tietoturvan ISO/IEC 27001 -standardin mukaisilla ja sen edellyttämillä toimilla, ja niihin liittyvän asiayhteyden avulla, voidaan samanaikaisesti ymmärtää myös toimintaympäristön tilaa tarkemmin. Standardin määrittelemiä vaatimuksia on siis kolmenlaisia: ulkoisiin ja sisäisiin seikkoihin liittyviä vaatimuksia sekä sidosryhmätoiminnan asettamia vaatimuksia. Sidosryhmiin liittyvät vaatimukset saattavat olla esimerkiksi lakisääteisiä vaatimuksia, viranomaisten vaatimuksia sekä sopimusvelvoitteita. (ISO/IEC 27001: 2017, 5-6; SFS-käsikirja 327: 2012, 88.)

Toimintaympäristöä analysoidaan kolmesta syystä: siksi, että hallintajärjestelmän soveltamisalasta voidaan päättää, jotta riskit ja mahdollisuudet kyetään määrittämään ja sen vuoksi, että voidaan varmistaa, että hallintajärjestelmä mukautuu ulkoisten ja sisäisten seikkojen muuttuessa (ISO/IEC 27003: 2017, 7). Soveltamisalan määrittäminen on keskeinen toimenpide siksi, että sen avulla luodaan perusta kaikille muille toiminnoille (ISO/IEC 27003: 2017, 10).

2.3.2 Johtajuus: sitoutuminen, tietoturvapolitiikka sekä roolit, vastuut ja valtuudet

Ylimmän johdon tulee osoittaa johtajuutta ja sitoutuneisuutta tietoturvallisuuden hallintajärjestelmään, jotta tietoturvapolitiikka ja -tavoitteet ovat yhdenmukaisia suhteessa organisaation strategiaan. (ISO/IEC 27001: 2017, 7). Tässä keskeisenä ulottuvuutena on myös oletus, että viestintäketjut ja ajatustenvaihdon yhteydet ovat kunnossa organisaation sisällä, jotta nopea kommunikaation mahdollistuu. ISO/IEC 27003:2017 –ohjeistuksessa mainitaankin, että viestintä voidaan toteuttaa käytännön esimerkeillä, joiden avulla havainnollistetaan todellisia tarpeita organisaation toimintaympäristössä sekä tietoturvavaatimuksista viestimällä (ISO/IEC 27003: 2017, 13).

Tietoturvapolitiikka ja –tavoitteet eivät voi olla aidosti yhdenmukaisia, mikäli viestit ja tiedot strategioista eivät tavoita koko organisaatiota ja kaikkia toimijoita. Ylimmän johdon sitoutuneisuus projektissa ilmenee lähinnä uteliaisuutena, riittävänä asianhallintana, haluna selvittää muutoksen kerrannaisvaikutuksia organisaation toimintaan. Ylimmälle johdolle ei tule eräiden ohjeistusten mukaan viestiä liian teknisellä tasolla (Andreasson & Koivisto 2013, 48). Hyvät suhteet ja luottamus standardin ISO/IEC 27001 asiantuntijoihin sekä projektia edistäviin alaisiin paitsi nopeuttavat ja selkeyttävät vaadittavia toimenpiteitä myös synnyttävät luottamusta siitä, että organisaatiossa ollaan arvioitu, että jatkuvan parantamisen politiikkaan on mielekästä sitoutua pitkällä tähtäimellä (ISO/IEC 27001: 2017, Vrt. 7). Tämä on viime kädessä vaikuttamista turvallisuuskulttuuriin, jolloin hienovaraisilla toimilla ja rakentavilla ajatuksilla voidaan saada muutoksia siihen, miten tietoturvaan ja syvälliseen hallintajärjestelmämuutokseen todellisuudessa asennoidutaan. Myös riskienhallinnan ja tietoturvan raportoinnin yhdistämistä voidaan suositella tietyissä tapauksissa (Andreasson & Koivisto 2013, 48).

Ylin johto varmistaa, että hallintajärjestelmän vaatimukset yhdistetään organisaation prosesseihin ja että resursseja on riittävästi (ISO/IEC 27001: 2017, 7). Näin ollen hallintajärjestelmän vaatimukset eivät olekaan irrallinen konstruktio suhteessa prosesseihin tai ydintoimintoihin vaan oleellinen osa niitä. Tässä yhteydessä tulisi päästä eroon näkemyksestä, jossa tietoturvana pidetään lähinnä pelkästään yksittäisiä turvatekniikoita ja –ratkaisuja, joiden tarkoituksena on ehkäistä tietyntyyppisiä uhkia ja ulkoisia hyökkäyksiä – päinvastoin, standardi kyllä mahdollistaa vallitsevien (toimivien) keinojen sisällyttämisen organisaation tietoturvatyön menettelyihin jatkossakin, mutta kokonaishallinnan näkökulmasta itse menetelmän sisäistäminen on monin kerroin yksittäisten varotoimien hyödyntämistä tehokkaampaa. Eräs keskeisimmistä menetelmähyödyistä on siinä, että standardissa edellytetään, että prosessit ovat tiedostettuja, esiteltävissä ja dokumentoitavissa, minkä johdosta hallintajärjestelmäperusta on sellaisenaan tuttu, vakaa ja ositettu. Näin ollen valmiudet ja valmiusajat reagoida yllätyksiin ovat asianmukaiset ja testaus- ja toipumistoimet ovat selkeät. Resurssienkäytön kannalta on tärkeää hyödyntää palveluja, jotka ovat skaalattavissa organisaation koon mukaisesti, olivat

kyseessä sitten esimerkiksi sisäiset projektit tai vaikkapa ulkoistettu lokienhallinta tai tietoturvavalvonta. (ISO/IEC 27002:2017, 50.)

Ylimmän johdon tulee viestiä hallintajärjestelmän vaatimusten tärkeydestä, jotta tavoitellut tulokset voidaan saavuttaa, vaikuttavuutta voidaan tukea ja jatkuva parantaminen mahdollistuu. Varsinkin isoissa organisaatioissa tieto saattaa hukkua tai vääristyä, vaikka ylin johto pyrkisikin painottamaan aiheen tärkeyttä. ISO/IEC 27003: 2017 –ohjeistuksen mukaan niissä tilanteissa, joissa tietoturvallisuuden hallintajärjestelmän toteuttamisesta vastaava ja sitä hyödyntävä organisaatio on osa isompaa organisaatiota, johtamista ja sitoutuneisuutta voidaan edistää osallistamalla kyseinen henkilö tai ryhmä, joka vastaa organisaation suuntaamisesta ja ohjaamisesta (ISO/IEC 27003: 2017, 13).

Voi olla vaikeaa kuvata standardin ISO/IEC 27001 mukaisen hallintajärjestelmän kattavuutta henkilöille, joilla ei ole aiempaa kokemusta aiheesta. Lisäksi mikäli työtavat ja –menetelmät ovat vuosikausia olleet ennallaan, voi tuntua vaikealta ja uhkaavaltakin ottaa nopealla aikataululla uusia ja totuttuja käytäntöjä haastavia menettelytapoja käyttöön. Vaaditaankin koulutustilanteita ja valistusta aiheesta, jotta jokainen voi täyttää omat tietoturvavelvoitteensa. Täytyy silti samalla muistaa, ettei standardissa edellytetä, että kaikkien organisaation toimijoiden tulisi ymmärtää hallintajärjestelmä kokonaisuudessaan, koska vaaditaan ainoastaan, että jokainen toteuttaa tietoturvavelvoitteitaan oman roolinsa mukaisesti. Tämä omien tietoturvavastuiden toteutus on avainasiassa pyrittäessä asetettuihin tuloksiin, jolloin myös vaatimukset toimenpiteiden vaikuttavuudesta täyttyvät suuremmalla todennäköisyydellä. Jatkuva parantaminen toteutuu, kun vanhemmat ja kokeneemmat työntekijät kouluttavat uusia tulijoita organisaation vastuisiin. Ylin johto tukee myös muuta johtoa heidän vastuualueillaan. (ISO/IEC 27001: 2017, 7.)

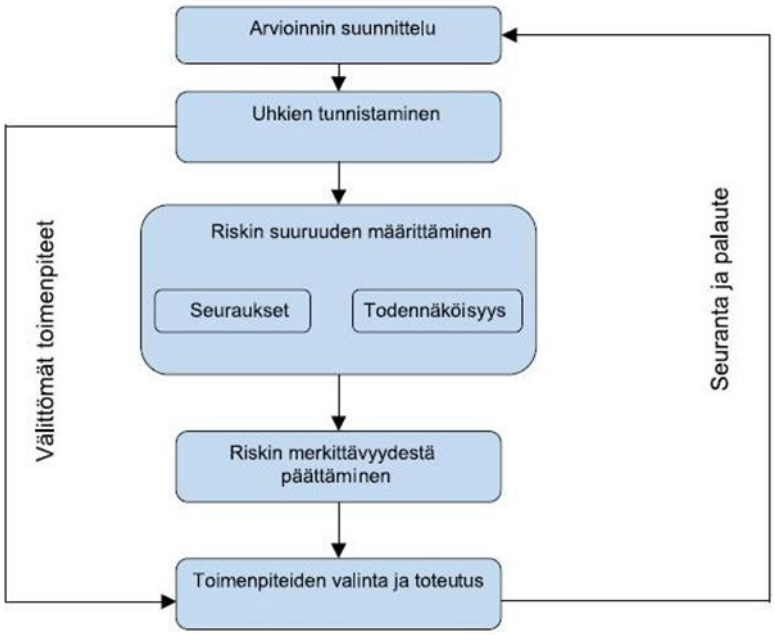
Lisäksi ylin johto määrittelee standardin ISO/IEC 27001 mukaisen hallintajärjestelmän vaatimusten mukaisesti, kenellä tai keillä on vastuut ja valtuudet varmistaa hallintajärjestelmän vaatimuksenmukaisuus sekä se, kenen vastuulla on raportoida ylimmälle johdolle hallintajärjestelmän suorituskyvystä (ISO/IEC 27001: 2017, 7).

Kuten mainittua, ylin johto laatii tietoturvapolitiikan, joka on saatavilla dokumentoituna tietona. Tämän tietoturvapolitiikan on oltava koko organisaation tiedossa. Lisäksi tiedon pitää olla tarvittaessa sidosryhmien saatavilla. Standardi edellyttää, että kaikesta hallintajärjestelmään liittyvästä on asianmukaisesti säilytettyä tietoa. Tiedon kerääminen vaatii aikaa ja standardin vaatimuksiin perehtymistä, koska saattaa käydä siten, että sisällöllisesti sopivaa tietoa on jo valmiina, mutta muodoltaan se ei ole sopivaa ja että sitä pitää muokata vaatimusten mukaiseksi, mikä vie aina aikaa ja resursseja. Ylimmän johdon tehtävä on varmistaa, että tietoturvavastuut, -roolit ja –valtuudet määritellään. Lisäksi organisaatiossa on oltava henkilö,

joka raportoi hallintajärjestelmän suorituskyvystä ylimmälle johdolle. Roolivastuiden selkeyttämisessä on useita käytännön hyötyjä standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomisvaiheessa. Asiantuntijan on esimerkiksi nopeampaa perehtyä osa-alueisiin, koska niille on nimetty vastuuhenkilöt. Lisäksi oleellista ydintä, hallintajärjestelmän suorituskykyä, on vaivatonta tarkastella, koska jäsentelyt ovat valmiina. (ISO/IEC 27001: 2017, 7.)

2.3.3 Riskien ja mahdollisuuksien käsittely

Riskien ja mahdollisuuksien käsittelyn avulla pyritään varmistamaan, että tietoturvallisuuden hallintajärjestelmällä päästään haluttuihin tuloksiin. Halutut tulokset määritetään alussa, minkä jälkeen arvioidaan, minkälaisia riskejä tai vastaavasti mahdollisuuksia toimenpiteisiin liittyy. Vaikka riskejä on useimmiten arvioitu jo ennalta, hallintajärjestelmän tuoma ulottuvuus mullistaa sen, miten riskeihin suhtaudutaan uudessa asetelmassa. Standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomisen jälkeen riskit eivät ole irrallisia vaan ne näyttäytyvät nimettyinä, jäsenneltyinä ja kokonaisuuden osina. Ulkoiset ja sisäiset tekijät tulee eritellä, jolloin myös osatekijät, muuttuvat prosessit ja niihin liittyvät riskit luokitellaan, jolloin uhkia ja mahdollisia haittavaikutuksia voidaan rajata kapeammalle alueelle. Samalla kun siis pyritään estämään tai vähentämään epätoivottuja vaikutuksia, jatkuvan parantamisen tavoite on toteutettavissa. (ISO/IEC 27001: 2017, 8; ISO/IEC 27003: 2017 16-27.)



Kuvio 1: Riskien arvioinnin ja hallinnan vaiheet (Murtonen 2003)

Standardin mukaan organisaatiossa tulee suunnitella riskeihin ja mahdollisuuksiin kohdentuvia toimia, jotta ne voidaan kytkeä hallintajärjestelmän prosesseihin, toteuttaa toimenpiteet ja arvioida niiden vaikuttavuutta. Kun riskienhallinnan toimet kytketään saumattomasti hallintajärjestelmän prosesseihin, niistä tulee luonnollistunut osa järjestelmän toimintaa, jolloin ei ole tarvetta ylikorostaa riskienhallintaa erillisenä toimintona, vaikka ei olekaan suoranaista estettä sille, että organisaation riskienhallintaa tarkastellaan kriittisesti ikään kuin itsenäisenä käytäntönä. (ISO/IEC 27001: 2017, 8-9.) Riskien arviointiin voidaan käyttää useita menetelmiä, joissa on erilaisia painotuksia. Eräs hyväksi havaittu menetelmä riskien käsittelyyn on MAGERIT-metodi, jota usein käytetään ISO/IEC 27001 –standardin käyttöönotossa (vrt. esim. Velasco 2018, 297).

Standardin mukaisesti organisaatiossa tulee suunnitella riskeihin ja mahdollisuuksiin kohdentuvia toimia, jotta ne voidaan kytkeä hallintajärjestelmän prosesseihin, toteuttaa toimenpiteet ja arvioida niiden vaikuttavuutta. Näin ollen vaikuttavuuden arvioinnissa voidaan pohtia, ovatko toimenpiteet todella edistäneet tietoturvallisuutta. Mikäli tehdyt toimet eivät vaikuta aiemmin määritettyihin tavoitteisiin, eli esimerkiksi tietoturvan parantamiseen, ne voidaan todeta riittämättömiksi. Tämä olisi siinä suhteessa ongelmallinen tilanne, että toisaalla standardissa määritellään tietoturvariskien arvioinnista ja käsittelystä. Standardin mukaan on siis päätettävä tietoturvariskien käsittelykeinot perustuen riskien arvioinnin tuloksiin, määritellään hallintamenettelyt keinojen toteutukseen ja varmistetaan ettei yksikään tarvittavista ja standardin edellyttämistä hallintakeinoista jää käyttämättä. Näin ollen on havaittavissa, että vaatimusosan tietynlainen pelkistetty muoto onkin täyttynyt organisaation omista tarpeista johtuen velvoittavaksi. (ISO/IEC 27001: 2017, 8-9.)

Lisäksi standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomisen yhteydessä koostetaan soveltuvuuslausunto, jossa on perustelut hallintakeinojen käytölle tai käyttämättä jätölle, tehdään suunnitelma tietoturvariskien käsittelylle sekä hankitaan suunnitelmalle ja jäännösriskeille riskien omistajan hyväksyntä. Organisaation tulee myös tallettaa dokumentaatiota tietoturvariskien käsittelyyn liittyvistä prosesseista. (ISO/IEC 27001: 2017, 9.)

2.3.4 Tietoturvatavoitteet ja suunnitelmat niihin pääsemiseksi

Keskeinen vaihe standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomiseen liittyen on, tietoturvatavoitteet ja –suunnitelmat ovat selvillä (ISO/IEC 27001: 2017, 9). Käytännössä organisaation täytyy siis määrittää asiaankuuluvien toimintojen ja tasojen tietoturvatavoitteet, joiden tulee täyttää seuraavat vaatimukset:

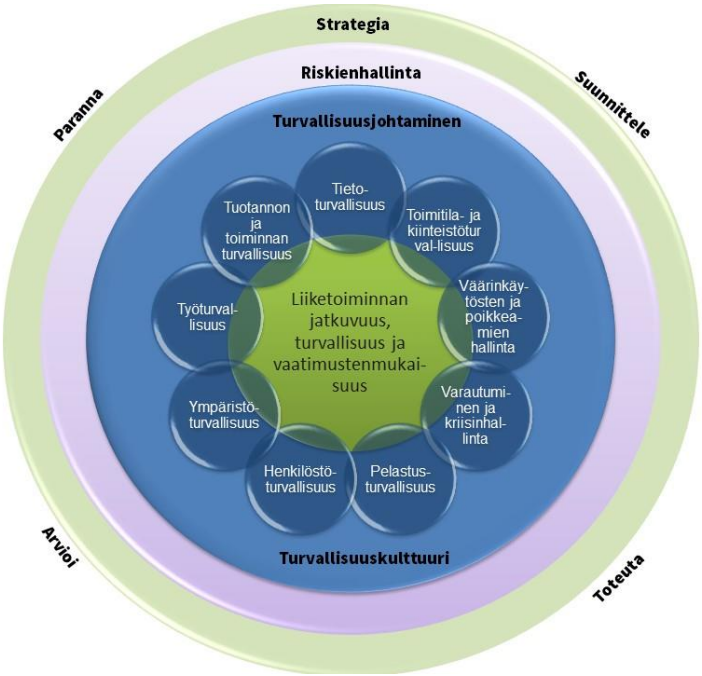
- niiden tulee olla yhdenmukaisia suhteessa tietoturvapolitiikkaan

- niitä tulee voida mitata, mikäli mahdollista
- niistä pitää viestittää
- niitä tulee päivittää tarvittaessa

On tärkeää, että tietoturvapolitiikka on suunniteltu ja ilmaistu standardin edellyttämällä tavalla, jotta siitä kumpuavat toimet ovat ennakoitavia ja helposti yhdistettävissä standardin mukaisuuteen. Mittaus on hyödyllistä standardin kannalta siksi, että sen avulla voidaan jatkossa numeerisinkin keinoin punnita vaikuttavuutta. Viestitysvalmius on ylläpidettävä riittävällä tasolla ja päivittämiselle on luotava käytännön puitteet. Kun organisaatiossa suunnitellaan keinoja tietoturvatavoitteiden saavuttamiseksi, sen tulee määritellä:

- mitä tehdään
- resurssit
- vastuut
- valmistumisaika
- tulosarviokeinot

Näistä tekijöistä muodostuu hallintaa kontrolloivia ja jäsentäviä reunaehtoja. Ensiksi määritellään mitä tehdään, jotta organisaatio voi saavuttaa asettamansa tietoturvatavoitteet. On selvitettävä, minkälaisilla resursseilla nämä tavoitteet ovat saavutettavissa. Vastuuhenkilöiden nimeäminen tarkentaa työnkuvaa ja lisää edistymisen edellytyksiä. Valmistumisajan ja tulosarviokeinojen rajausten avulla voidaan heijastella onnistumisen astetta suhteessa tavoitteisiin ja ajallisiin määreisiin. (ISO/IEC 27001: 2017, 9.)



Kuvio 2: EK:n turvallisuusympyrän kaltaisen mallin avulla voidaan hahmottaa kokonaisturvallisuuden osa-alueita, mistä voi olla hyötyä organisaation ymmärtämisessä myös standardin mukaiseen tietoturvallisuuden hallintajärjestelmään siirryttäessä.

2.3.5 Standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomisen yhteydessä määritettävät tukitoiminnot: pätevyys, tietoisuus, viestintä ja dokumentointi

Organisaatiossa määritellään, millainen pätevyys sen ohjauksessa työskentelevillä henkilöillä pitää olla, koska heidän työnsä vaikuttaa tietoturvallisuuden tasoon. Organisaation on siis varmistettava näiden henkilöiden pätevyystiedot koulutuksen, harjoittelun ja kokemuksen osalta. Lisäksi vaadittava pätevyys on tarvittaessa hankittava eri keinoin, jolloin tällä tavalla tehdyt toimenpiteet pitää vielä arvioida vaikuttavuuden osalta. Tämän jälkeen organisaatiossa on säilytettävä asianmukaista ja ajantasaista dokumentoitua tietoa näyttönä pätevyydestä. (ISO/IEC 27001: 2017, 10.)

Organisaatiossa työskentelevien tulee olla tietoisia tietoturvapolitiikasta, hallintajärjestelmän vaikuttavuudesta ja sen tason parantamisen hyödyistä sekä vaatimusten noudattamatta jättämisen seurauksista. Ajatuksena tässä on, että organisaation ohjauksessa työskentelevät henkilöt voivat helpommin tiedostaa, miten he voivat omalta osaltaan edistää tietoturvallisuuden hallintajärjestelmän vaikuttavuutta, ja minkälaista hyötyä tietoturvallisuuden tason parantamistoimista on. Vastaavasti samalla tulee ymmärrys seurauksista, joita vaatimusten noudattamatta jättämisellä saattaa olla. (ISO/IEC 27001: 2017, 10.)

Organisaation tulee määrittää standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomisen yhteydessä, miten ulkoista ja sisäistä viestintää toteutetaan ja millaista viestintää tarvitaan. Tulee selvittää esimerkiksi:

- mistä ja milloin viestitään
- keiden kanssa viestitään
- ketkä viestivät
- minkälaiset viestintäprosessit tulee toteuttaa

Viestinnän koordinoinnilla saavutetaan ennustettavuutta, roolien täsmentymistä ja tietoa viestintäprosesseista, jolloin on helpompi havaita, mikäli näihin käytäntöihin liittyy tietoturvariskejä tai vastaavanlaisia aukkoja suhteessa hallintajärjestelmään (ISO/IEC 27001: 2017, 10).

Dokumentoidusta tiedosta on ISO/IEC 27001 -standardissa tarkat vaatimuskohdat. Yleisvaatimusten lisäksi määritellään, miten dokumentoitua tietoa luodaan, päivitetään ja hallitaan. Ytimekkäästi voidaan todeta, että standardin mukaan dokumentoitua tietoa tietoturvan hallintajärjestelmästä on oltava siten, että sitä on aina saatavilla muodossa, joka sopii käyttötarkoitukseen. (ISO/IEC 27001: 2017, 10-11.)

2.3.6 Toiminnasta eli toiminnan suunnittelusta ja ohjauksesta sekä tietoturvariskien arvioinnista ja käsittelystä

Organisaatio tekee suunnitelmia ja toteuttaa prosesseja, jotka ovat oleellisia tietoturvavaatimusten täyttämisen ja määritettyjen toimien toteuttamisen kannalta. Lisäksi näitä toimenpiteitä tulee ohjata. Toimia avaavien dokumentaatioiden tulee olla asianmukaisesti järjestetyt. Tärkeää on, että dokumenteista on vaivattomasti osoitettavissa, että organisaation on toiminut suunnitelmien mukaisesti ja että prosessit (myös ulkoiset) on toteutettu määritellysti ja valvotusti. (ISO/IEC 27001: 2017, 11-12.)

Tietoturvariskien arviointi on suoritettava suunnitelmien mukaisin aikavälein tai merkittäviä muutoksia ehdotettaessa tai muutosten yhteydessä. Tietoturvariskien arvioinneista on pidet-

tävä dokumentaatiota. Lisäksi organisaation tulee ottaa käyttöön käsittelysuunnitelma tietoturvariskeille, ja dokumentaatio tietoturvariskien käsittelytuloksista tulee säilyttää. (ISO/IEC 27001: 2017, 11-12.)

2.3.7 Suorituskyvyn arviointi – seuranta, mittaus, analysointi ja arviointi sekä sisäinen auditointi ja johdon katselmus

Organisaatiossa tulee arvioida tietoturvan tasoa ja vaikuttavuutta tietoturvallisuuden hallintajärjestelmään liittyen. Organisaatio määrittää, mihin kohdennetaan seurantaa ja mittausta, ja tähän kuuluvat mukaan myös tietoturvaprosessit ja hallintakeinot. Lisäksi on määritettävä, millä seurannan, mittauksen, analysoinnin tai arvioinnin menetelmillä on mahdollista varmistaa tulosten kelvollisuus. Tässä pyrkimys on hyödyntää menetelmiä, jotka mahdollistavat vertailun ja toistettavuuden periaatteita. Lisäksi dokumentaatiota tulee säilyttää siitä, kun organisaatio määrittää, milloin seurantaa ja mittausta toteutetaan ja, että ketkä sen toteuttavat. Samoin on määritettävä, ketkä analysoivat ja arvioivat mittausten tuloksia ja milloin. (ISO/IEC 27001: 2017, 12-13.) Kuten on havaittavissa, suorituskyvyn arviointiin liittyvät toimenpiteet ovat vaativia ja tarkasti määriteltyjä, myös siksi, että ne tukevat vahvasti sisäistä auditointia, johdon katselmusta sekä jatkuvaa parantamista.

ISO/IEC 27001:2017	***Mitä***	***Miten***	***Milloin***	***Miksi***
Sisäinen auditointi	Organisaatio määrittää, onko hallintajärjestelmä vaatimusten ja kansainvälisen standardin mukainen sekä vaikuttava.	Objektiivisesti ja puolueettomasti laaditaan auditointiohjelmia, kriteerit, soveltamisala, raportointi ja dokumentaatio.	Suunnitelluin aikavälein.	Jotta selviää, onko tietoturvallisuuden hallintajärjestelmän toteutus ja ylläpito vaikuttavaa.
Johdon katselmus	Selvitetään aiempien katselmointien vuoksi aloitettujen toimien tila,	Dokumentoiduilla tiedoilla muutostarpeista, jatkuvan parantami-	Suunnitelluin aikavälein.	Voidaan varmistaa hallintajärjestelmän soveltuvuus, asianmukaisuus ja vaikuttavuus.

ISO/IEC 27001:2017	*Mitä*	*Miten*	*Milloin*	*Miksi*
	ulkoiset ja sisäiset muutokset, tietoturvan tason kehityssuunnat, palaute ja riskienarviointi.	sen mahdollisuuksista ja toimenpiteiden tilanteesta.		

Taulukko 1: Sisäisen auditoinnin ja johdon katselmuksen ydinkohdat (ISO/IEC 27001: 2017, 12-14).

2.3.8 Parantaminen: Poikkeamat ja korjaavat toimenpiteet sekä jatkuva parantaminen

Poikkeama on tietoturvallisuuden hallintajärjestelmän vaatimuksen täyttymättä jääminen (ISO/IEC 27003:2017, 44). Kun poikkeama havaitaan, organisaatiossa on reagoitava siihen ja tilanteen mukaan on aloitettava toimet asian hallitsemiseksi ja korjaamiseksi ja/tai käsiteltävä poikkeaman seurauksia. Lisäksi organisaation tulee arvioida, tarvitaanko poikkeaman syyt poistavia toimenpiteitä, jotta ongelma ei toistu tai esiinny muualla. Tämänkaltaiset toimenpiteet voivat olla esimerkiksi poikkeaman katselmointi, syiden selvittäminen tai vastaavanlaisten poikkeamien tai niiden mahdollisuuksien etsintä. Lisäksi tarvittavat toimenpiteet tulee toteuttaa, korjaavien toimien vaikuttavuus tulee arvioida ja tarvittaessa organisaatiossa saatetaan joutua tekemään muutoksia hallintajärjestelmään. (ISO/IEC 27001: 2014, 14.)

Korjaavien toimien tulee olla tarkoituksenmukaisia suhteessa poikkeaman aiheuttamiin vaikutuksiin. Lisäksi toimista on säilytettävä dokumentoitua tietoa todisteena liittyen poikkeamien luonteeseen ja tehtyihin toimenpiteisiin sekä tehtyjen toimenpiteiden tuloksiin. Jatkuvalla parantamisella tarkoitetaan hallintajärjestelmän soveltuvuuden, riittävyyden ja vaikuttavuuden jatkuvaa parantamista organisaatiossa[??] (ISO/IEC 27001: 2017, 14).

3 Ongelmaesimerkkejä, syiden arviointia ja ratkaisuehdotuksia

Seuraavassa esitetään ongelmaesimerkkejä vaikeuksista, joita saattaa esiintyä standardin käyttöönotossa. Tämän jälkeen analysoidaan ja arvioidaan syitä esitettyihin ongelmiin, jotta tulee ymmärrettäväksi, että syyt saattavat johtua monenlaisista tilanteista organisaatiossa. Lopuksi esitellään ratkaisuehdotuksia ja konstruktiivisia näkökulmia, joiden avulla ongelmista päästään eteenpäin. Ongelmien ratkaisuun sovelletaan konstruktiivista ratkaisumetodia, jossa

havainnoidaan ongelma, etsitään juurisyitä, rakennetaan tapa ongelman selvittämiseen ja luodaan uusi kokonaisratkaisu. Lisäksi jokaisen esitetyn ongelman yhteydessä ehdotetaan yhden ongelmaratkaisumallin hyödyntämistä. Ongelmanratkaisumallit (DSR-, CWA- ja STS-menetelmät) on valittu ongelman luonteen perusteella, eli tutkimalla, mikä menetelmä sopii parhaiten tietyn ongelman ratkaisemiseksi. Korostettakoon, että ongelmanratkaisumallien esittelyn tarkoituksena on osoittaa, että hidasteiden tai esteiden sattuessa konstruktiivisen ongelmanratkaisun apuna voidaan käyttää erilaisia menetelmiä, joiden avulla yksittäisistä ongelmatilanteista pääsee eteenpäin, ei niinkään tarkastella malleja ainoina oikeina vaihtoehtoina ongelmien ratkaisuun, koska erilaisia menetelmiä on useita ja niillä kaikilla on omat hyvät ja huonot ominaisuutensa. Ongelmaesimerkit ovat joiltain osin muokattuja ja todellisista standardin käyttöönottotilanteista johdettuja hidasteita, joiden tarkoituksena on tässä opinnäytetyössä osoittaa ensisijaisesti, miten erilaisia tilanteita saattaa joutua huomioimaan standardin käyttöönotossa.

3.1 Mahdollisia ongelmakohtia Standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomisessa organisaatiolle

Standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomisen yhteydessä on useita erilaisia vaiheita, joiden yhteydessä saattaa tulla viivästyksiä aiheuttavia ongelmia, mikäli asiat eivät etenekään syystä tai toisesta suunnitellusti. Tässä luvussa arvioidaan mahdollisia viiveitä aiheuttavia pulmatilanteita. Etenemistapa on seuraavanlainen: ensin otetaan esiin jossain tietyssä vaiheessa ilmenevä ongelma, sitten arvioidaan syytä ongelmaan ja lopuksi esitetään ratkaisu tai ratkaisuehdotuksia asian ratkaisemiseksi. Esimerkit ovat kuvitteellisia, mutta täysin mahdollisia, ja vaikka ISO/IEC 27001 –standardin vaatimusosien ja ISO/IEC 27003 –ohjeistusten avulla kaikki esiintyvät ongelmat organisaatiossa tulisi voida kyetä ratkaisemaan, on tapausten yhteydessä esitetty myös vaihtoehtoisia tapoja hahmottaa ja ratkaista ongelmia, jolloin päästään takaisin ISO/IEC 27001 –standardin vaatimuksenmukaisuuteen. Kaikki ongelmaesimerkit ovat poikkeamia, millä tarkoitetaan tietoturvallisuuden hallintajärjestelmän täyttymättä jäämistä. Poikkeamiin on reagoitava, koska muutoin ei voida toteuttaa ISO/IEC 27001 –standardin vaatimuksenmukaisuutta. (ISO/IEC 27003:2017, 44.)

3.1.1 Yhtenäisyyden, selkeän linjan ja tietoturvapolitiikan puutteet organisaatiossa

Organisaatio osoittaa kiinnostusta standardin mukaiseen hallintajärjestelmään siirtymiseen. Tietoturvakontrolleja toki on, mutta yhtenäisyys tai selkeä linja puuttuu ratkaisuista. Kun tiedetään, että standardi edellyttää organisaatiolta selkeää tietoturvapolitiikkaa, sitä aletaan tehdä, mutta linjaukset ovat perustaltaan epäjohdonmukaisia, muodon vuoksi tehtyjä

ja epäyhtenäisiä suhteessa päämääriin: ISO/IEC 27001:2017 -standardin edellyttämä vaatimus siitä, että tietoturvapolitiikan on sovelluttava organisaation tietoturvatavoitteisiin, ei täyty (Ks. ISO/IEC 27001: 2017, 7).

Ongelman syitä voi olla monia, mutta esitetyssä tapauksessa vaikuttaa, etteivät standardin edellyttämät roolit ja niihin liittyvät vastuut ole sisäistettyjä. Lähtökohta on se, että organisaatio määrittää tietoturvapolitiikan, jonka johto voi hyväksyä ja jossa täsmennetään organisaation lähestymiskeinot tietoturvan tavoitteiden saattamiseen hallituiksi. (ISO/IEC 27002:2017, 9.) Keskeisin ongelma saattaa olla se, että organisaatiossa ei ymmärretä riittävän hyvin sitä, että vaikka standardin vaatimusosat ovat toisaalta joustavia ja erilaisille ratkaisuille tilaa antavia, yhdessä kontrollien kanssa niiden reunaehdot on ehdottomasti syytä ottaa tosissaan. Standardin mukaisessa toiminnassa ei ole turhia tekijöitä ja kaikki ratkaisut ovat perusteltuja hallinnan lisäämiseksi.

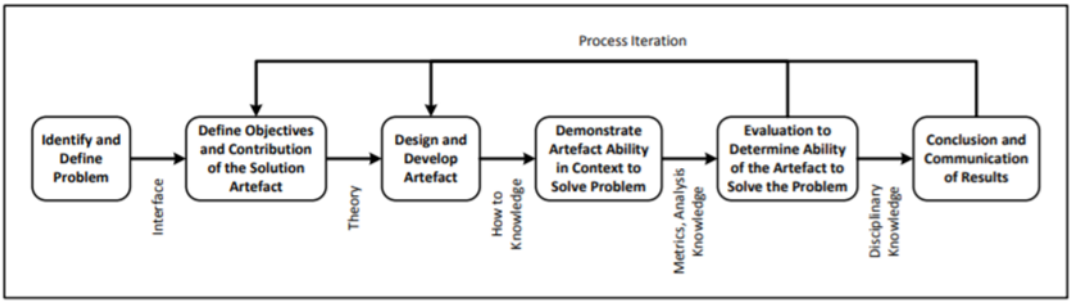
Ratkaisu ongelmaan on, että johto ottaa standardin edellyttämän selvemmän roolin tietoturvallisuutta koskevassa ohjauksessa (ISO/IEC 27002:2017, 9). Mikäli yhden yhtenäisen tietoturvapolitiikan laatiminen on jossain olosuhteissa hankalaa, standardi mahdollistaa tilanteen, jossa tietoturvapolitiikka kootaan joukosta itsenäisiä, mutta toisiinsa liittyviä asiakirjoja (ISO/IEC 27002:2017, 10). Keskeistä on, että tietoturvapolitiikat ovat linjassa organisaation toiminta-ajatuksen kanssa (ISO/IEC 27001: 2017, 7). Muutoin on vaarana, etteivät politiikat ole linjassa käytännön ratkaisujen kanssa, jolloin syntyy tilanne, jossa kokonaisuus on mielivaltainen, epäyhtenäinen ja hallitsematon. Tällöin ei olla linjassa standardin ISO/IEC 27001 mukaisen hallintajärjestelmän vaatimusten suhteen. Jotta ongelma voitaisiin ratkaista, tietoturvapolitiikkojen tulisi kattaa vaatimukset, jotka ovat lähtöisin liiketoimintastrategiasta, asetuksista, laeista ja sopimuksista sekä nykyisestä ja ennustetusta tietoturvauhkaympäristöstä. Nämä luovat ylimmän tason rakenteen tietoturvapolitiikalle, minkä jälkeen yksityiskohtaisemmat määritteet ja kuvaukset voidaan seuraavaksi sisällyttää dokumentaatioihin. (ISO/IEC 27002:2017, 9.)

Tietoturvapolitiikassa tulisi olla myös lausumia, joissa määritellään tietoturvallisuus, tietoturvatavoitteet ja –periaatteet, joita käytetään ohjaamaan kaikkia tietoturvallisuuteen liittyviä toimintoja. Lisäksi tietyille rooleille täytyy määrittää sekä yleisiä että kohdistetumpia vastuita tietoturvallisuudesta. Myös prosessit, joilla käsitellään poikkeamia ja poikkeuksia tulee määritellä. (ISO/IEC 27002:2017, 9.) Näiden mainittujen ylemmän tason linjausmäärittelyjen lisäksi on hyödyllistä kuvata organisaatiota asiakohtaisilla politiikoilla sekä kattavilla tietoturvallisuutta edistävillä toimenpiteillä, joihin voivat lukeutua esimerkiksi pääsynhallinta-, varmuuskopiointi- ja tiedonsiirtokäytännöt (ISO/IEC 27002:2017, 10).

Kuten havaitaan, työtä ja huolellisuutta vaaditaan, mikäli dokumentaatio on hallintajärjestelmää luotaessa epäyhtenäistä. Kuitenkin kun linjaukset ovat kunnossa ja järjestelmällisesti

merkittyjä ja ollaan siirrytty jatkuvan parantamisen vaiheeseen, tuotetun dokumentaation määrä vähenee, jolloin on enemmänkin kyse päivittämisestä ja uusien, esiin nousevien ongelmien käsittelystä (ISO/IEC 27001: 2017, 12).

Mikäli organisaatiossa koetaan, että tietoturvapolitiikan määrittäminen on haasteellista siten, että se aidosti ja saumattomasti soveltuu toiminta-ajatukseen ISO/IEC 27001 –standardin edellyttämällä tavalla, on mahdollista hyödyntää vaihtoehtoisia menetelmiä hahmottaa pulmia tuottavaa asetelmaa. DSR-menetelmän (*Design Science Research*) avulla on mahdollista paitsi tuottaa uusia tietojenkäsittely ja –hallintamalleja myös arvioida nykyisiä. Menetelmän avulla kyetään tuottamaan, kuvailemaan, selittämään ja ennakoimaan tietoa. DSR-menetelmää käytetään paitsi uuden suunnittelun apuvälineenä myös ongelmanratkaisumallina. Ongelmien havainnoinnissa ja ratkaisussa mallista saattaisi olla hyötyä pyrittäessä hahmottamaan yhtenäisyyttä organisaation tavoitteiden, tietoturvapolitiikan ja toiminta-ajatuksen välillä. (Oosthuisen, Pretorius 2016, 16)



Kuvio 3: DSR-menetelmä ongelmanratkaisun apuna (Oosthuisen, & Pretorius 2016, 16)

3.1.2 Johdon tehtävät, muutoksesta viestiminen ja epätietoisuus rooleista

Ylin johto on sitoutunutta, mutta ei viesti käynnissä olevasta standardin ISO/IEC 27001 mukaisen hallintajärjestelmän luomiseen liittyvästä muutoksesta riittävän tehokkaalla tavalla organisaation sisällä. Asiaan liittyvät henkilöt organisaatiossa eivät tästä syystä täysin ymmärrä omaa kokonaisuuttaan eivätkä sitä miksi tietoturvaroolit muuttuvat tai ovat muuttumassa, miten uusia tietoturvarooleja ja –vaatimuksia tulisi hoitaa, millaisia seurauksia vaatimusten täyttämättä jättämisestä on, ja tästä vyyhdistä syntyy epätietoisuutta ja vääriä oletamuksia.

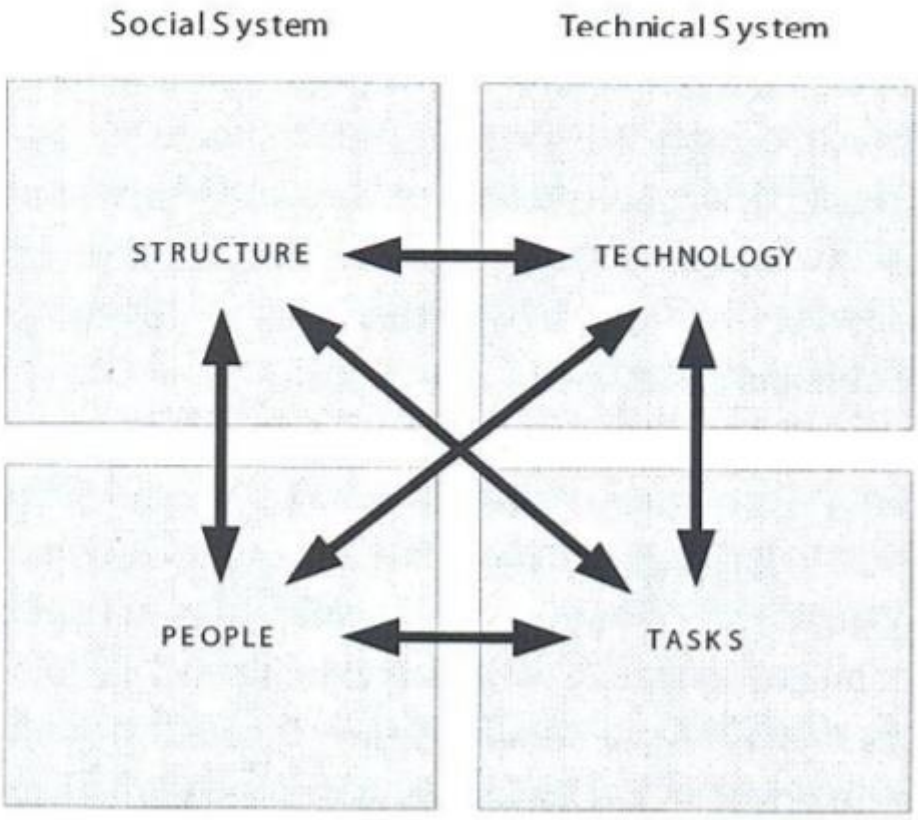
Standardin ISO/IEC 27001 mukaan sekä johdon roolit, että toimijoiden tietoturvavastuut tulee määritellä (ISO/IEC 27001: 2017, 7). Itse ongelma syntyy kuitenkin lähinnä roolien epäselvyy-

destä sekä viestinnän ja/tai tiedotuksen epäonnistumisesta, joten standardin mukaan ratkaisut näihin kysymyksiin löytyvätkin lähinnä kohdista Johtajuus (5.1 Johtajuus ja sitoutuminen ja 5.3 Organisaation roolit ja vastuut) ja Tukitoiminnot (7.2 Pätevyys, 7.3 Tietoisuus sekä 7.4 Viestintä). (ISO/IEC 27001: 2017, 7 & 10).

Kirjaimellisesti ottaen tietoturvavastuut jaetaan tietoturvapolitiikkojen mukaisesti, mutta mikäli tässä oletetaan, että politiikat ovat standardin edellyttämällä tavalla määritellyt, on todellisia juurisyitä ehkä mielekkäintä etsiä lähinnä viestinnän epäonnistumisesta. Tällöin on tarkasteltava mahdollisesti myös kohtia tietoturvallisuuden organisointi, sisäinen organisaatio sekä rooli- ja vastuukysymykset. (ISO/IEC 27002:2017, 11.) Standardi edellyttää, että johto tarjoaa ohjausta ja tukea tietoturvallisuuden toteutukseen liiketoiminnan vaatimuksien ja asiaan liittyvien lakien ja asetuksien määräämällä tavalla. Näin ollen havaitaan, että johdon on tiedostettava asemansa ja tehtävänsä, jotta riittävä tietoisuus hallintajärjestelmästä on jaettavissa asiaankuuluville henkilöille organisaatiossa. (ISO/IEC 27002:2017, 9.)

Ohjeistuksen mukaan sisäisiä asioita määriteltäessä organisaatiossa olisi tunnistettava eri tietojärjestelmiensä välinen tiedonkulku riittävän yksityiskohtaisella tasolla (27003, 9).

ISO/IEC 27001 –standardin vaatimukset ovat esimerkin organisaatiossa tiedossa, mutta ongelma on ensisijaisesti viestinnässä, jonka osalta standardin ohjeet ovat erittäin kattavat ja selkeät. Onkin mielekästä etsiä vaihtoehtoisia tapoja hallita syntynyttä ongelmaa, joka ensisijaisesti toki näyttää liittyvän viestinnän toteutukseen, mutta saattaa mahdollisesti juontua myös muista syistä. STS-teorian (*Socio-Technical Systems*) tarkoitus on auttaa nykyaikaisia ja monimutkaisia organisaatioita ymmärtämään rakenteitaan paremmin. Teorian mukaan organisaatiot koostuvat sosiaalisista ja teknisistä järjestelmistä, jotka ovat sekä itsenäisiä että keskenään vuorovaikutuksessa. Sosiaaliseen osaan lukeutuvat ihmiset, heidän piirteensä ja vuorovaikutus, joka syntyy organisaatiossa. Teknisessä osassa tarkastellaan organisaation prosesseja ja tehtäviä sekä teknologiaa, jonka tarkoituksena on olla mahdollistamassa toimintoja, joiden avulla työpanos muuntuu organisaation päämääräksi tai tuloksiksi. Ennen kaikkea STS-teoria auttaa hahmottamaan työntekijöiden ja teknisten järjestelmien yhtenäisyyttä, jolloin voidaan saavuttaa näkökulmia, joiden avulla ymmärretään myös syntyviä ongelmia yksityiskohtaisemmin. Esimerkin ongelmassa rooleista, vastuista ja velvollisuuksista tiedottaminen ei toteudu ISO/IEC 27001 –standardin edellyttämällä tavalla, joten STS-teorian sosiaalisuutta käsittelevistä painotuksista saattaisi olla mahdollista löytää ratkaisuja ongelmaan. Viestintään ja tiedonkulun ongelmiin saattaa löytyä ratkaisuja sosiaalisen ja teknisen rajapinnoilta. Mikäli ISO/IEC 27001 –standardin vaatimustasot ovat joillain osa-alueilla organisaatiolle haasteellisia, voi olla hyötyä, mikäli on löydettävissä menetelmiä tai teorioita, kuten STS, joiden avulla asioista päästään eteenpäin kohti vaatimuksenmukaisuutta. (Ada, Gupta & Sharman 2009, 281-282.)



Kuvio 4: STS-malli auttaa hahmottamaan organisaation toimintaympäristöä siten, että erityisesti henkilöstön, rakenteen ja työtehtävien keskinäinen suhde tulee näkyväksi (Ada Gupta & Sharman 2009, 282)

3.1.3 Ongelmat dokumentoidun tiedon tallentamisessa ja löytämisessä organisaatiossa

Dokumentoitua hallintajärjestelmän kannalta oleellista tietoa kyllä tuotetaan muilta osin standardin edellyttämällä tavalla, mutta sitä tallennetaan hajanaisesti organisaatiossa eikä sitä sen tähden ole vaivatonta löytää. Organisaation vastuuhenkilöt ja muu henkilöstö tiedostavat ongelman, mutta nopeaa ratkaisua on vaikeaa löytää, koska täysin yhtenäisiä käytäntöjä tai tietojärjestelmiä ei ole.

Standardin ISO/IEC 27001:2017 mukaisen hallintajärjestelmän luominen on vaativa prosessi eikä ole nopeaa tai vaivatonta saada kaikkia asioita kuntoon standardin vaatimusten edellyttämällä tavalla. Dokumentaation tulee olla löydettävissä suhteellisen helposti, kun asianomaiset tarvitsevat sitä tietoturvatehtäviensä hoitamiseen. Tiedonhallintajärjestelmät ovat esimerkkitapauksessa ilmeisen levällään organisaation kokonaistietojärjestelmissä. Asiassa olisi

syytä ryhtyä standardin edellyttämälle jatkuvan parantamisen polulle, millä tarkoitetaan sitä, että organisaatiossa tulee parantaa jatkuvasti tietoturvallisuuden hallintajärjestelmän soveltuvuuteen, riittävyyteen ja vaikuttavuuteen liittyviä tekijöitä (ISO/IEC 27001: 2017, 13). Korostettakoon, ettei ongelma vaikuta suoranaiselta tietoturvariskiltä, mutta käyttöä ja siten toimintaa hidastavana ja hankaloittavana pulmana se tulisi ratkaista siten, että asian voisi katsoa olevan riittävällä tasolla. Tietoturvallisuus on ensisijainen periaate, mikä ilmenee kuvaavasti standardin pääsynhallinnan ohjeistuksissa, joissa todetaan, että kun luodaan sääntöjä, lähtökohdan tulisi olla, että kaikki on kiellettyä, ellei sitä erikseen ole sallittu, sen sijaan, että ajattelu olisi, että kaikki on sallittua, ellei sitä erikseen kielletä (ISO/IEC 27002:2017, 27).

Mikäli turvallisuustoiminta nähdään organisaatiossa vain välttämättömänä ja vaadittuna osa-alueena, jolla ei ole merkitystä tuottavana tai arvoa lisäävänä tekijänä, on vaikeaa ottaa käyttöön yhtenäistettyjä turvallisuuden tai hallinnan järjestelmiä, joissa henkilöstön, käytäntöjen ja välineistön avulla pyritään asetettuihin tavoitteisiin (Garcia 2008, 21).

Ensisijainen ratkaisu on siinä, että soveltamisalaa kuvaavaan tietoon tulisi sisällyttää rajat ja rajapinnat organisaatiossa. Samat määritykset olisi tehtävä tieto- ja viestintätekniikan osalta. (ISO/IEC 27003:2017, 11.) Tällä voidaan esimerkin tapauksessa tavoitella sitä, että tehtyjen ratkaisujen perustelut tehdään kaikille näkyviksi organisaatiossa, jolloin kukaan henkilöstön edustaja ei pidä toimenpiteitä mielivaltaisina eikä siten turhina.

Lisäksi ratkaisuna on tarkastella standardin vaatimusosan kohtia dokumentoituun tietoon (Kohta 7.5) liittyen (ISO/IEC 27001: 2017, 11). Standardi edellyttää, että dokumentoitua tietoa tulee sisällyttää tietoturvallisuuden hallintajärjestelmässä, mikäli se on määritelty vaikuttavuuden kannalta välttämättömäksi (ISO/IEC 27001: 2017, 10). Standardin ISO/IEC 27001 mukaisessa hallintajärjestelmässä tiedon tulee luotaessa ja päivitettäessä olla asianmukaisesti merkittyä ja kuvattua, jolloin muun muassa otsikointi, päiväys, laatija ja viitenumero täytyy merkitä selkeästi, mikä auttaa tiedon löytämisessä (ISO/IEC 27001: 2017, 11).

Lisäksi dokumentoitu tieto tulee tallentaa asianmukaisesti, jolloin muun muassa kieli, ohjelmistoversio ja kuvat on määritelty. Myös soveltuvuuden ja riittävyyden tarkistus ja hyväksyminen on varmistettava (ISO/IEC 27001: 2017, 11). Dokumentoitua tietoa hallitaan myös sillä, että varmistetaan että se on tarvittaessa saatavilla käyttötarkoitukseen sopivassa muodossa. Tämä liittyy oleellisesti nyt käsiteltävään ongelmaan. Lisäksi asianmukaisesta suojauksesta tulee huolehtia, mikä tarkoittaa esimerkiksi sitä, että luottamuksellisia tietoja ei luovuteta luvatta, tietojen asiaton käyttö on estetty ja että tiedot pysyvät muuttumattomina kokonaisuuksina. (ISO/IEC 27001: 2017, 11.)

Organisaatiossa tiedon dokumentoinnin hallittavuus ulottuu lisäksi seuraaviin kohtiin: jakeluun, tietoihin pääsyyn, esille saantiin ja käyttöön. Nuo mainitut neljä tiedonkäsittelyn ja –

käytön vaihetta liittyvät ainakin osittain nyt esiteltyyn ongelmaan. Muita standardin nimeämiä vaiheita ovat tiedon varastointi ja säilytys, muutostenhallinta sekä säilyttämisen ja hävittämisen ohjeistukset. (ISO/IEC 27001: 2017, 11.)

Ongelman ytimessä saattaakin olla esimerkiksi se, että tieto on tallennettuna siten, ettei sitä ole helppoa nopeasti löytää organisaation sisäverkon työtiloista, koska hakurobotit ja -menetelmät ovat puutteellisia varsinkin, jos ei tarkalleen tiedä mitä, miten ja mistä etsiä. Tämä on hyvin yleistä varsinkin isoissa organisaatioissa, joissa tietoa on useista eri aihealueista ja joissa vain osaan tiedosta on kaikilla lukuoikeudet. Eräs ratkaisu voikin olla, että verkkotyötiloihin luodaan yhtenäisempiä käytäntöjä ja että hakemistorakenteita pyritään selkeyttämään. Ongelma on tietysti hankala työskentelyn jouduttamisen ihanteiden näkökulmasta, mutta parannuskeinot ovat käytännössä usein aikaa vieviä ja hankaliakin. Nämä ovat kuitenkin tekijöitä, joita mitataan, kun arvioidaan hallintajärjestelmää vaikuttavuuden näkökulmasta. Standardissa ISO/IEC 27001 huomioidaan kuitenkin se seikka, että dokumentoidun aineiston laajuus vaihtelee eri organisaatioissa, koska siihen vaikuttavat muun muassa organisaation koko, toimintojen tyyppi, prosessien laajuus sekä monimutkaisuus ja henkilöiden pätevyys (ISO/IEC 27001: 2017, 10).

ISO/IEC 27001 –standardi antaa erittäin selkeät ja toimivat reunaehdot toteuttaa tietoaineiston tallennusta ja dokumentaatiota, mutta mikäli syystä tai toisesta tähän aihealueeseen liittyvät ongelmat osoittautuvat hankaliksi ratkaista organisaatiossa, voi olla eduksi tutkia CWA –mallin (*Cognitive Work Analysis*) mukaisia tapoja jäsentää organisaation toimintaympäristöä. Tässä mallissa ei kysytä ohjeelliseen ajatteluun johdattavia kysymyksiä (kuten ”miten järjestelmän tulisi toimia”) eikä kuvaileviin vastauksiin johtavia kysymyksiä (”Miten järjestelmä itse asiassa käyttäytyy”) vaan kehitystä tukevia kysymyksiä (”Miten työtä voidaan toteuttaa”). Tästä havaitaan, että pelkästään ajattelutavan muutos voi ratkaisevalla tavalla auttaa organisaatiosta vastaavia löytämään ratkaisukeskeisempiä keinoja hallita ongelmia. Koska esimerkkitapauksessa tiedon tallennus ja löytäminen tuottavat ongelmia organisaatiossa, CWA-mallin mukainen ajattelu saattaisi olla keino, jolla käytäntöjä kyettäisiin yhdenmukaistamaan, kunnes ISO/IEC 27001 –standardin vaatimuksenmukaisuus olisi esitetyn ongelman osalta kunnossa.

(Oosthuisen, Pretorius 2016, 17.)

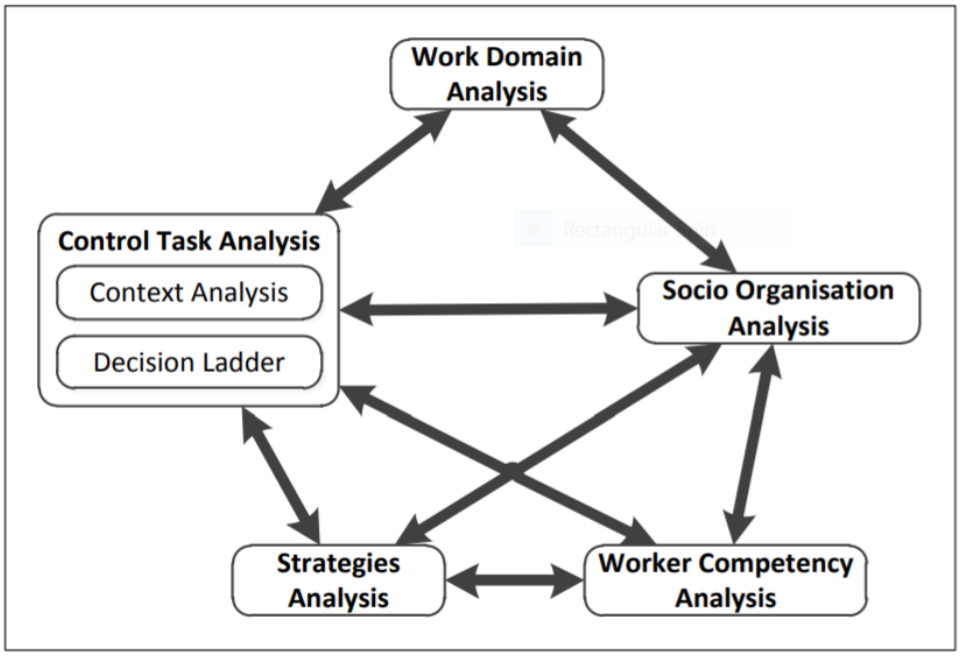


Figure 3: Cognitive work analysis

Kuvio 5: CWA-malli jäsentää organisaatiota ja sen toimintoja käytännönläheisesti (Oosthuisen, Pretorius 2016, 18).

Tietoaineisto on erilaista jokaisessa organisaatiossa, vaikka joitain yhteneväisyyksiä olisikin ja siksi onkin huomattava, ettei tietoaineiston osalta voida antaa ohjeistuksia, jotka kattaisivat kaikki tilanteet. Tietoaineistojen hallintaan tulisi suhtautua siten, että turvallisuus, toimenpiteet ja työtehtävien päämäärät ovat kurinalaisesti jäsenneltyinä ja järjestettyinä. (Vrt. Garcia 2008, 22.)

4 Tulokset

Seuraavassa luvussa esitetään tuloksia tutkimuskysymyksiin esimerkkien analyysin pohjalta. Tarkoitus ei ollut antaa yksityiskohtaisia ohjeistuksia ongelmien ratkaisuun, koska sellaisia ei voi tosiasiallisesti olla. On oleellista ymmärtää, että jokainen organisaatio on erilainen, joten standardin käyttöönoton yhteydessä ilmeneviin ongelmiin on reagoitava aina tilanteen edellyttämällä tavalla, vaikka tiettyjä ongelmanratkaisumenetelmiä käytettäisiinkin. Tietyissä aiheeseen liittyvissä tutkimuksissa on esitelty hyötyjä, joita standardin käytöstä on saatu organisaatiolle. Esimerkiksi tutkimuksessa *Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry* on lueteltu useita konkreettisia tuloksia, joita ISO/IEC 27001 –standardista on tullut organisaatiolle, joista mainittakoon:

- tiedonsäilytyksen, -suojaamisen ja –hävittämisen tehostuminen organisaatiossa
- tietojärjestelmiin kohdistuvien haavoittuvuuksien, uhkien ja riskien vähentäminen hyväksyttäville tasoille
- tietoturvallisuuteen keskittyvä ennakoiva ote
- tietoturvaroolien ja –vastuiden määrittyminen
- tiedon luottamuksellisuuden, eheyden ja saatavuuden prosesseissa
- keskeisen tiedon tiedon turvaaminen (sisäisissä ja ulkoisissa toiminnoissa ja prosesseissa)
- liiketoiminnan jatkuvuuden ja toipumisen suunnitelmien kehittyminen
- tietoturvallisuuden hallintajärjestelmän vaikuttavuuden mittaamisen kehittyminen
- kilpailukykyisyyden, luottamuksen ja vakuuttavuuden lisääntyminen kansallisessa ja kansainvälisessä toiminnassa (Velasco et al 2018, 298)

Tämänlaiset tulokset ovat usein kuitenkin hyvin kyseenalaisia tutkimuksen luotettavuuden kannalta, koska vaikka voidaan olettaa, että ISO/IEC 27001 –standardin mukaisella toiminnalla voidaan kohentaa mainittuja seikkoja organisaatiossa, asianmukaisen aineiston kerääminen on haasteellista ja vaatii pitkän aikavälin mittaustuloksia ollakseen uskottavaa. Lisäksi mittaustuloksia tulisi tarkastella ISO/IEC 27004:2016 –ohjeistusten valossa, jotta tarkastelusta saadaan yhtenäinen, luotettava ja säännönmukainen. Ennen kaikkea ongelmallista on se, mikäli numeerisia tuloksia tulkitaan liikaa eikä niitä ole tarkasteltu suhteutettuna riittävän pitkän aikavälin vertailuaineistoon. Tulisi huomioida, että ISO/IEC –mittausstandardit tarjoavat ensisijaisen ja luotettavan menettelyn juuri ISO/IEC –toimenpiteiden luotaamiseen.

Tässä opinnäytetyössä keskiössä ei luonnollisestikaan ollut valmiiden vastausten antaminen esitettyihin ongelmakohtiin, koska ongelmat voidaan ainoastaan ymmärtää ymmärtämällä organisaatiota ja sen toimintaympäristöä. Tulosten valossa on kuitenkin mahdollista hyödyntää ongelmien luonteisiin sopivia menetelmiä organisaatiosta tai toiminnan luonteesta johdettuna.

4.1. Opinnäytetyön tulokset

Ensisijaiset tutkimuskysymykset olivat:

- mikä on ISO/IEC 27001
- mihin ISO/IEC 27001 liittyy
- miksi ISO/IEC 27001 tulisi ottaa käyttöön
- miten ISO/IEC 27001 voidaan ottaa käyttöön

Opinnäytetyössä on selvitetty, että ISO/IEC 27001 on kansainvälinen tietoturvallisuuden hallintajärjestelmä, joka liitetään saumattomasti organisaation toimintaympäristöön ja prosesseihin. Organisaatio ottaa ISO/IEC 27001 –standardin käyttöön, koska sen avulla tietoturvallisuudesta tulee hallittua.

Entä mihin ISO/IEC 27001:2017 liittyy? Kysymyksen voisi tulosten perusteella pikemminkin muotoilla mihin ISO/IEC 27001:2017 *kiinnittyy*, koska siten hallintajärjestelmän kytkös organisaation tietoturvaan, suojattaviin kohteisiin ja kokonaishallintaan tulee konkreettisemmaksi. Hallintajärjestelmä mukautuu organisaation toimintoihin, jotta niiden hallinnan sattumanvaraisuutta saadaan vähennettyä merkittävästi. Tämä on samalla eräs keskeisistä syistä, miksi ISO/IEC 27001:2017 halutaan ottaa organisaatioissa käyttöön.

Opinnäytetyössä on esitetty ISO/IEC 27001 –standardin vaatimusosien perusteella toteutettavia ratkaisu- ja parantamisehdotuksia esiin nostettuihin kuvitteellisiin ongelmakohtiin. Vaikka ongelmat ja haasteet ovat toisinaan monisäikeisiä ja –ulotteisia, ISO/IEC 27001 –standardin avulla on mahdollista hahmottaa toimintaympäristöä ja sen ongelmia jäsennellyllä ja rakentavalla tavalla. Kuvaillut ongelmat on esitetty tutkimuskysymyksen kannalta siten, että niiden avulla saadaan nopeasti käsitys kokonaistoiminnasta ja sen puutteista organisaatiossa. Tällaisten kuvitteellisten ongelmanratkaisujen etuna on, että ne ovat tutkimuskysymysten näkökulmasta ja keskeisiltä osin todellisen kaltaisia tai ainakin vastaavanlaisia kuin todelliset ongelmat, ja lisäksi organisaation salaisia tietoja ei jouduta käsittelemään. Tällaista tietynlaista narratiivista esittämistä voidaan arvostella, mikäli sen katsotaan olevan perinteisen laadullisen tutkimuksen näkökulmasta epätieteellistä. Todellisuudessa tämän kaltaisen tutkimusotteen ansiosta oli kuitenkin mahdollista tuoda ilmi, miten käytännönläheisiä ongelmia ISO/IEC 27001:2017 –standardin käyttöönotossa on odotettavissa, mikä oli eduksi myös tutkimuskysymyksen ymmärryksen kannalta. Näin ollen empiirisessä merkityksessä ”tieteellisemmissä” tutkimusongelmissa olisi myös omat ongelmansa, jotka tulisivat ilmi viimeistään siinä vaiheessa, kun ratkaisumalleja aletaan etsiä standardin vaatimuksista. Puhdas narratiivisuuskaan ei ole toimivaa, varsinkaan mikäli kyseisellä menetelmällä päästään vain ”paikalliseen, henkilökohtaiseen ja subjektiiviseen” tietoon (Aaltola & Valli 2010, 157.) Kriittinen vaihe organisaation ongelmien arvioinnissa on juuri ongelma-alueiden tunnistaminen, kohdennus, analyysi ja nimeäminen, koska ongelmanratkaisun nopeuden kannalta on ensiarvoisen tärkeää, että arviot organisaation toimintaympäristön tilasta tehdään realistisesti, objektiivisesti, puolueettomasti ja kiihkottomasti, jotta siirtymä seuraaviin vaiheisiin, kuten juurisyiden ymmärtämiseen ja ongelmien varsinaiseen ratkaisemiseen ISO/IEC 27001 –standardin vaatimusosien pohjalta sujuisi ilman suurempia hidasteita ja esteitä.

Kun asiantuntija pyrkii saamaan tietoa organisaatiosta tavoitteenaan edistää ISO/IEC 27001 –standardin mukaisen hallintajärjestelmän käyttöönottoa, hänen tulee pystyä muodostamaan

riittävän yksityiskohtainen kokonaiskuva, joka saadaan tosiasiassa aina jonkin asteisista narratiiveista, ovat ne sitten selostuksia, esityksiä, esitelmiä, perehdyttämisiä tai dokumentaatioita organisaation vallitsevasta tilasta. Vaatii paitsi ISO/IEC 27001 -standardin tietoturvallisuuden hallintajärjestelmän erinomaista tuntemusta myös viileää tulkinta- ja analyysitaitoa, jotta osaa suhteellisen nopeasti ja puolueettomasti erottaa oleellisen epäoleellisesta organisaatiossa standardin vaatimusosan valossa, jotta voi tehokkaasti ja hallitusti edistää käyttöönoton prosessia. Tehtävä on yhtäältä käytännöllistä, mutta myös käsitteellistä, erityisesti kun vaaditaan korkeaa abstraktion ymmärrystä. Abstraktiolla tarkoitetaan tässä pääosin konkreettisen kohteen tietyn piirteen tai piirrejoukon eristämistä ja tarkastelua sellaisenaan.

Keskeisin tämän opinnäytetyön tekemisen yhteydessä syntynyt oivallus on tämä: tietämisen keinojen ja tiedon määrittelyn syvällinen ymmärrys on edelleen haasteellista, mutta joskus kaoottistenkin ympäristöjen jatkuvuuden toimintaedellytyksiä voidaan kohentaa nopeasti ja tehokkaasti pelkästään jäsentämällä toimintaan vaikuttavia osakokonaisuuksia perustellulla ja käytäntövaltaisella tavalla.

4.2. Johtopäätökset opinnäytetyön tuloksista

Tässä alaluvussa kuvataan tiivistetysti ja saavutettujen tulosten perusteella, miten ja millaisten vaiheiden avulla organisaatio voi aloittaa ISO/IEC 27001 –standardin mukaisen tietoturvallisuuden hallintajärjestelmän käytön.

Keskeistä on ensin tutustua huolellisesti ja kriittisesti organisaation toimintaympäristöön, minkä jälkeen voidaan alkaa syventää ymmärrystä siten, että aloitetaan tarkastella organisaatiota ISO/IEC 27001 –standardin vaatimuskohtien näkökulmasta – tavoitteena on tässä vaiheessa saada kokonaiskuva. Tämän jälkeen tarkastellaan organisaation nimettyjä osa-alueita, kuten osastoja, toimintoja ja tehtäväkokonaisuuksia tai muita sellaisia, minkä jälkeen etsitään kunkin toiminnon osalta vastaavat kohdat standardista ja kirjataan ne ylös: esimerkiksi organisaation viestintäosaston toimintojen kannalta keskeisimmät standardin kohdat liittyvät viestinnän vaatimusosiin, mutta eivät silti pelkästään niihin. On keskeistä, että tietoturvan asiantuntija tutustuu itsenäisesti organisaatioon voidakseen ymmärtää, miten kohteessa toimitaan (Garcia 2008, 17).

Seuraavaksi tulee tutustua tehtävänkuvauksiin, tehdä työntekijöitä ja johtoa tietoiseksi tietoturvallisuuden rooleistaan hallintajärjestelmässä. Samalla havaitaan, että tieto organisaatiosta lisääntyy jatkuvasti. Sen jälkeen edistetään hallintajärjestelmän käyttöönoton yleisiä edellytyksiä ja tehdään riskienarviointien pohjalta jatkuvaa parannustyötä, jotta askel askeleelta voidaan lisätä edellytyksiä siirtyä mahdollisimman saumattomasti ISO/IEC 27001 –standardin mukaiseen tietoturvallisuuden hallintajärjestelmään. Kun parannukset ovat riittävän

vaikuttavia ja toiminta on vaatimuksenmukaista, organisaatio voi pyrkiä siihen, että standardin mukaisen tietoturvallisuuden hallintajärjestelmä sertifioidaan.

Käytännön vihjeenä on laittaa standardin edellyttämät perusrakenteet kuntoon ja määritellä ne, koska niiden avulla päästään nopeammin jatkuvaan parantamiseen. Tätä ennen on kuitenkin tarpeen testata ja mitata hallintajärjestelmän toimenpiteiden vaikuttavuutta standardin ISO/IEC 27004:2016 avulla, koska vain asianmukaisilla datan keräämisen ja organisoinnin työkaluilla voidaan saada riittävän yksityiskohtaista tietoa organisaatiosta.

Riippumatta organisaation koosta, ISO/IEC 27001 –standardin mukaisen tietoturvallisuuden hallintajärjestelmän käyttöönotto on tavallisesti vaativa ja aikaa vievä prosessi. Sen vuoksi on tärkeää tietää ajoissa, mitä odottaa ja minkälaisia ongelmia täytyy ratkaista ja miten. Tämän opinnäytetyön avulla on mahdollista saada selvyyttä käyttöönoton vaiheista. Parannuksia voidaan toteuttaa projektinhallintamenetelmien avulla (SFS-käsikirja 327: 2012, 267). Tässä opinnäytetyössä korostetaan sitä, että ISO/IEC 27001 -standardin mukaista tietoturvallisuuden hallintajärjestelmää toteutetaan asiantuntevan ja ammattimaisen ydinjoukon johdolla, joka osaa viestiä organisaation johdolle ja muille tärkeille toimijoille vaatimuksenmukaisuudesta tehokkaalla tavalla. Alussa suositaan kuiluanalyysejä ja riskienhallintamenetelmiä, jotta osataan arvioida organisaation tyytyväisyyttä. Samalla saadaan palautetietoa, jonka avulla voidaan kuvata organisaation kykyä ottaa vastaan muutoksia aikaansaavia uudistuksia.

Eräs konstruktiivinen tapa lähestyä kohdeorganisaation ongelmakohtia, on tuottaa uhkien luonnehdintaa seuraavien vaiheiden avulla:

1. Listaa tarvittavat tiedot, joiden avulla uhat voidaan määritellä

2. Kerää tietoja mahdollisista uhista

3. Jäsennä tieto käyttökelpoiseksi

(Garcia 2008, 26).

On keskeistä, että organisaation turvattavat kohteet ja mahdolliset uhat tunnistetaan, jolloin hallintajärjestelmä saadaan alusta alkaen fokusoitumaan riittävän vaikuttavasti oleellisiin kohteisiin. Tämän seurauksena vastuu- ja roolikysymykset ovat kirkkaasti havaittavissa, jolloin hallintajärjestelmä ei pohjaudu sattumanvaraisuuteen. Menetelmillä DSR (Design Science Research framework), STS (Socio-technical Systems) ja CWA (Cognitive Work Analysis) on kaikilla paikkansa organisaation ongelmanratkaisun välineinä, kun ensin huomioidaan ongelman ja organisaation luonne ja erityispiirteet, standardin vaatimuksenmukaisuus ja hallintakeinot, joilla pyritään lisäämään standardin mukaista kokonaisturvallisuutta yksityiskohtaisemmalla tasolla. Turvallisuuskäytäntöjen mukaan kohteen tunnistusmenetelmiä käytetään, jotta osataan määritellä suojattavia kohteita. Kohteet asetetaan tärkeysjärjestykseen analysoimalla

seurauksia, joita syntyisi siitä, että suojattaviin kohteisiin liittyvät uhat toteutuisivat (Garcia 2008, 53-54).

On huomattava, että huolellisella suunnittelulla ja tehokkailla riskienhallintamenetelmillä voidaan suurimmat ongelmakohdat jopa välttää. Edellytyksenä kuitenkin on, että asiantuntija perehtyy ennalta organisaation heikkouksiin, jotta tiedetään, onko standardin mukaiseen tietoturvallisuuden hallintajärjestelmään siirtymiseen ylipäätään edellytyksiä tai resursseja. Jos riittävän moni organisaatiossa ymmärtää standardista saatavat hyödyt tietoturvallisuuden hallittavuuden kannalta, toteuttamiselle on erinomaiset lähtökohdat. (ISO/IEC 27003:2017, 13.)

Mikäli tietoturvallisuuden hallintajärjestelmä havaitaan kuitenkin tehottomaksi, toimitaan karkeasti ottaen kuten turvallisuusjärjestelmien kehittämisen vaiheissa tyypillisestikin: tunnistetaan haavoittuvuudet, päivitetään alkuperäistä suojausjärjestelmää suunnittelu- ja analyysijaksojen päätteeksi ja tarkistetaan, onko tavoitteet määriteltävä joiltain osin uudelleen. Tätä sykliä toistetaan, kunnes voidaan mitatuilla tuloksilla osoittaa, että hallintajärjestelmä täyttää sille asetetut tavoitteet (Garcia 2008, 6).

Lopulta organisaatio voi pyrkiä saamaan sertifikaatin ISO/IEC 27001 –standardin mukaiselle tietoturvallisuuden hallintajärjestelmälle, mikä viime kädessä todistaa vaikuttavuuden ja tehtyjen toimenpiteiden tehokkuuden.

Lähteet

Painetut

Aaltola, J. & Valli, R. (toim.) 2007. Ikkunoita tutkimusmetodeihin I. Jyväskylä: PS-kustannus.

Aaltola, J. 2010. Filosofia, tiede, ymmärtäminen. Teoksessa Aaltola, J. (toim.) Ikkunoita tutkimusmetodeihin II. Jyväskylä: PS-kustannus, 12-27.

Ada, S., Gupta, M. & Sharman, R. 2009. Handbook of Research on Social and Organizational Liabilities in Information Security. Hershey: IGI Global.

Alasuutari, P. 2011. Laadullinen tutkimus 2.0. Tampere: Vastapaino.

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tallinna: AS Pakett.

Garcia, M.L. 2008. The Design and Evaluation of Physical Protection Systems. Second Edition. Burlington: Butterworth-Heinemann USA

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2002. Tutki ja kirjoita. Helsinki: Tammi.

ISO/IEC 27001: 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen standardisoimisliitto SFS; Geneva: International Organization for Standardization.

ISO/IEC 27001: 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen standardisoimisliitto SFS; Geneva: International Organization for Standardization.

ISO/IEC 27002: 2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Helsinki: Suomen standardisoimisliitto SFS; Geneva: International Organization for Standardization.

ISO/IEC 27003: 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Ohjeistusta. Helsinki: Suomen standardisoimisliitto SFS; Geneva: International Organization for Standardization.

ISO/IEC 27004:2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Seuranta, mittaus, analysointi ja arviointi. Helsinki: Suomen Standardisoimisliitto SFS; Geneva: International Organization for Standardization.

Murtonen M. 2003. Riskien arviointi työpaikalla. Työkirja. Sosiaali- ja terveysministeriö. Tampere.

Oosthuisen, R & Pretorius, L. 2016. Assessing the Impact of New Technology on Complex Sociotechnical Systems, *South-African Journal of Industrial Engineering*, *27*, s. 15-29.

Saarela-Kinnunen M. & Eskola J. Tapaus ja tutkimus = tapaustutkimus? Julkaisussa: Aaltola J, Valli R, toim. Ikkunoita tutkimusmetodeihin I. Metodin valinta ja aineiston keruu: virikkeitä aloittelevalle tutkijalle, s. 158-169. Jyväskylä: PS-kustannus, 2001. Chydenius-Instituutin julkaisuja 2.

SFS-käsikirja 327: 2012. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen standardisoimisliitto SFS.

Valtionhallinnon tietoturvakäsitteistö. 2003. Vahti 4/2003. Helsinki: Valtiovarainministeriö.

Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P. & Moscoso-Zea, O. 2018. Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. *In 3rd International Conference on Information Systems and Computer Science (Inciscos).* (s 294-300). Quito: Ecuador

Yin, R. K., 1994. Case Study Research Design and Methods: Applied Social Research and Methods Series. Second edn. Thousand Oaks, CA: Sage Publications Inc.

Sähköiset lähteet

Yritysturvallisuus. 2020. Elinkeinoelämän keskusliitto. EK:n turvallisuusmalli. Viitattu 31.3.2020. https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

Kuviot

Kuvio 1: Riskien arvioinnin ja hallinnan vaiheet (Murtonen 2003) 22
Kuvio 2: EK:n turvallisuusmalli https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/.....25
Kuvio 3: DSR-menetelmä ongelmanratkaisun apuna (Oosthuisen, & Pretorius 2016, 16) 31
Kuvio 4: STS-malli auttaa hahmottamaan toimintaympäristöä (Ada Gupta & Sharman 2009, 282) 33
Kuvio 5: CWA-malli jäsentää organisaatiota käytännönläheisesti (Oosthuisen, Pretorius 2016, 18) 36

Taulukot

Taulukko 1: Sisäisen auditoinnin ja johdon katselmuksen ydinkohdat (ISO/IEC 27001: 2017, 13). 28

Liitteet

Liite 1: Keskeiset käsitteet..... 45

ISO/IEC JTC 1

ISO/IEC Joint Technical Committee 1 ISO:n ja IEC:n yhteinen komitea, jonka tehtävänä on tietotekniikan yleisten menetelmien ja tekniikoiden standardointi.

Katselmus

Hankkeen tai työvaiheen päätyttyä pidettävä työn tulosten arviointi. Katselmukseen osallistuvat yleensä hankkeen osapuolet, mutta usein myös ulkopuolisia. Katselmuksen tuloksia käytetään usein päätöksentekoon työn jatkamisesta.

Riskianalyysi

Systemaattisen menetelmin tapahtuva uhkien ja riskien arviointi.

Riskienhallinta

Järjestelmällinen toiminta riskien rajoittamiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa

Sertifikaatti

Kansallisen tai kansainvälisen toimivaltaisen viranomaisen antama tai muu pätevä todistus siitä, että tietotekninen tuote tai palvelu täyttää tiettyä tietoturvallisuuden tasoa vastaavat vaatimukset.

Standardi

Valtuutetun tahon tietyllä alalla käytettäväksi hyväksymä tai alalla laajasti omaksuttu tuotetta tai toimintaa koskeva malli, mitta, ominaisuus tai nimitys.

Tietoturvallisuus

1) Tavoitetila, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa siten, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille.

2) Lainsäädäntö ja muut normit sekä toimenpiteet, joiden avulla pyritään varmistamaan tietoturvallisuus niin normaali- kuin poikkeusoloissakin.

Tietoturvapolitiikka

1) Valtakunnan tasolla tietoturvanormien ja niiden täytäntöönpanon muodostama kokonaisuus.

2) Organisaation tasolla johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta.

Turvallisuuskulttuuri

Oman, sidosryhmien jäsenten ja ulkopuolistenkin turvallisuuden huomioon ottaminen toiminnassa ja suunnittelussa.