HAAGA-HELIA
ammattikorkeakoulu

Organisaation tietoturvan ja liiketoiminnan jatkuvuuden kehittäminen, case: Aalto-Yliopisto, Palvelukeskus PAVE

Leena Satakieli

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2013

Tekijä tai tekijät Leena Satakieli	**Ryhmä tai aloitusvuosi** 2010
Opinnäytetyön nimi Organisaation tietoturvan ja liiketoiminnan jatkuvuuden kehittäminen Case: Aalto-Yliopisto, Palvelukeskus PAVE	**Sivu- ja liitesivumäärä** 58 + 9
Ohjaaja tai ohjaajat Petri Hirvonen	

Tietoturvan roolin merkitys kasvaa nykyorganisaatioiden toiminnassa. Liiketoiminta ja IT vaikuttavat yhä enemmän toisiinsa, minkä tuloksena nähdään niiden yhteiset kehityslinjaukset ja integrointi. Tietoturvan kehittämistä kannattaa lähestyä liiketoiminnan tarpeiden näkökulmasta. Kun tietoturvatyötä käsitellään prosessina ja jatkuvuuden suunnitelma on ajan tasalla, organisaation toiminnalla saavutetaan korkeampi suoritus- ja kilpailukyky, tavoitettu asiakastyytyväisyys ja korkeatasoinen tuottavuus.

Tämän opinnäytetyön ja tutkimuksen tarkoituksena oli ajankohtaisten kirjallisuuslähteiden, parhaiden käytäntöjen ja standardien pohjalta kehitellä selkeä, jäsennelty, elämänlähtöinen organisaation tietoturvan kehittämisen toimintamalli.

Tietoperusta (teoria, kirjallisuuskatsaus) -osuudessa on käsitelty kolme aiheeseen liittyvää kokonaisuutta. Ensiksi on tutkittu ja esitetty tietoturva nykyvaatimusten valossa. Toiseksi on kuvattu keinoja, joiden avulla organisaation tietoturvan nykytila selvitetään ja tarkastetaan, ja sitten tehostetaan. Kolmanneksi on esitetty organisaation riskienhallintaan ja liiketoiminnan jatkuvuuden suunnitteluun liittyviä teoria-asioita.

Tulokset (toteutus, empiria) -osuudessa on esitetty, miten teorian pohjalta tietoturvatarkastusta ja liiketoiminnan jatkuvuutta pitää suorittaa käytännössä kohdeorganisaatiossa. Osuus sisältää mallit, pohjat, dokumentit ja työkalut, joiden avulla näitä asioita suoritetaan. Näin teorian analyysin ja empirian suorituksen tuloksena aikaansaatu toimintamalli esitettiin tietoturvan kehittämisehdotuksena kohdeorganisaation johdolle.

Työn tuloksena syntyvää mallia ja välineitä hyödyntämällä kohdeorganisaatio pystyy tehokkaasti ja suhteellisen suoraviivaisesti suorittamaan tietoturva-auditointia esim. sisäisen tarkastuksen toimesta sekä ylläpitämään riskienhallintatyötä ja kehittämään liiketoiminnan jatkuvuutta. Laajemmin työn tuloksia voidaan hyödyntää myöhemmin muissakin organisaatioissa ja yrityksissä.

Tämä on kvalitatiivinen eli laadullinen tapaustutkimus, jossa käytetään myös toimintatutkimuksen otetta.

Asiasanat
Tietoturva, tarkastus, liiketoiminnan jatkuvuus, riskienhallinta

Author(s) Leena Satakieli	**Group or year of entry** 2010
The title of thesis Developing the information security and business continuity in an organization Case: Aalto-University, Service Center PAVE	**Number of report pages and attachment pages** 58 + 9
Advisor(s) Petri Hirvonen	

The importance of the role of information security is growing in organizations nowadays. Business and IT are increasingly influenced by each other. The result of this is their joint development in policies and integration. The development of information security should be approached from the perspective of business needs. When the security work is handled as a process and the continuity of business is up to date, an organization has higher performance and competitiveness, and it reaches customer satisfaction and a high level of productivity.

The purpose of this thesis was to develop a clear, structured and life-oriented approach for improving the information security in an organization by using current literature, best practices and standards. The study was carried out by using the approaches of constructive, qualitative, descriptive types of research including a case study.

The theoretical part the thesis includes three matters regarding the subject. First of all, the requirements of modern information security were studied and presented. Secondly, the means by which the current state of an organization's information security can be audited and developed to a higher level were described. Thirdly, the risk management and the theory concerning the business continuity planning of an organization were presented.

The empirical part describes how the security audit and business continuity planning should be carried out in the target organization in practice. The part includes models, templates, documents and tools that help with these issues. By combining the analyses of the theoretical part and results of the empirical part, the operating model of information security improvement in an organization was achieved as the main result of the thesis. The model was presented to the management of the target organization as a proposal on how to develop its information security.

The target organization can use the model and the tools to improve its own information security and business continuity e.g. by using internal audit department or a team. More broadly, the results can be further used in other organizations and companies.

Key words
Information security, audit, business continuity, risk management

Sisällys

1 Johdanto

1.1 Tutkimuksen tausta

Tietoturvan merkitys niin pk- kuin isoissakin yrityksissä ja organisaatioissa on kasvanut koko ajan ja tulee kasvamaan, mikä johtaa siihen, että liiketoiminta ei pysty enää onnistuneesti ja tuloksellisesti kehittymään ilman kestävää ja vahvaa tietoturvaa.

Kohdeorganisaatiolla (siitä alempana tarkemmin) on tarve arvioida ja jatkokehittää tietoturvaansa ja taata toimintansa jatkuvuus. Tutkimuksen päämääränä on standardien, lainsäännösten, julkishallinnon ja VAHTI -suositusten (Valtionhallinnon tietoturvallisuuden johtoryhmä), parhaiden käytäntöjen ja ajankohtaisten kirjallisuuslähteiden pohjalta rakentaa elämänlähtöinen organisaation tietoturvan kehittämisen toimintamalli. Työn tuloksena syntyvää mallia ja välineitä hyödyntämällä organisaatio pystyy tehokkaasti ja suhteellisen suoraviivaisesti arvioimaan tietoturvansa nykytila suorittamalla tietoturva-auditointia esim. sisäisen tarkastuksen toimesta sekä toteuttamaan riskienhallintatyötä ja samalla takaamaan liiketoiminnan jatkuvuus. Työn tulosten merkittävyys kohdeorganisaatiolle ilmenee siinä, että sen toimintoja (mm. aiheeseen liittyvät prosessit ja käytännöt) parannetaan, minkä seurauksena kohoaa myös koko organisaation toiminnan, johtamisen ja laadun taso. Laajemmin työn tuloksia voidaan hyödyntää muissakin organisaatioissa ja yrityksissä.

Tutkimuksen tehtävänä on luoda organisaatiolle mahdollisuus varmistua siitä, että sen tietoturva on tarvittavalla tasolla, sillä pystytään tukemaan liiketoiminnan jatkuvuutta ja vastaamaan tietoturvallisuuden nykyajan vaatimuksiin ja haasteisiin, toimimaan proaktiivisesti ja systemaattisesti. Tutkimuksessa tämä tehtävä toteutetaan esittämällä tietoturvan kehittämisen toimintamallia eli etenemistapaa, joka osoittaa oikeassa järjestyksessä suoritettavia toimenpiteitä, menetelmiä ja välineitä sekä esimerkkien muodossa niitä tuloksia, joihin pyritään.

Toimintamallin luomista tukevat tutkimuksen kaksi tärkeintä osuutta: tietoperusta ja tulokset, jotka kytkeytyvät kiinteästi toisiinsa. Tietoperustaosuudessa (teoria, kirjallisuuskatsaus) on käsitelty niitä asioita, joita on toteutettu käytännössä tulokset-

osuudessa. Näitä aiheeseen liittyviä aisakokonaisuuksia on kolme. Ensiksi on tutkittu ja esitetty tietoturva nykyvaatimusten valossa. Toiseksi on kuvattu keinoja, joiden avulla organisaation tietoturvan nykytila selvitetään ja tarkastetaan, ja sitten tehostetaan. Kolmanneksi on esitetty organisaation riskienhallintaan ja liiketoiminnan jatkuvuuden suunnitteluun liittyviä teoria-asioita. Tulokset (toteutus, empiria) -osuudessa on esitetty miten tietoperustan eli teorian pohjalta tietoturvatarkastusta ja liiketoiminnan jatkuvuutta pitää suorittaa käytännössä kohdeorganisaatiossa. Osuus sisältää mallit, pohjat, dokumentit ja työkalut, joiden avulla nämä kohdat suoritetaan. Näin teorian analyysin ja empirian suorituksen tuloksena aikaansaatu toimintamalli (kuvattu Pohdinta-luvussa) esitettiin tietoturvan kehittämisehdotuksena kohdeorganisaation johdolle.

1.2 Tutkimusongelma, -kysymykset, -tavoitteet

Tutkimuksen aihe *Organisaation tietoturvan ja liiketoiminnan jatkuvuuden kehittäminen* sai alkunsa havainnoista ja hiljaisista signaaleista, joita tuli vastaan tutkimuksen tekijälle AMK-koulutuksen ja työelämän aikana. Aihe on ajankohtainen, kysytty ja selvästi tarvitsee lisää tutkimista ja kehittämistä. Ko. aihe liittyy tutkimuksen tekijän työpaikkaorganisaation (tästä eteenpäin nimellä *case-* ja *kohdeorganisaatio*) hankkeeseen, jonka tulokset tulevat vaikuttamaan ratkaisevasti koko organisaation toimintaan.

Tämän opinnäytetyön ja tutkimuksen tuloksina saadaan tietoturvaan liittyvien toimintojen ja asioiden selkeyttäminen, yhdenmukaistaminen, prosessinomainen toiminta, keskitetty ohjaus ja valmis mallisto ja työkalusto. *Tutkimusongelmaksi* siten tulee: *Miten selvitetään ja tarkistetaan organisaation tietoturvatasoa, miten sitä parannetaan, miten saavutetaan toiminnan jatkuvuus, miten pitää toimia, mitä huomioida sekä mihin tuloksiin pyrkiä ja kuinka käyttää niitä niin, että tietoturva organisaatiossa olisi jatkossa entistäkin tehokkaampaa, taloudellista ja vastaisi jatkuvasti kasvaviin vaatimuksiin.*

Pohjautuen yllä kuvattuun ongelmaan, kohdeorganisaatiossa toteutettavan hankkeen päämääriin ja tavoitteeseen, tämä käytännönläheinen tutkimus vastaa kahteen tutkimuskysymykseen. Ensimmäisen kysymyksen avulla pyritään selvittämään organisaation tietoturvan nykytila ja esittämään tuloksia ja kehitysehdotuksia tietotoruvan jatkokehittämistä varten. Toinen kysymys keskittyy organisaation liiketoiminnan jatkuvuuden

suunnitteluun, jossa mm. hyödynnetään ensimmäisen kysymyksen tuloksia. Kumpaakin kysymystä käsitellään sekä tietoperusta- että tulokset-osuuksissa. Tietoperusta on laajempi ensimmäisen kysymyksen osalta, koska sisältää sen läpikäymien alueiden lisäksi myös teoriaosuuden organisaation tietotuvan periaatteista, mitkä ovat välttämättömiä kummankin kysymyksen käsittelyssä.

Ensimmäinen *tutkimuskysymys K1* on seuraava:

K1. Miten esitetään kirjallisuudessa ja toteutetaan käytännössä seuraavat asiat: kuinka selvittää organisaation tietoturvan nykytila, sen puutteet, ongelmat ja muutostarpeet, miten ja mitä tuloksia saadaan, miten ja kenelle esitetään, miten hyödynnetään, ja mitä vaatimuksia näille kaikille pitää olla?

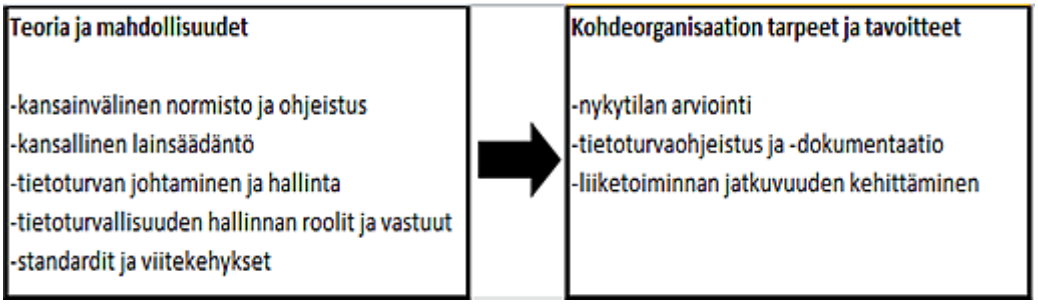
Näin tämä K1-kysymys esittää seuraavia tavoitteita tutkimuksen tuloksille. Yhtenä *tavoitteena* on esittää tutkittujen kirjallisuuslähteiden pohjalta ko. kysymyksessä ja sen seuraavissa tavoitteissa mainitut asiat niin, että niitä voi hyödyntää käytännössä. *Toisena tavoitteena* on selvittää mitä tietolähteitä, ohjauksia ja ohjeistuksia ko. arvioinnissa käytetään sekä mitä vasten sitä suoritetaan, eli mitkä asiat toimivat arvioinnin perusteina ja kriteereinä. *Kolmantena tavoitteena* on kuvata menetelmä eli prosessi ja eteneminen, jonka mukaan tietoturvan arviointi pitää tapahtua. *Neljäntenä tavoitteena* on saada käsitys siitä, mitä tuloksia pitää saada aikaan, sekä missä muodossa, kenelle ja miten esittää ja miten jatkokäsitiellä, jolloin ko. asioita havainnollistetaan tietoturvatarkastusraportin esimerkkinä eli pohjana.

Toinen *tutkimuskysymys K2* on seuraava:

K2. Miten nykyteorian ja -vaatimusten pohjalta toteutetaan käytännössä seuraavat asiat: miten tietoturvan arvioinnin jatkeeksi suunnitellaan liiketoiminnan jatkuvuus, mitä ko. suunnitelma pitää sisällään, miten sitä käytetään ja mitä vaaditaan, jotta lopputuloksena organisaatio saisi käyttöönsä tehokkaat pelastustyökalut ja jatkuvasti uusiutuvan ja paranevan prosessin eikä pelkän dokumentaatiokansion.

K2-kysymykseen liittyen, samoin kuin edelliskysymyksessä, *ensimmäisenä tavoitteena* on esittää tutkitun kirjallisuuslähteiden pohjalta K2-kysymyksessä ja sen seuraavissa tavoitteissa mainitut asiat niin, että niitä voi hyödyntää käytännössä. *Toisena tavoitteena* on selvittää ja valmistella organisaation liiketoiminnan jatkuvuussuunnitelmaa varten sen rakenne ja pääosat, mm. tietoturvapolitiikka ja -organisaatio, vastuut, toiminnot, suojattavat kohteet, riskienhallinta jne. *Kolmantena tavoitteena* on kuvata työkalut ja dokumentit, joiden avulla suunnitelmasta saadaan irti konkretiaa ja hyötyä. *Neljäntenä tavoitteena* on esittää valmis suunnitelmaesimerkki, josta ilmenee jatkuvuussuunnittelun malli, käynnistettävät ja suoritettavat toimenpiteet kertasuorituksina sekä myös prosesseina.

Seuraavassa esitetään yleiskuva tutkimuksen alustavasta viitekehyksestä.



Kuvio 1. Tutkimuksen alustava käsitteellinen viitekehys

1.3 Tutkimuksen rajaus

Mallin ja välineistön kehittämisessä pyritään käsittelemään asioita yleisemmällä tasolla, mahdollisuuksien mukaan rajoittumatta kohdeorganisaation ominaispiirteisiin. Työn ulkopuolelle jäävät kokonaan tai osittain: taloudelliset näkökulmat, mahdollisesti tarvittaviin tietojärjestelmiin ja niiden kehittämishankkeisiin liittyvä seikat. Hankkeen projektihallinta esitetään vain pääpiirtein. Työssä esitettävät linjaukset ja periaatteet myötäilevät alan standardien vaatimuksia ja suosituksia. Tällä on pyritty siihen, että menetelmät ja tulokset vastaavat tärkeitä vaatimuksia eivätkä sisällä mitään ylimääräistä tai turhaa. *Tulokset*-osuudessa esitetyt tietoturvatarkastusraportti ja liiketoiminnan jatkuvuuden suunnitelma ovat esimerkkejä ja pohjia/malleja näille toteutuksille kohdeorganisaatiossa. Näin varsinaista ko. tarkastusta ei ollut tarkoitus toteuttaa tämän tutkimuksen puitteissa.

1.4 Tutkimuksen metodologia ja opinnäytetyön menetelmät

Tämä on kvalitatiivinen eli laadullinen tapaustutkimus, jossa käytetään myös toimintatutkimuksellista otetta. Sekä kvalitatiivinen että toimintatutkimus ovat tutkimusstrategioita eli niillä kuvataan tapaa, jolla tutkimus syntyy.

Kvalitatiivisessa tapaustutkimuksessa pyritään tunnistamaan, tulkitsemaan ja kuvaamaan kohteen merkitystä ja laatua kuluttajien ja asiakkaiden näkökulmasta. Kun lähdetään selvittämään kvalitatiivista tapaustutkimusta, voidaan miettiä kysymyksiä mitä, miksi ja miten. Aineiston keruumenetelmä valitaan tutkimusongelman perusteella.

Toimintatutkimuksessa pyritään kehittämään tutkimuskohteen (kohdeorganisaation) toimintaa ja ympäristöä vaikuttamalla siihen uusilla näkökulmilla ja ideoilla. Vaikuttamaan päästään, kun tutkija osallistuu organisaation toimintaan ja käyttää erilaisia analyysimenetelmiä toimintatutkimuksen suorittamiseksi. Tapaustutkimuksen vaiheistus on seuraava: selvitetään kohdeorganisaation nykytila, selvityksen pohjalta kehitetään tutkimuksen toimintamalli, suoritetaan mahdollisimman vaikuttavia keinoja/tapoja, joiden vaikutuksia seurataan, minkä jälkeen tarjotaan kehittynyttä toimintamallia kohdeorganisaatiolle.

Työvälineistönä toimivat alan ja aihealueen kansainväliset ja kotimaiset standardit, parhaat käytännöt, julkishallinnon ja VAHTI -suositukset sekä ajankohtaisin kirjallisuus. Näitä käsitellään omissa luvuissaan jäljempänä tässä työssä.

Työmenetelminä toimivat edellisessä kohdassa esitettyjen materiaalien ja lähteiden tutkiminen, läpikäynti, siinä kuvattujen ja suositeltavien välineiden ja menetelmien hyödyntäminen sekä case-tapaukseen sovittaminen. Suunnittelema työ sisältää lähestymistavat, toteuttamisprosessin kuvaukset sekä siihen liittyen työkalut (dokumenttipohjat, arviointikuvaukset, työkalut mm. taulukoiden muodossa), joiden avulla pystyttäisiin tehokkaasti tarkistamaan kohteen tietoturvan tasoa ja suunnittelemaan liiketoiminnan jatkuvuutta.

1.5 Sanasto ja terminologia

Tutkimuksen kohdealueella tapahtuvaa kehitystä myötäilee oma spesifinen terminologia, joka on käytännössä aika laaja. Lista tämän työn sisältämistä termeistä on esitetty Liitteessä 1. Sen lisäksi tärkeimmät lyhennykset on selitetty suoraan tämän työn teksteissä.

1.6 Tutkimuksen organisaatio ja kumppanit

Opinnäytetyön tekijä, hankkeen työn toimittaja, sihteeri ohjauskokouksissa: Leena Satakieli
Opinnäytetyön ohjaaja: Petri Hirvonen
Toimeksiantajan edustaja: Hemmo Rissanen, Palvelukeskus PAVE:n johtaja, kohdeorganisaation hankkeen koordinaattori

Yhteistyökumppanina toimii Palvelukeskus PAVE, joka on Aalto-ylipiston osa ja sisäinen organisaatio, joka vastaa sen kirjanpidosta ja taloushallinnon tehtävistä. Sisäisiin sidosryhmiin kuuluvat PAVE:n asiakkaat, toimittajat, niiden asiantuntijat ja vastuuhenkilöt.

2 Tietoperusta: teorian ja kirjallisuuden käsittely

Tämä luku esittää *Tietoperusta*-osuutta ja sen kaksi alalukua sisältävät vastaukset vastaavien tutkimuskysymysten alakysymyksiin ja tavoitteisiin *teorian ja kirjallisuuden* osalta. Ensimmäinen alaluku käsittelee K1-tutkimuskysymystä ja siinä kuvataan ja läpikäydään tietoturvan keskeisintä termistöä, roolia organisaatiossa, siihen liittyvää normistoa ja standardeja, hallinnointikuvioita organisaatiossa, vastuita, valvontaa, seurantaa, mittaamista ja lisäksi tarkkaillaan arviointiprosessia. Toisessa alaluvussa käsitellään K2-tutkimuskysymyksen teoriaperustaa, ml. liiketoiminnan jatkuvuus ja sen suunnittelu, jolloin perehdytään alueen termistöön, tavoitteisiin ja hyötyihin, standardeihin, roolitukseen, jatkuvuussuunnitelman laatimisprosessiin ja valmiin suunnitelman testaukseen.

2.1 Tietoturva ja sen tarkastaminen organisaatiossa

2.1.1 Mitä tietoturva on

Tietoturva itse käsitteenä tarkoittaa tietojen, palvelujen, järjestelmien, sovellusten ja tietoliikenteen suojaamista uhkatekijöiltä, joita ovat esim. huijausyritykset, roskapostit, henkilökohtaisten tietojen loukkaus, virukset ja tietojen vakoilu. Tietoturvallisuuden tärkeimpiin osa-alueisiin kuuluvat saatavuus, luottamuksellisuus ja eheys. Saatavuus tai useimmin käytetty termi käytettävyys on sitä, että tieto on saatavilla silloin, kun sitä tarvitaan. Luottamuksellisuus tarkoittaa sitä, että tietoja ja tietojärjestelmiä voivat käsitellä vain ne henkilöt, joilla on siihen oikeus. Kolmas osa-alue on eheys, jossa tiedon oikeellisuus on siinä määrin oikeaa, että tallennetun tiedon muutosta ei ole tehty sen jälkeen, kun tiedon todennettu tekijä on sitä viimeksi muokannut (VAHTI 2012.) Hyvään tietoturvallisuuteen kuuluu työntekijöiden ymmärrys sen merkityksestä ja se, että työskennellään sen saavuttamiseksi lainsäädäntöä toteuttaen (Laaksonen, Nevasalo & Tomula 2006, 17).

2.1.2 Ohjeistus ja dokumentaatio tietoturvan perustana

Hakala (2006, 34) kertoo, että hyvä tietoturva edellyttää tarkkaan suunniteltua johtamista, systemaattista ja prosessinomaista toimintaa. Tärkeimpiä edellytyksiä tietoturvatyölle on organisaation toimintoja kattava dokumentoitu tietoturvapolitiikka ja ohjeisto. Sen tarkoitus on kertoa, miten tarvittavaa tietoturvatasoa ylläpidetään ja parannetaan ja mitä toimenpiteitä käytetään sen saavuttamiseksi. Tietoturvatyön ohjeita käytetään organi2saation tietojen käsittelyssä, Internetin ja sähköpostin käytössä, laitteiden ja järjestelmien käytössä, eri prosesseissa ja toiminnoissa. Kyseiset ohjeet laaditaan standardien ja viitekehysten mukaan. Seuraavaksi esitetään tietoturvaohjeistuksen kolme tasoa ja niiden tehtävät.

Taulukko 1. Tietoturvaohjeistuksen kolme tasoa ja tehtävää. (Miettinen 2002, 22)

TASO	TEHTÄVÄ
Politiikka	Otetaan huomioon tietoturvallisuuden puitteet ja vastuut
Standardit	Kuvataan tietoturvan käytäntö, voi tarkoittaa myös organisaation omia sisäisiä toimintatapoja, ei pelkästään yleisiä tietoturvastandardeja
Toimintaohjeet	Tapa, jolla tietoturvaan liittyvät asiat käsitellään

2.1.3 Kansainvälinen normisto ja ohjeistus

OECD (Organisation for Economic Cooperation and Development) eli Taloudellisen yhteistyön ja kehityksen järjestö on ensimmäisiä tietojärjestelmien ja -verkkojen ohjeistusten tekijöitä. Ko. ohjeistuksen tarkoituksena on nostaa etusijalle turvallisuussuunnittelu ja -hallinto, jolloin organisaatiossa tullaan ymmärtämään turvallisuuden tarve. Ohjeistus sisältää yhdeksän periaatetta, joita ovat turvallisuustietoisuus, vastatoimet, vastuullisuus, eettisyys, riskien arviointi, demokratia, turvallisuuden hallinta, turvallisuuden suunnittelu ja uudelleenarviointi. OECD turvallisuusohjeistus on otettu huomioon myös VAHTI-ryhmän laatimissa tietoturvaohjeistuksissa. (Laaksonen ym. 2006, 23–24.)

Sarbanes-Oxley Act eli SOX - kyseinen säännös ohjaa, kuinka taloudellista tietoa tulisi käsitellä organisaatiossa. Säännös ohjaa säilyttämään kaikki tilinpäätöksiä koskevat tiedot missä tahansa muodossa seuraavan seitsemän vuoden ajan. SOX-säännös on saanut alkunsa Yhdysvalloissa eikä se koske suoraan suomalaisia organisaatioita. Se koskee vain niitä organisaatioita, joiden nimi on Yhdysvaltojen pörssissä SEC:ssä sekä joitakin suomalaisia tytäryhtiöitä, jotka toimivat ulkomailla ja joiden toiminta koskettaa koko organisaatiota. Se sisältää hyviä lähestymistapoja ja käytäntöjä, joiden käyttö on hyödyllistä ja suositeltava tietoturvatyössä (Laaksonen ym. 2006, 24–25.)

EU-lainsäädäntö ja Suomen kansallinen lainsäädäntö toimivat samansuuntaisesti myös tietoturvan osalta. Euroopan yhteisön direktiivit eivät ole suoraan osa kansallista lainsäädäntöä, mutta ne edellyttävät kansallista implementointia. Direktiivejä on paljon ja juuri tietoturvaa koskettavia ainakin kaksi: henkilötietojen suoja, sähköisen viestinnän tietosuoja. (VAHTI 2011, 15–16.)

2.1.4 Kansallinen lainsäädäntö

Suomessa ei ole omaa yhtenäistä tietoturvalakia, joka sisältäisi kaikki tietoturvavelvoitteet. Lainsäätäjä on nähnyt parempana vaihtoehtona sisältää tietoturvavelvoitteet jonkin muun lain osaksi. Suomalaisten perusoikeudet on määritelty perustuslaissa, eikä niistä voida poiketa kuin lain perusteella. Tietoturvatoimenpiteissä on otettava huomioon jokaiselle taholle kuuluva yksityisyyden suoja. Kansalliseen lainsäädäntöön kuuluvat lait ovat perustuslaki, julkisuuslaki, henkilötietolaki, laki kansainvälisistä tietoturvallisuusvelvoitteista, laki yksityisyyden suojasta työelämässä, sähköisen viestinnän tietosuojalaki, liike- ja ammattisalaisuudet, laki tietoyhteiskunnan palvelujen tarjoamisesta, laki sähköisestä asioinnista viranomaistoiminnassa, laki sähköisestä allekirjoituksesta ja viestintämarkkinalaki. (Laaksonen ym. 2006, 27–30.)

2.1.5 Viitekehykset ja standardit

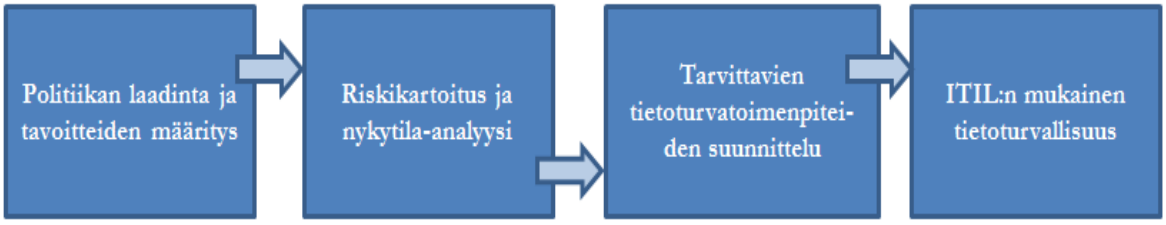
Laaksosen ym. (2006, 83) mukaan tietoturvan hallinnoinnin avuksi on kehitetty erilaisia standardeja ja viitekehyksiä eli malleja. Niiden avulla pyritään suunnittelemaan ja toteuttamaan organisaation tietoturvallisuutta. Malleja ei tarvitse käyttää yksinään, niiden eri ominaisuuksia voidaan yhdistellä. Eniten käytettyjä ja tunnettuja ovat:

- Viitekehykset: Cobit, ITIL, GAISP
- Standardit: Bs-standardi, ISO-standardit, ISF

Viitekehykset

COBIT (Control Objectives for Information and related Technology) -viitekehystä voidaan hyödyntää määriteltäessä tietojenkäsittelyn liiketoiminnallisia tavoitteita ja sitä, miten niiden saavuttamista voidaan mitata. COBIT määrittelee tietoturvallisuuden kannalta tärkeitä prosesseja, jotka tuottavat organisaatioille tarpeellista informaatiota. (Laaksonen 2006, 92.)

ITIL (Information Technology Infrastructure Library) on suunniteltu kattamaan IT:n tärkeimmät palvelutuotannon toimintatavat. Viitekehyksen prosessit ja palvelut pyrkivät tukemaan tietoturvallisuutta. Yksi tärkeimmistä ja suurimmista prosesseista on tietoturvallisuuden johtaminen, jossa määritellään tietoturvallisuuden taso, missä taas pyritään ehkäisemään riskitilanteita ja korjataan jo aiheutuneita vahinkoja. ITIL pyrkii säännöllisesti tarkastamaan tietoturvallisuuden nykytilan ja raportoimaan siitä. Ko. periaatteissa ja linjauksissa ITIL ei eroa paljoa ISO 2700x -standardien vaatimuksista. (Haren 2007, 23–25.) Seuraavaksi esitellään ITIL:n tietoturvatoimenpiteet vaiheittain.



Kuvio 2. ITIL:iä noudattavat tietoturvatoimenpiteet (Laaksonen ym. 2006, 99)

GAISP (Generally Accepted Information Security Principles) esittää eri järjestelmäturvallisuuden periaatteita. Viitekehys on pääpainotteisesti tarkoitettu tietolähteeksi järjestelmien ja laitteiden valmistajille sekä käyttäjille. GAISP:n tavoitteena on yhdistää julkisen ja yksityisen sektorin tietoturvaperiaatteet koko maailmassa. (Laaksonen ym. 2006, 100.)

Tietoturvan standardit

ISO 2700x -standardit ovat oleellisimpia ja laajimmin levinneitä ympäri maailmaa. Nykyään puhutaan eniten yleisemmästä ISO 27001 -standardista, joka kattaa tietoturvajohtamis- ja hallintajärjestelmien perustamisen, toteuttamisen, käyttämisen, valvomisen, arvioimisen, huoltamisen ja parantamisen. Standardi auttaa suojaamaan kaikki tietoturva-asiat: tiedot, asiakirjat, koneet, verkot jne. ISO 27001 on perustettu kansainvälisessä standardointiorganisaatiossa, jota käytetään sertifioinnissa. ISO 27001 korvaa entisen BS 7799 -standardin ja sen monia ominaisuuksia hyödynnetään muiden standardien nojalla, kuten ISO/IEC 17799:2005, ISO 9001 yms. (Calder & Watkins 2012, 34–36.)

ISF (Information Security Forum) on kansainvälinen järjestö, joka on julkaissut Standard of Good Practice for Information Security -standardin. Standardin tehtävänä on auttaa käytännönläheisesti tiedonkäsittelyprosessien riskienhallintaa. Standardi on jaettu viiteen tärkeään osa-alueeseen, joista kukin osa-alue esittää siihen kuuluvia tietoturvaasioita: tietoturvallisuuden hallinta organisaatiotasolla, liiketoimintakriittiset järjestelmät, tietojärjestelmät, tietoverkot, järjestelmäkehitys. (Laaksonen ym. 2006, 100.)

Tietoturvatarkastuksen standardit

Alla tullaan esittämään standardeja, jotka kattavat tietoturvallisuuden hallintajärjestelmän vaatimukset, tietoturvahallinnan menettelytavat, sanaston ja määritelmät, laatujärjestelmät ja ympäristöasioiden hallinnan. Tarkastuksen standardeja noudattamalla voidaan olla varmoja siitä, että kaikki tärkeät asiat otetaan huomioon auditointia suorittaessa.

COSO riskinhallinnanmalli on tunnetuin sisäisen valvonnan viitekehyksistä. Mallissa on viisi komponenttia: valvontaympäristö, riskien arviointi, valvontatoiminnot, informaatio ja kommunikaatio, seuranta. Viimeisin päivitetty versio on julkaistu toukokuussa 2013, ja sen tarkoituksena on selkeyttää mallia (COSO 2013.)

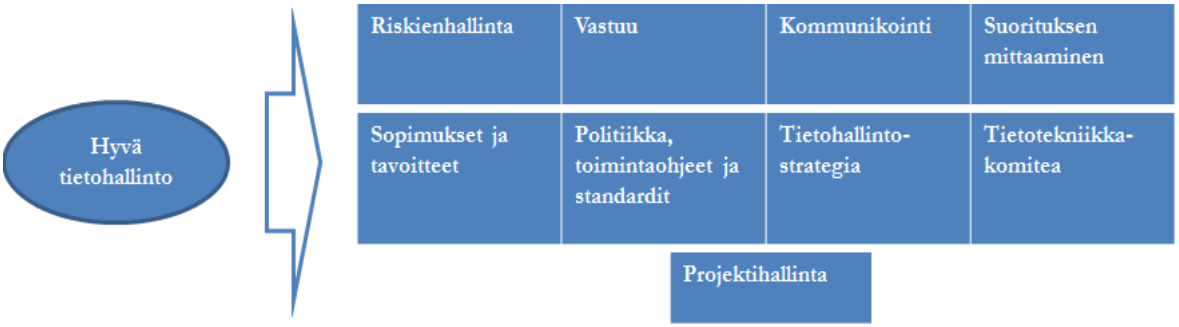
IIA (International Standards for the Professional Practice of Internal Auditing) on kansainvälinen ammattistandardien johdanto, jonka tarkoituksena on toteuttaa organisaation sisällä tapahtuvaa tarkastusta. Ammattistandardi kuvaa periaatteet, miksi sisäinen tarkastus tehdään, määrittää ajatusmallin tarkastettavien tehtävin suorittamiselle ja kehittämiselle, luo pohjan sisäisen tarkastuksen tuloksen arvioinnille, parantaa toiminnallisten prosessien kehittämistä ja avaa käsitteistöä (Sisäiset tarkastajat ry 2012, 28.)

2.1.6 Tietoturvan johtaminen ja hallinnointi organisaatiossa

Tällä, kuten usealla muullakin organisaation toiminta-alueella, onnistumisen lähtökohta on johdon sitoutuminen. Tietoturvallisuuteen ja sen politiikkaan liittyen tämä tarkoittaa johdon tahtotilan ilmaisemista tietoturvallisuuden toteuttamiseksi. Lisäksi johdon tulee

pystyä arvioimaan liiketoiminnan kehittyminen ja sen aiheuttamat tietoturvavaatimukset sekä huolehtia siitä, että resursseja on riittävästi hyvän tietoturvan takaamiseksi. Tietoturvavastaavan on raportoitava johdolle säännöllisesti tietoturvallisuuden tilasta, kehityksestä ja tietoturvavelvoitteiden toteuttamisesta. (VAHTI 2011, 11–14.)

Jotta hallinnointi olisi tarpeeksi hyvää, IT-taitoja ja tietoturvatietoja tulisi hyödyntää organisaatioissa monipuolisesti. Lisäksi hyvään hallinnointiin tarvitaan toiminnan järjestämistä, vastuun jakamista ja ratkaisujen tiedottamista eri tahoille. Seuraavassa kuvassa esitetty organisaation jokainen hallinta-alue pitää olla kytkettynä tietoturvatyöhön.



Kuvio 3. Hyvään tietohallintotapaan tarvittavat työkalut (Laaksonen ym. 2006, 124)

2.1.7 Tietoturvallisuuden hallinnan roolit ja vastuut

Tehokas tuloksellinen toiminta edellyttää vastuiden määrittämistä ja valvomista. Tietoturvan osalta tämä on tärkeä onnistumisen tekijä. Standardit ja normisto ovat joustavia tietoturva-organisaation rakenteen ja laajuuden suhteen. Käytännössä ko. asiat määräytyvät pitkälti organisaation tarpeiden ja tavoitteiden mukaan. Seuraavassa esitetään yleistason vaihtoehto keksikokoiselle organisaatiolle (Nurmi 2011, 32–34.)

Tietoturvaorganisaatio on ryhmä, joka on vastuussa mm. tietoturvan operatiivisesta toiminnasta ja joka yleensä laatii turvaohjeet muille liiketoimintayksiköille ja valvoo niiden noudattamista sekä raportoi omalle tai ylimmälle johdolle. **Johto** taas päättää, kuka kuuluu tietoturvaorganisaatioon ja mahdollistaa tarvittavat resurssit tehtävien suorittamista varten.

Tietoturvapäällikkö laatii yksikön johtajien kanssa toimintaohjeet, joita jokainen yksikkö noudattaa. Johdon tulee tiedottaa henkilöstölle tietoturva-asioista ja antaa myös heille mahdollisuuden osallistua niiden valmisteluun. Tällöin tietoturvapolitiikka toimii oikein ja asetetut tavoitteet ovat saavutettavissa.

Tietojen omistajat vastaavat tiedosta, sen laadusta ja käyttötavoista. Yleisesti tiedon omistaja on johtaja tai päällikkö tai muun vastaavan tason organisaation jäsen, vaikka hän ei välttämättä olekaan tiedon tuottaja. Tiedon omistaja kontrolloi, että tieto on luotettavaa ja päättää, kenellä on oikeus tarkastella ja muokata sitä. Tiedon omistajan on otettava huomioon lainsäädäntöön kuuluva mm. henkilötietolaki, laki yksityisyyden suojasta työelämässä ja tietosuojalaki, jotka määrittelevät kenellä on oikeus käsitellä arkaluonteista tietoa ja esimerkiksi tunnistamistietoja.

Jokaisella liiketoiminnan prosessilla on omistaja, joka vastaa kyseisestä prosessista sekä siitä, että siinä on huomioitu tietoturvallisuus. **Prosessin omistajien** tehtäviin tietoturvan osalta kuuluu mm. riskikartoitusten tekeminen, prosessin suojaustavasta päättäminen, tietoturvallisuuden ja liiketoiminnan tavoitteiden saavuttaminen, henkilöstön tietoturvan osaamisen varmistaminen ja ko. asioihin liittyen säännöllinen raportointi ja jatkuva seuranta.

Toimivan tietoturvan toimintaympäristön edellytyksenä on järjestelmän pääkäyttäjän valitseminen. **Järjestelmän pääkäyttäjä** vastaa systeemien ja sovellusten toimivuudesta ja siitä, että sen tuottama ja käyttämä tieto on varmasti luotettavaa. Pääkäyttäjä saa hallita sovelluksiin liittyviä tietoturvallisuuden käyttöoikeuksia, mutta ei saa päättää niistä. Käyttöoikeuksista voivat päättää vain järjestelmän, tiedon tai prosessin omistaja. Lisäksi järjestelmien pääkäyttäjät ovat vastuussa järjestelmien päivityksistä ja ylläpidosta. Laki yksityisyyden suojasta tulee ottaa huomioon tilanteissa, joissa käsitellään henkilötietoja, esim. sähköpostia. Järjestelmien pääkäyttäjät kuuluvat yleensä tietohallintoon.

Tietohallinnon tärkeimpiä tehtäviä on toteuttaa tietoturvallisuuden tekninen puoli ja ylläpito, mutta se ei saa päättää järjestelmien tai tietojen suojaustasosta. Siitä päättävät tiedon, prosessien ja järjestelmien omistajat. Tietohallinto yleensä vastaa myös mm.

laitetilojen suojaamisesta, tiedonsiirron turvallisuudesta, lokitiedostojen keräämisestä ja säilyttämisestä sekä kulunvalvonnasta ja operatiivisen toiminnon monitoroinnista. Lokitietojen avulla voidaan valvoa organisaation toimintaa ja raportoida siitä organisaation liikkeenjohdolle. Raportoinnissa tulisi ottaa huomioon tunnistamistietojen käsittelyä koskevat määräykset.

Sisäinen tarkastus pyrkii estämään toiminnan epäkohtia sekä turvaamaan toiminta-edellytyksiä. Varsinainen sisäisen tarkastuksen tehtävä on arvioida mm. tietoturvallisuuden tasoa ja tarkastella organisaation toimintaa tietoturvapolitiikkaan nojaten. Sisäinen tarkastus raportoi kaikki havaintonsa organisaation johdolle. Ulkoisen tarkastuksen päätehtävään kuuluu tilintarkastus eli organisaation tilinpäätöksen, kirjanpidon sekä yhtiön hallinnon tarkastaminen.

Henkilöstön tehtäviin kuuluu mm. tiedon käsittely, siirtäminen ja säilyttäminen tietoturvaohjeita noudattaen, sekä omien salasanojen hallinta ja turvallinen käyttö. Kunkin työntekijän tulee myös itse huolehtia omasta tietoisuudestaan liittyen tietoturvapolitiikkaan. Jotta tämä onnistuisi, tulisi työntekijän osallistua tietoturvallisuuskoulutuksiin.

Ulkoisilla sidosryhmillä on myös oma roolinsa organisaatiossa. Johtotaso tai tietoturvapäällikkö vastaa niistä, sillä hänen täytyy osata arvioida ulkopuolisten toimijoiden pätevyys ja työkokemus. Tärkeintä ulkopuolelta ostettavan palvelun tai toiminnon osalta on arvioida oikein tietoturvariskit ja ohjeistaa oman organisaation henkilöstöä. (Nurmi 2011, 14–16.)

2.1.8 Tietoturvallisuuden valvonta, seuranta ja mittaaminen

Tietoturvallisuus myös käsittää tärkeät tehtävät, kuten valvonnan, seurannan ja mittaamisen. Ilman niitä tietoturva ei ole jatkuvaa eikä kehittyvää. Tietoturvan *valvonnan* päätehtävänä on varmistua siitä, että tietoturvatyö toteutetaan tehokkaasti ja liittyvää ohjeistusta noudatetaan. Valvonta sisältää kaksi osaa: organisaation oman toiminnan valvonta ja ulkopuolisen toimintaympäristön valvonta. Valvontaa toteutetaan seuraamalla lokeja, raportteja ja tarkkailemalla prosesseja ja tilanteita. Tarkkailtavia sisäisen valvon-

nan osa-alueita ovat pääsynvalvonta, verkkoliikenteen valvonta, käytön valvonta, muutoshallinta ja järjestelmäkehitys. Ulkopuolisen toimintaympäristön tehtävien valvontaan kuuluu säädösympäristön tarkkailu. Tarkkailu voidaan toteuttaa esim. seuraamalla erilaisia julkisia tiedotteita, muutoksia ja uutisia lainsäädännössä ja standardeissa. Hyviä lähteitä ovat esim. viestintävirasto CERT (Computer Emergency Response Team), jolla on oma verkkosivu, jossa se listaa tietoja uusista uhista ja julkaisee ohjeet niiden ennaltaehkäisemisestä ja korjaamisesta. (Puhakainen 2010, 20.)

Kuvio 4. Viitekehys tietoturvallisuuden seurannasta ja valvonnasta (Laaksonen ym. 2006, 262)

Tietoturvan *seuranta* tarkoittaa toiminnan analysointia. Jotta tietoa voitaisiin analysoida ja toimintaa kehittää, tarvitaan oman organisaation, sen IT:n ja tietoturvauhkien tuntemusta. Seurannassa vertaillaan tällä hetkellä tapahtuvaa toimintaa ja asetettuja tavoitteita keskenään.

Taulukko 2. Tietoturvallisuuden auditoinnin ja seurannan vaiheistus. (Laaksonen ym. 2006, 266)

Vaihe 1	Vaihe 2	Vaihe 3	Vaihe 4
Tavoitteiden läpikäynti ja valvonnan kohteiden määrittely	Hallinnollisten toimien seuranta, toimintatapojen läpikäynti	Tekninen seuranta, ulkoinen ja sisäinen haavoittuvuustestaus	Kehitysehdotusten laatiminen ja toiminnan suuntaaminen

Tietoturvallisuuden *mittaamisessa* on tarkoitus tuottaa tietoa, joka auttaa toiminnan johtamisessa. Mittaamisella pyritään selvittämään kaikki organisaation mahdolliset puutteet

ja pyritään löytämään uusia kehitettäviä kohteita. Suojaustoimenpiteiden suunnittelu ja investointipäätösten tekeminen on johdettu tuotetusta informaatiosta. Ennen varsinaista mittaamista päätetään, mitä aletaan mitata ja miten se voi tehostaa toimintojen kehitystä ja tieturvallisuuden tasoa. Vasta tämän jälkeen voidaan aloittaa itse mittaus. (Laaksonen ym. 2006, 261–268.)

2.1.9 Tietoturvan nykytilan arviointiprosessi

Tämän luvun edellisissä alaluvuissa käsiteltiin organisaation tietoturvan merkittävimpiä osa-alueita. Seuraavassa esitetään, miten tietoturvatarkastusta valmistellaan ja suoritetaan, mitä ko. prosessi sisältää, sen eri vaiheita, suunnittelua, etenemistä, tietolähteitä, evidenssejä, tulosten käsittelyä yms.

- Alustava tutkimus: etukäteisaineiston hankinta (mm. julkinen tieto) ja siihen perehtyminen, alustava arviointisuunnitelma, tietolähteet, kriteerit, resurssit, riskit, rajoitukset, tarkastuskohteet, sisäinen hyväksyminen
- Aloituskeskustelu: suoritetaan kohteen johdon kanssa, huomioidaan sen toivomukset arviointisuunnitelmasta, -prosessista ja -tuloksista
- Kenttävaihe: kohteen tietolähteiden (sisäinen tieto) kerääminen, haastattelut, tutkinta ja analysointi, havaintojen dokumentointi, tarvittavissa kohdissa välitulokset ja -istunnot kohteen johdon kanssa, havaintojen vertailu tarkastuskriteereihin nähden, analysointi ja johtopäätökset
- Luovutettava dokumentaatio, luonnokset: liiketoiminnan jatkuvuuden suunnitelma, tietoturvan arviointiraportti, jossa mukana kehittämisehdotukset
- Loppukeskustelu: pidetään kohteen johdon kanssa, kerätään sen toivomukset ja odotukset mahdollista jatkoyhteistyötä varten
- Dokumentaation lopulliset versiot: laadinta ja toimittaminen kohteen johdolle, asiakastyytyväisyyskysely, tarvittaessa dokumentaation läpikäynti kohteen johdon ja henkilöstön kanssa, oman työsuorituksen sisäinen laatuarviointi
- Seurannan tai jatkoprojektin suunnitelman laatiminen ja toteutus
- Toimeksiannon sulkeminen.

Suunnittelu ja alustava tutkimus

Miettisen (2002, 26) mukaan suunnittelu on arviointiprosessin tärkeimpiä vaiheita. Kun tavoitteisiin ja työsuunnitelmaan ei ole paneuduttu tarpeeksi, se voi aiheuttaa epämääräisiä tuloksia ja arvioinnin onnistuminen on heikommin toteutettavissa. Jokainen tehtävä on erikseen suunniteltua, mikä tarkoittaa sitä, että jokainen tehtävä sisältää laajuuden, tavoitteen, ajoituksen ja käytettävät resurssit. Näin ollen sisäisen tarkastajan on otettava suunnittelussa huomioon seuraavat seikat:

- tutkittavan toiminnon tavoitteet ja valvonnan keinot
- toiminnot, niiden tavoitteet, resurssit ja toteuttamista uhkaavat riskit sekä keinot, joilla riskit saadaan minimoitua
- mahdollisuus toimintojen riskienhallinta- ja valvontajärjestelmien merkittävään parantamiseen.

Jotta tarkastaja saa alustavasta tutkimuksesta kattavan, informaatiota tulee kerätä paljon ja eri lähteistä. Lähteiden avulla saadaan kuva arviointikohteesta ja siihen liittyvistä uhista sekä voimassa olevista hallintamenettelyistä. Hyviä lähteitä ovat kaikki aiemmat raportit, sidosryhmät, Internet, kirjat, lehdet, johto ja muu henkilökunta. Kun käydään läpi strategioita, toimintasuunnitelmia ja -kertomuksia, raportteja, prosesseja yms., saadaan hyvä käsitys toiminnon kulusta.

Arviointisuunnitelman laadinta

Miettinen (2002, 36) kertoo, että arviointisuunnitelmaa laadittaessa sisäisen tarkastajan on mietittävä, miten voidaan tuoda lisäarvoa organisaatiolle ja parantaa sen toimintaa. Tarkastajan on mietittävä myös erikseen, miten hän voi tuoda lisäarvoa nimenomaan organisaation johdolle.

Tarkastuksen tavoitteet

Pickettin (2003, 56–58) mukaan ensiksi lähdetään selvittämään tavoitteita: mikä on tietoturvan nykytila, puutteet, ongelmat, muutostarpeet jne. Tavoitteet kertovat, mikä on tarkastajan päämäärä tutkimuksessa. Ne määrittävät tutkimuksen työn laajuuden. Tarkastuksessa on huomioitava myös mahdolliset riskit, jotka voivat haitata ja hidastaa tavoitteiden saavuttamista. Suunnitteluvaiheessa riskien arvioinnin tarkoituksena on tunnistaa tärkeitä toiminnan alueita, joita tulee tutkia mahdollisina tehtävän kohdealueina. Tavoitteissa siis kerrotaan, miksi arviointi ylipäätään suoritetaan ja mihin sillä pyritään, mitkä asiat halutaan varmistaa, mitkä toiminnot tarvitsevat kehittämistä ja näiden kysymysten avulla voidaan lähteä parantamaan koko organisaation toiminnallista ja taloudellista tulosta. Kun tarkastaja pohtii edellä mainittuja kysymyksiä eikä tiedä vastausta, tulee hänen kysyä asiaa johdolta. Johdon antamien vastausten perusteella tarkastaja tekee omat arviot ja johtopäätökset. Kun tarkastaja ja johto ovat päättäneet yhdessä arvioinnin sisällöstä ja arviointisuunnitelma on hyväksytty, voidaan aloittaa suunnitelman toteutus.

Tarkastuksen tietolähteet

Alustavan tutkimuksen kuvauksessa (ylempänä) mainittujen tietolähteiden lisäksi varsinaisesti käynnistyneessä tarkastuksessa tietolähteinä (evidensseinä) toimivat organisaation dokumentaatiot ja avainhenkilöiden mielipiteet ja vastaukset kysymyksiin haastatteluissa ja työpajoissa arviointiprosessin aikana. Seuraavassa taulukossa on kuvattu lyhyesti nämä tietolähteet ja niihin liittyvät esimerkkikysymykset (joita käytännössä voi olla kymmeniä tai jopa satoja, tarkastustapauksesta riippuen), joita esitetään avainhenkilöille haastatteluissa kenttävaiheessa. (Pickett 2003, 62–63.)

Taulukko 3. Tarkastuksen tietolähteet ja kysymykset. (Holopainen ym. 2006, 325)

Tietolähteet	**Kysymykset/Selvitykset**
Tietohallinnon strategiat, suunnitelmat ja budjetti	Onko tietohallinnon asema tavoitteisiin nähden kohdallaan? Ovatko resurssit oikein mitoitetut? Onko tietotekniikasta kilpailullista etua? Mikä on tietoturvan rooli organisaation strategiassa?
Tietoturvapolitiikka, ohjeet	Onko nämä laadittu? Onko johdon tuki apuna? Ovatko tietoturvaperiaatteet kohdallaan toimintaan, toimintaympäristöön ja riskeihin nähden? Minkä viestimien kautta henkilökunta saa informaatiota, onko näihin sitouduttu? Onko laadittu organisaatiokaaviot, työnkuvaukset, jotka kertovat raportointisuhteen, vastuun ja töiden jaon?
Johtoryhmien pöytäkirjat	Selviävätkö pöytäkirjoista uudet hankkeet ja projektit sekä resurssien suuntaaminen niihin?
Systeemikehitysten ohjeet	Millaiset vaatimukset on kyseessä systeemiprojekteissa, laadunvarmistuksessa ja dokumentaatiossa?
Operointiohjeet	Miten operointi on erotettu muista tehtävistä, mitkä ovat vastuut ja raportointisuhteet?
Henkilöstöperiaatteet	Miten henkilöstö hankitaan, irtisanotaan, sitoutetaan ja kehitetään?
Henkilöstön haastattelut; tietohallintohenkilöstö	Onko henkilöstön osaaminen ja tehtävien suorittaminen samalla tasalla? Tunteeko henkilöstö organisaation tavoitteet ja tietoturvatarpeet ja onko sitoutunut niihin?

Arviointiperusteet

Arviointiperusteet eli -kriteerit ovat ne dokumentit, joita vasten tehdään tarkastus. Toisin sanoen käytännössä niihin verrataan organisaation nykytilanne. Kriteereinä toimivat ulkoiset standardit, suositukset, kehikot ja parhaat käytännöt, joita ovat COBIT, ITIL, ISO/EIC, ISACA, VAHTI, SSE-CMM, IIA. Näistä on kerrottu ylempänä omissa kohdissaan. Sisäisiin kriteereihin kuuluvat johdon tavoitteet, arvot, strategia, tuloskortti, budjetit, hyväksytyt ohjeistukset ja suunnitelmat. (VAHTI 8/2006, 19–22.)

Tarkastuksen kohteet

Tarkastuksen kohteita ovat liike- ja IT-toiminta ja niiden tietoturva. Tietolähteiden avulla tunnistetaan seuraavat *liiketoiminnan* alueet ja pyritään arvioimaan niiden tietoturvatilanne: liiketoiminnan kriittiset alueet, tuotteet ja palvelut, toimittajat ja asiakkaat, organisaatiorakenne, toiminta- ja menettelytavat, tehtävät, tehtävien vastuut ja roolit, kehityshankkeet, investoinnit, laatujärjestelmät, valtuusmenetelmät, päätöksentekotavat ja -dokumentoinnit, valvontaperiaatteet ja järjestelyt, riittävyys suunnittelussa ja päätöksenteossa. Henkilöstön puolelta tunnistetaan ilmapiiri, motivaatioaste, alihankkijat ja toimittajat, konsultit, tuki, ylityö, kuormat ja riskit. (Pickett 2003, 121.)

Tietoturva-arvioinnin näkökulmasta tarkastellaan *IT*:tä (suhteessa liiketoimintaan), johon vaikuttaa tuloksellisuus, toiminnallinen ja taloudellinen tavoitteiden täyttyminen, strategianmukaisuus ja lainmukaisuus. Tarkastuksen kohteena ovat myös organisaation ja IT:n johtamistavat ja politiikka, jotka saadaan auki dokumentoinnista ja toteutuksen seurannasta, sekä seuraamalla prosessinomaisen lähestymistavan astetta. Hankkeiden ja hankintojen avulla voidaan kehittää IT:tä ja kokonaisarkkitehtuuria. Omaisuuden hallinta selviää siihen liittyvistä raporteista, mm. miten omaisuutta hankitaan ja poistetaan, kaikki siihen kuuluvat päätöksenteot ja prosessit. Tutkitaan myös IT-infraa ja ympäristöä eli kenen omistuksessa ja vastuulla se on.

Seuraavaksi on lueteltu yllä mainittujen huomioiden lisäksi muitakin IT:n kannalta tarkastettavia kohteita: organisaation toimittajien omat alihankkijat ja ympäristöt, dokumenttienhallinta, projektinhallinta, virhetilanteiden selvittely, varajärjestelmät, raportointi- ja päätöksentekotuen järjestelmät, laadunvarmistus, muutos- ja riskienhallinta, toipumiskyky, OLA, SLA yms. sopimukset. Operational Level Agreement (OLA) on hankintasopimus, jossa määritellään organisaation sisäosastojen väliset vastuut ja päätetään hyödykkeistä ja palveluista, jotka toimitetaan. Service Level Agreement (SLA) on palvelutasosopimus ulkoisen palveluntarjoajan ja organisaation välillä. Siinä käsitellään vastuita palveluiden tuottamisessa. (Holopainen ym. 2006, 346–348.)

Tarkastuksen osa-alueet

Pickett (2003, 145) kertoo, että johdon kanssa päätetään siitä, mitä seuraavista osa-alueista tullaan tarkastamaan tarkemmin vai tullaanko käsittelemään kaikki osa-alueet kokonaisvaltaisesti. Osa-alueita ovat: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laiteturvallisuus, ohjelmistoturvallisuus, tiedon ja datan turvallisuus, ulkoistamisen tietoturvallisuus. Eri toiminnoissa ja niiden vaikuttavuusalueilla näitä on joskus vaikea selkeästi rajoittaa toisistaan, joten tilanteesta ja kontekstista riippuen ne saattavat olla osittain päällekkäiset. Seuraavassa näitä jokaista esitetään hieman tarkemmin.

Hallinnolliseen tietoturvallisuuteen organisaatiossa kuuluvat lähinnä tietoturvapolitiikka ja ohjeistus, organisointi, seuranta, valvonta, raportointi ja kehitys. Ne kertovat samalla johdon asenteesta ja ne saadaan selville mm. tutkimalla organisaation kotisivut, vuosikertomukset yms. Ylimmän johdon hyväksymästä kirjallisesta dokumentista saadaan selville periaatteet, jotka kattavat mm. tietoturvan tavoitteet, soveltamisen, vastuut, valvonnan, voimaantulon, tiedottamisen sekä sitouttamisen. Käytön politiikka käsittelee salasanapolitiikkaa, sähköpostin käyttöä, kolmannen osapuolen pääsyä järjestelmiin, toimintaa Internetissä, sosiaalisessa mediassa, tukea, Help Desk - ja Service Desk -käyttöä. Lisäksi käyttövaltuuspolitiikassa ja -ohjeistuksissa käydään läpi prosesseja, nopeutta, poikkeuksia, tarkkuutta ja käyttäjäryhmiä. Niissä mainitaan mm. siitä, miten käyttöoikeuksia anotaan, kuka ne myöntää, mihin perustuen niitä myönnetään/evätään (säännöt) ja miten niitä voi itse (väärin)käyttää. Tiedon luokitteluohjeistuksessa käydään läpi, onko tieto julkista, sisäistä, luottamuksellista, salaista vai erittäin salaista. Lisäksi käsitellään tiedon kopiointia, hävittämistä, postittamista, säilyttämistä, verkossa siirtämistä yms. Tietoturvakoulutuksissa on esiinnyttävä jatkuvaa kehitystä, pelkästään Intrassa uuden tiedon julkaiseminen ei riitä, vaan koulutuksen täytyy tapahtua kädestä pitäen. (VAHTI, 2007–2013.)

Henkilöstö- ja fyysinen turvallisuus sisältää tietoturvatarkastuksessa arvioitavia osa-alueita:

- Henkilöstöturvallisuus: luotettavuusriskien hallinta, taustojen tarkistukset, sijaisuudet (oikeudet, osaaminen, tehtäväkierto), roolien ja käyttöoikeuksien märittelyt, valvonta
- Fyysinen turvallisuus: tilat, laitteet, ihmiset, varastointi, arkistointi, materiaalit

Tietoliikenneturvallisuus kattaa tarkastuksessa arvioitavia osa-alueita:

- Luottamuksellisuus: vain niihin oikeutettujen henkilöiden ja ryhmien saatavissa, ei paljasteta sivullisten käyttöön
- Eheys: ei muuttunut laitteisto- ja ohjelmistovikojen tai luonnontapahtumien tai oikeudettoman inhimillistoiminnan seurauksena, saatavuus, niihin oikeutettujen henkilöiden estettä hyödynnettävissä hyväksyttävällä vasteajalla
- Kiistämättömyys: vastaanottaja ei voi kiistää saaneensa sitä
- Verkot: vastuut, palomuurit, protokollat, pääsyt, liittymät, tiedonsiirto

Laite- ja ohjelmistoturvallisuus sisältää tietoturvatarkastuksessa arvioitavia osa-alueita:

- Laiteturvallisuus: pääsyvalvonta, saatavuuden toimenpiteet (alihankkijat), kahdennukset kuormajako, sovellus- ja ohjelmistoturvallisuus, tunnistaminen, pääsyvalvonta, käyttöoikeudet, vaaralliset työyhdistelmät, administrator-tason käyttäjien mahdollisuus muuttaa liiketapahtumia tuotannossa, tarkkailu, lokimenettelyt, päivitykset, virustorjunta, kontrollien toimivuus: yleiset ja sovelluksen omat lisenssit, tekijänoikeudet, sopimukset
- Sekä laitteiden että ohjelmistojen osalta: prosessit, konfiguraatio- ja muutoshallinta, automaattinen valvonta ja inventointi, testaukset, katselmoinnit, tuotantoonsiirrot, versionhallinta, ympäristöt (tuotanto, kehitys, testi)

Tiedon ja datan turvallisuus: pääsyt, suojaus - salakirjoitus säilytettäessä ja siirrettäessä, saatavuus, käytettävyys, oikeellisuus, luottamuksellisuus, salassa pitäminen, turvalli-

nen käsittely, talletusmuodot ja -mediat, elinkaaren hallinta, epäselvyyksien selvittely ja dokumentointi, muutosten jäljittäminen ja palauttaminen, omistajuudet, vastuut ja roolit (myös kirjallisesti), yhdenmukaiset periaatteet (prosessit)

- Pääkäyttäjät: admin-pääsyt, jäljittäminen, raakadata ja DB
- Varmistukset (backup): säilytysajat ja -tilat, palautettavuus ja sen testaaminen ja nopeus, kirjallinen suunnitelma ja päiväkirja (Nurmi 2011, 46.).

Kenttävaihe

Nurmen (2011, 54) mukaan kenttävaiheeksi kutsutaan vaihetta, jossa tutkitaan ja arvioidaan tietoa. Kenttävaiheeseen sisältyy neljä eri vaihetta: informaation hankkiminen, haastattelut, tutkinta, analysointi ja arviointi, havaintojen vertailu tarkastuskriteereihin, dokumentointi ja työn valvonta.

Kun tarkastaja hankkii tietoa, on tärkeää muistaa, että tiedon pitäisi sisältää riittävästi informaatiota, olla laadukasta, olennaista ja hyödyllistä. Tieto ei voi olla vain kuultua jostain, sen täytyy olla todistettua faktaa. On olemassa useita tarkastuslistoja ja mm. COSO:n ja VAHTI:n toteamuksia, jotka helpottavat tiedon arviointia. Tarkastaja valmistelee selkeästi ja tarkasti kaikki dokumentoitavat havainnot, jotka tarkastuksen johtaja sitten arvioi. Dokumentaatiossa tulisi olla selvillä, mitä ja miten tehtäviä on tehty ja miten ne on todistettu. Jokainen arviointi ja analyysi pitää merkitä yhteenvetolomakkeeseen. Lomake helpottaa laadunvarmistajaa arvioimisessa, sillä siitä näkee heti, miten työ on suoritettu ja mitä asioita on tutkittu. Kaikissa työpapereissa tulisi olla mainittuna arvioijan nimi ja päiväys arvioinnin suorituspäivästä. (Holopainen ym. 2006, 201–203.)

Tarkastusraportti, rakenne ja sisältö

Tarkastusraportilla voi olla suuri vaikutus organisaation tietoturvan ja sitä kautta koko toiminnan kehitykseen, sillä sen suositusten pohjalta yleensä lähdetään toteuttamaan muutosta, joka tuo organisaatiolle ja sen sidosryhmille lisäarvoa ja hyötyä. Arvioinnin lopputulokseen vaikuttaa raportin ulkonäkö, sisältö, rakenne ja jäsentely. Hyvään ra-

kenteeseen sisältyy kansilehti, sisällysluettelo, yhteenveto johdolle ja yksityiskohtaiset havainnot. Kansilehti kuvastaa ammattimaista työtä ja tekijää. Sisällysluettelosta pääsee helposti seuraamaan työn sisältöä ja lukemaan kohtaa, joka lukijaa kiinnostaa. Yhteenvedossa johdolle käy ilmi noin viisi päähavaintoa, joihin liitetään syyt, seuraukset ja suositukset. Johdon tulisi saada lukea raportista myös ne tehtävät, jotka eivät ole toteutuneet ja joilla on vaikutusta lopputulokseen. Yksityiskohtaiset havainnot jaetaan sellaisten otsikoiden alle, kuten raportin tausta, arviointiperusteet, havainnot, menettelytapa ja syy, seuraukset/riskit/mahdollisuudet, kehitysodotukset, johdon toimenpidesuunnitelma ja seuranta. (Holopainen ym. 2006, 220–222.)

Loppukeskustelu ja lopullinen arviointiraportti

Kun tarkastus on valmis, käydään raportti läpi organisaation johdon kanssa. Tarkastaja kertoo omat havainnot ja suositukset. Keskustelu käydään läpi tarkastajan asioiden ymmärtämisen varmistamiseksi. Keskusteluun voi osallistua muutakin henkilökuntaa. Kaikki esimiehen erimielisyydet raportista tulee kirjata ylös. Kun edellinen on hoidettu kuntoon, valmis raportti toimitetaan organisaation johdolle asiakastyytyväisyyskyselyn kanssa ja saatu palaute sisällytetään vielä lopulliseen raporttiin. Lopuksi tarkastaja ja johtaja käyvät läpi seuraavia asioita: tehtiinkö arviointi tavoitteen ja laajuuden mukaisesti, tuotettiinko lisäarvoa, noudatettiinko kaikkia standardeja oikein, onko tarkastus tehty ohjeiden mukaan, millaisesta budjetista on kyse. Lisäksi tarkastellaan, mikä meni hyvin ja mikä ei, mitä on opittu ja onko mitään parannettavaa seuraavaa arviointia ajatellen. Näiden asioiden pohtimisen jälkeen arviointi voidaan sulkea ja aineisto arkistoida. (Holopainen ym. 2006, 186–187.)

2.2 Liiketoiminnan jatkuvuus ja sen suunnittelu

Edellisessä alaluvussa käsiteltiin tietotoruvaa ja sen tarkastusta teorian ja kirjallisuuden valossa ensimmäisenä osana tietoperustaa. Sen toinen osa eli seuraava alaluku tarkastelee liiketoiminnan jatkuvuutta ja sen suunnittelua.

2.2.1 Jatkuvuussuunnittelun termistö

Liiketoiminnan jatkuvuussuunnitelma on kokonainen prosessi, joka on laadittu organisaation liiketoimintaprosessien turvaamiseksi. Ko. käsitteisiin kuuluvat mm. varautuminen, jatkuvuus, toipuminen, valmiussuunnittelu. Näitä termejä ymmärretään eri tavalla eikä niitä aina osata käyttää oikein. Erot näkyvät esim. julkishallinnon ja yksityissektorin välillä sekä varautumisen ja varautumissuunnittelun välillä. Turvaaminen tapahtuu sekä normaalitilanteissa että häiriötilanteissa. Tärkeintä on osata erottaa toisistaan nämä tilanteet sekä niiden rinnalle kuuluvat poikkeusolot. Häiriötilanteita ovat esim. tietojärjestelmän virhe, väärinkäytös, katkos, tulipalo yms. Kun jokin ongelmatilanne tapahtuu, käytössä on varautumissuunnitelma ja valmiussuunnitelma. Kunkin olosuhteen mukaan valitaan oikea suunnitelma. (Laaksonen ym. 2006, 225.) Seuraava kuva esittää ko. käsitteiden loogiset alueet liittyen tilanteisiin tai oloihin (alimmainen rivi).

Kuvio 6. Jatkuvuussuunnitelman tietoturvasuunnittelu (Alppisara 2012)

Tässä tutkimuksessa keskitytään nimenomaan toiminnan jatkuvuussuunnitteluun, koska se kattaa tärkeimmät ja todennäköisimmät tilanteet ja olot. Jatkuvuuden käsite kuuluu myös tietoturvallisuuden, toiminnan laadunvarmistamisen ja organisaatioiden riskienhallinnan osaksi. Valtionhallinnon tietoturvakäsitteistö päättää sen, miten tietojenkäsittely ja tiedonsiirto on turvattava häiriöiden aikana ja niiden jälkeen. Kun suunnitellaan jatkuvuutta, seuraavat asiat on otettava huomion: organisaation sijainti, ympäristö, toiminnan luonne ja laajuus. Tiedon kannalta mietittäviä asioita ovat: miten tietoa siirretään, muutetaan ja hävitetään. (Laaksonen ym. 2006, 227.)

2.2.2 Jatkuvuussuunnitelman tavoitteet ja hyödyt

Niin kuin ylempänä jo mainittiin, jatkuvuussuunnitelman tavoitteeksi on määritelty liiketoiminnan turvaaminen ja negatiivisten vaikutusten vähentäminen. Ennen jatkuvuussuunnitelman tekoa kannattaa miettiä, mitä sillä halutaan saavuttaa. Jatkuvuussuunnitelma kannattaa tehdä vain silloin, kun siitä saadaan liiketoiminnallista hyötyä. Kun se on ajan tasalla, toiminta on tehostettua ja säästyy resursseja. Hyvä ja ajan tasalla oleva dokumentaatio vaikuttaa myös positiivisesti jatkuvuussuunnitelmaan, konfiguraatio- ja muutostenhallintaan. (Iivari & Laaksonen 2009, 27–28.)

2.2.3 Jatkuvuussuunnittelun standardit ja vastuut

Jatkuvuussuunnitelma laaditaan organisaation tarpeiden ja erityispiirteiden mukaan. Siinä hyvänä pohjana on standardi ISO 27031, ISO 27005, VAHTI-suositukset, NIST 800. Liiketoiminnan jatkuvuuden suunnittelun, toteutuksen ja kehittämisen vastuut ovat tietoturvaorganisaatiolla, koska jatkuvuus on osa tietoturvaa. Liiketoiminnan jatkuvuuden organisointi ja vastuuttaminen vastaavat yleensä pitkälti tai kokonaan tietoturvan organisaatiota ja vastuita, joita on käsitelty edellisessä tietoperustan alaluvussa.

2.2.4 Jatkuvuussuunnitelman laatimisen vaiheet

VAHTI (2010) sanoo, että on tärkeää laatia organisaatiokohtainen malli, jonka mukaan jatkuvuussuunnitelma toteutetaan ja kehitetään. Ensiksi suunnitellaan tavoitteet, osallistujat, ohjeistus, jaetaan vastuut, minkä jälkeen pyritään tunnistamaan suojattavat kohteet sekä prosessit, apuvälineet ja mallit, joilla ko. kohteita suojataan. Suojattava kohde on mikä tahansa asia, joka on organisaatiolle arvokas. Kun tapa ja osallistujat on valittu, aletaan toteuttaa riskienhallintastrategiaa, jonka tarkoituksena on arvioida riskit ja pienentää tai torjua ne kokonaan. Keskeinen osa jatkuvuudenhallintaa on riskien hallintatyö. Kun kaikki riskit on tunnistettu ja arvioitu, suunnitellaan toimenpiteet, joiden avulla ko. riskejä minimoidaan ja eliminoidaan, sekä toimitaan tilanteissa, joissa ko. riskit toteutuvat. Kyseessä on silloin toipumissuunnittelu, joka on osa jatkuvuussuunnittelua (mikä näkyy ylempänä kuviossa 6). Liiketoiminnan jatkuvuussuunnitelma sisältää

joukon työkaluja, joita ovat mm. lomakkeet, listat, taulukot yms., joissa kerrotaan kaikki tarvittavat tiedot, kuvaukset, toimet, toiminnot ja toipumiskäsittelyt. Liiketoiminnan jatkuvuussuunnitelman laadinnan jälkeen se auditoidaan (esim. sisäisesti), päivitetään ja testataan. (Laaksonen ym. 2006, 231.)

2.2.5 Jatkuvuussuunnitelman testaus

Laaksonen ym. kertovat, että (2006, 231–232.) jatkuvuussuunnitelmasta ei ole mitään hyötyä, jos sitä ei testata. Testaus on välttämätön osa kehitystä, koska testaamisella saadaan selville, onko kaikki asiat ja riskit huomioitu ja ajan tasalla. Tarkoituksena on olla varmoja siitä, että suunnitelma toimii mahdollisten ongelmien sattuessa. Testauksesta käy ilmi suunnitelman sisältö, kaikki suunnitelmaan kuuluvat henkilöt, heidän vastuut ja roolit liiketoiminnan ja tietoturvallisuuden turvaamisessa. Testauksella kannattaa olla oma aikataulu, johon merkitään suoritettavien testien määrä, tyyppi ja ajankohta. Testaus kannattaa tehdä vähintään joka vuosi ja aina silloin, kun organisaatiossa tapahtuu muutoksia, esim. henkilöstö- ja tietomuutos, järjestelmien ja ohjelmien päivitys, laitteiden isommat hankinnat, lainsäädäntö-, prosessi-, sijainti- yms. muutos. Testaustapoja on useita organisaation tarkoituksesta, päämääristä ja tilanteesta riippuen. Yleisimpiä ovat toiminta- ja pöytätestaus. Ensimmäisessä testaus suoritetaan toteuttamalla suunnitelman toimenpiteet mahdollisimman lähelle niiden kuvauksia. Toisessa suunnitelman askelia käydään läpi puhumalla ja kommunikoimalla työpajoissa.

3 Tulokset: toteutus, empiria

Tämä luku esittää tutkimuksen *Tulokset*-osuutta, jolloin sen kaksi alalukua vastaavat tutkimuskysymysten alakysymyksiin ja tavoitteisiin *empirian* eli *toteutuksen* osalta. Ensimmäinen alaluku käsittelee K1-tutkimuskysymystä ja siinä esitetään organisaation *Tietoturvatarkastuksen raportin* esimerkki eli pohja/malli. Se on käytännön toteutus siitä, mitä käsiteltiin K1:een liittyen *Tietoperusta*-osuudessa edellisluvussa. Näin malliraportti pohjautuu normistoon, standardeihin ja parhaisiin käytäntöihin. Ko. pohja esittää oikeanlaista raportin rakennetta, sisältöä ja muotoa. Kuten tietoperustassa mainittiin, raportti sisältää kaksi tärkeintä osaa: *Johdon yhteenveto* ja *Kehityskohteet*, kun taas tässä toteutusta-

pauksessa ko. kehityskohteita on vain yksi (mikä riittää esimerkin antamiseksi). Tärkeimmät loogiset kohdat ja kokonaisuudet on korostettu *kursivoidulla* tekstillä.

Toinen alaluku jatkaa empiriaosuutta K2-tutkimuskysymyksen osalta ja siinä esitellään organisaation *Liiketoiminnan jatkuvuussuunnitelman* esimerkki eli malli. Se esittää mm. suunnitelman rakenteen, pääosat, sisällöt ja työkalut. Tässäkin tapauksessa ko. malli pohjautuu siihen, mitä käsiteltiin K1:een liittyen *Tietoperusta*-osuudessa edellisluvussa.

Seuraavissa alaluvuissa vastaavasti olevat *Tietoturvatarkastuksen raportti* ja *Liiketoiminnan jatkuvuussuunnitelma* ovat käytännössä itsenäisiä dokumentteja ja ne on esitetty sellaisinaan. Pienenä poikkeuksena on se, että tässä ne eivät sisällä omassa formaatissaan omia kansilehtiään (selkeyden vuoksi), eivätkä sisällysluetteloa (se on näkyvissä tutkimuksen sisällysluettelossa omina osina tässä luvussa).

Aivan luvun aluksi esitetään lyhyesti kohdeorganisaatio ja sen toiminta.

Tietoa Kohdeorganisaatiosta

Aalto, PAVE on säätiö, jonka pääasiallisena päämääränä, tavoitteena ja työtehtävänä on tarjota asiakkailleen (yliopistot, AMK:t tms.) kysynnän mukaan taloushallinnon palveluita, mukaan lukien mm. palkanlaskenta ja palkanmaksu, palvelusuhdeasiat, osallistuminen tekniseen rekrytoimiseen, vuosiloma- ja poissaolotietojen ylläpito sekä sähköisten arkistointien, tilastointien ja raporttien hoito. Näihin asioihin liittyen tuotetaan pääkäyttäjäpalveluja sekä erilaisia asiantuntijapalveluja. Asiakkuus alkaa asiakasprojektilla, jonka palvelukeskus toteuttaa yhdessä Kohdeorganisaation kanssa. PAVE:ssa toimii yli 40 ammattilaista viidessä eri tiimissä.

3.1 Organisaation tietoturvan tarkastusraportti (malli)

3.1.1 Johdon yhteenveto

Tietoturvan arvioinnin suorituksen *syynä* oli Kohdeorganisaation johdon tilaus/toimeksianto. Arvioinnin kohteena oli Kohdeorganisaation ja sen palveluntoimitta-

jien liiketoiminnan, prosessien ja käytäntöjen tietoturva. *Tavoitteena* oli varmistua siitä, että Kohdeorganisaation tietoturva on hyvällä toimintatasolla, pystyy tukemaan organisaation liiketoiminnan jatkuvuutta ja vastaa tietoturvallisuuden parhaiden käytäntöjen ja tärkeimpien standardien vaatimuksia. *Arviointiperusteina* on käytetty ISO/IEC 2700x, 17799, Cobit, ITIL, Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ja JHS -suosituksia.

Menetelminä oli lähestymistapa, jossa organisaation ja sen IT-palveluntoimittajien dokumenteista, selvittelyissä ja haastatteluissa kerättiin tiedot sekä keskeisten henkilöiden kokemukset ja näkemykset Kohdeorganisaation tietoturvan ja liiketoiminnan jatkuvuuden tilasta, haasteista, tarpeista ja toiveista.

Arviointilaajuus kattoi Kohdeorganisaation ja sen IT-palveluntoimittajien tietoturvan kaikki perusalueet: Hallinnollinen ja Fyysinen turvallisuus, Henkilöstö-, Tietoliikenne-, Laitteisto-, Ohjelmisto-, Tietoaineisto- ja Käyttöturvallisuus. Tarkastuksen tilaajan pyynnöstä enemmän huomiota oli kiinnitetty seuraaviin alueisiin: Jatkuvuussuunnittelu, Valmiussuunnittelu, Ulkoistamisen tietoturvallisuus. Samasta syystä *tarkastuksen ulkopuolelle* kokonaan tai osittain jäivät konesalien käynnit, IT-infran, laitteistojen, verkkojen, sovellusten testaukset ja tarkastukset, projektihallinta, taloudelliset näkökulmat, tietojärjestelmien rakentaminen ja hankinnat.

Arvioinnin *suorittajana* toimi projektityöntekijä Leena Satakieli pp.kk.vvvv - pp.kk.vvvv. Tarkastus ja raportti on suoritettu sisäisen tarkastuksen *ammattistandardien* mukaisesti (IIA:n standardi 2340). Arvioinnista ei aiheutunut erillis*kuluja*. *Edellistä* vastaavaa arviointia tietojemme mukaan ei ole suoritettu ainakaan viime vuosien aikana. Arvioinnissa saatuja tietoja ja *suosituksia* on tarkoitus käyttää Kohdeorganisaation ja sen palvelutoimittajien ja asiakkaiden toiminnoissa.

Yleisarvio

Kokonaisarviona Kohdeorganisaation ja sen palvelutoimittajien tietoturvan tilasta voidaan suoritetun arvioinnin otantojen perusteella todeta, että tietoturvaa hoidetaan hy-

vin. Prosessien sisäinen valvonta on tyydyttävällä tasolla. Riskienhallinta ja corporate governance ovat nekin tyydyttävällä tasolla.

Pääasialliset havainnot ja suositukset (esimerkki)

Havainnot ja niistä seuraavat suositukset oli tehty sen *perusteella*, että tarkastuksen aikana pitämissä haastatteluissa vastaukset kysymyksiin oli kielteisiä, epävarmoja, epämääräisiä tai niitä ei pystytty vahvistamaan dokumentaatiolla. Siitä johtuen jotkut havainnoissa mainitut asiat ehkä ovatkin olemassa/käytössä, mutta joko kehitysvaiheessa tai vaativat parannusta.

Tarkastuksen tavoitteet saavutettiin. Saatiin varmistus siitä, että Kohdeorganisaation tietoturva on pääasiassa hyvällä toimintatasolla ja pystyy tukemaan organisaation liiketoiminnan jatkuvuutta. Samalla todettakoon, että toiminnoissa ja käytänteissä on parantamisvaraa, jolloin parhaiden käytäntöjen ja tärkeimpien tietoturva- ja niihin liittyvien standardien vaatimusten huomioiminen ja toteuttaminen käytännössä edistää organisaation tietoturvan ja koko toiminnan tason kohottamista.

Pääasialliset kehitysesitykset kohdistuivat Kohdeorganisaation toiminnan seuraavassa esittämiin kohtiin (alempana on kerrottu omissa osioissaan jokaisesta kohdasta tarkemmin). Siinä tapauksessa, *jos ko. havaintoihin ei reagoida*, *riskeinä* ovat mm. Kohdeorganisaation imagon ja tuloksen heikkeneminen.

- **Kehityskohde A**: Kohdeorganisaation ja sen palveluntoimittajien tietoturva(järjestelmä), siihen liittyvä ohjaus ja toiminnot vaativat tarkempaa järjestämistä, dokumentointia ja tehostamista sekä systemaattisempaa lähestymistapaa. Myös riskienhallintaa omana prosessina ei toteuteta, dokumentoida, kehitetä eikä valvota Kohdeorganisaation omissa eikä palveluntarjoajien toiminnoissa. Suosittelemme tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista ja käyttämistä. Sen osana muodostetaan riskienhallinta sekä omassa toiminnassa että palvelujen toimittajien kontrollien osalta.

- **Kehityskohde B**

  <<ko. teksti tähän>>
- **Kehityskohde C**

  <<ko. teksti tähän>>

Raporttiluonnos ja yksityiskohtaiset *havainnot on käyty läpi* Kohdeorganisaation johdon kanssa pp.kk.vvvv. Johtaja on pp.kk.vvvv antanut johdon toimenpidesuunnitelman suositusten toimeenpanosta ja ne on kirjattu raportin *Kehityskohteet* -osassa (seuraavassa) kunkin havainnon lopussa olevan kehitysehdotuksen perään.

3.1.2 Kehityskohteet

KEHITYSKOHDE A: TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ

Arviointiperusteet

ISO/IEC 27001, 4.1 Tietoturvallisuuden hallintajärjestelmä. Yleiset vaatimukset
Organisaation tulee luoda, toteuttaa, käyttää, valvoa, katselmoida, ylläpitää ja jatkuvasti kehittää dokumentoitua tietoturvallisuuden hallintajärjestelmää, joka tukee organisaation liiketoimintoja ja organisaatioon kohdistuvia riskejä.

Johdon tietoturvaopas, 2.2011, Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI), 2 Organisaation johdon keskeiset tietoturvavelvoitteet
Organisaatioiden johto on keskeisessä asemassa tietoturvallisuuden ylläpitämisessä ja kehittämisessä. Tietoturvatyölle tulee nimetä vastuuhenkilö, esim. tietoturvapäällikkö sekä osoittaa hänelle riittävät resurssit hoitaa ja toteuttaa organisaation tietoturvavelvoitteita organisaation toimintaympäristön ja ulkoisten vaatimusten edellyttämällä tavalla. Tietoturvallisuus tulee organisoida ja vastuuttaa erityisesti riskienhallintatoimessa, tietohallintotoimessa, sopimus- ja hankintatoimessa sekä lainmukaisuuden valvonnassa. ... Tietoturvallisuutta voidaan hallita hallintajärjestelmällä, jossa määritetään keskeiset tietoturvavastuut, riskienhallintamenettelyt sekä kehitys-, seuranta- ja raportointiprosessit. Hal-

lintajärjestelmä voidaan toteuttaa osaksi organisaation vallitsevia toiminnan suunnittelu- ja seurantamekanismeja, esimerkiksi laatuohjelmaa.

Havainnot, syyt ja seuraukset (= riskit ja mahdollisuudet)

Organisaation ja sen palveluntoimittajien tietoturva on *kokonaisuudessaan* hyvällä tasolla. Sen kuntoa ja sisältöä *tarkemmin tarkastettua* kävi ilmi, että siihen liittyvä ohjaus ja toiminnot vaativat tarkempaa järjestämistä, dokumentointia ja tehostamista sekä systemaattisempaa lähestymistapaa. Myös saatujen tietojen mukaan riskienhallinta omana prosessina vaatii tarkempaa ja systemaattisempaa toteuttamista, dokumentoimista, kehittämistä ja valvomista Organisaation oman ja palveluntarjoajien toiminnoissa.

Perimmäisenä syynä tähän on se, että Organisaatio on sen kokoinen, että siinä ei välttämättä ehdi huomata kasvavia tietoturvaohjaustarpeita. Riskienhallinnan tärkeyttä ei ehditä jäsentelemään omaksi toiminnaksi tai siihen ei nähdä tarvetta.

Tietoturvajärjestelmän osalta *nykyinen toimintatapa* ei ole huono, vaikka ei myöskään välttämättä edesauta tietoturvan tehokasta hallintaa. Riskienhallintatyön ja sen parantamisen osalta on *suositus* käyttää pikaisia toimenpiteitä. Asioiden kehittäminen suositusten (alla) mukaan auttaisi Organisaatiota saamaan positiivisempaa mainetta ja parantamaan entisestään omaa imagoa palveluntarjoajana asiakkaiden ja muiden sidosryhmien silmissä. Toteutettuna yhteistyössä palveluntoimittajien kanssa, tämä parhaimmillaan vahvistaisi Organisaation tietoturvaa ja riskienhallintaa, parantaisi sen sisäisten ja kumppanitoimintojen turvallisuutta, yleislaatua ja sitä kautta vaikuttaisi tulokseen. Sen sijaan *asian jättäminen ennalleen* saattaa aiheuttaa päinvastaisia seurauksia, mikä voi ilmetä muun muassa riskeinä liiketoiminnalle.

Organisaation johto on kyllä huomannut tietoturvan kehitystarpeet, minkä tuloksena ovat mm. tämän tietoturvatarkastuksen ja liiketoiminnan jatkuvuuden suunnitelman tarpeiden esille tuominen ja ko. toimeksiannon antaminen tämän työn tekijälle.

Kehitysehdotukset

Sen varmistamiseksi, että yllä mainitut riskit eivät toteutuisi, työn tekijä suosittelee tietoturvallisuuden hallintajärjestelmän tehostamista ja käyttämistä, valvomista ja katselmointia, ylläpitämistä sekä jatkokehittämistä. Sen osana vahvistetaan riskienhallintaa sekä omassa toiminnassa että palvelujen toimittajien kontrollien osalta.

Käytännön toteutuksen voi suorittaa omana erillisenä projektina tai hyödyntäen tietoturvatarkastuksen yhteydessä projektityöntekijän toimesta luotua liiketoiminnan jatkuvuuden suunnitelmaa. Suunnitelma pitkälti kattaisi tietoturvallisuuden hallintajärjestelmän, koska sisältäisi suurimman osan sen standardien vaatimia osa-alueita (tietoturvapolitiikka, -organisaatio, -resurssit, roolit ja vastuut, riskienhallinta ja -hyväksymiskriteerit, katselmukset, koulutukset, jatkokehitys jne.)

Johdon toimenpidesuunnitelmat

ja vastuuhenkilön nimi sekä tavoitteellinen toteutuspäivä

<<ko. teksti tähän>>

Johdon selvitys kehitysehdotusten toteutuksesta

<<ko. teksti tähän>>

Tarkastajan arvio kehitysehdotusten toteutuksesta

<<ko. teksti tähän>>

KEHITYSKOHDE B: XX

<<ko. teksti tähän>>

KEHITYSKOHDE C: YY

<<ko. teksti tähän>>

3.2 Organisaation liiketoiminnan jatkuvuuden suunnitelma (malli)

3.2.1 Dokumentin tarkoitus ja rakenne

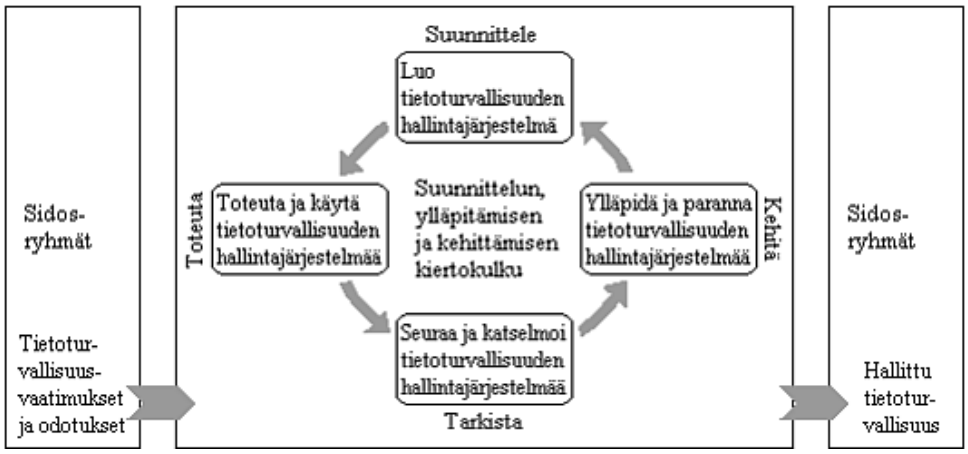
Tämä dokumentti on [Organisaatio/Oy]:n liiketoiminnan jatkuvuussuunnitelma. Suunnitelma esittää tarkoituksenmukaista etenemistapaa osoittamalla oikeassa järjestyksessä suoritettavia toimenpiteitä, joita kuvaavat suunnitelman luvut ja kohdat. Kohdat sisältävät viittauksia organisaation tietoturvan ja siihen liittyvän toiminnan dokumentteihin ja kokonaisuuksiin. Näin suunnitelma toimii myös eräänlaisena Kohdeorganisaation tietoturvan metahakemistona ja systematisoituna linkistönä. Tällöin sitä on tärkeää pitää ajan tasalla myös. ko. alueen osalta, mistä vastaa tietoturvapäällikkö.

Suunnitelman ensimmäisissä luvuissa kuvataan tietoturvapolitiikka, tietoturvaorganisaatio, siihen liittyvät roolit ja vastuut. Seuraavaksi esitetään suojattavat kohteet, minkä jälkeen siirrytään riskienhallinnan käsittelyyn. Sen tärkeimpiä osioita on toipumisen suunnittelu, jota esittää toipumissuunnitelma ns. perusriskien toteutuessa. Seuraavat luvut kuvaavat tietoturvan ja jatkuvuuden koulutusta, jatkuvuussuunnitelman testausta, ylläpitoa ja päivitystä, seurantaa ja raportointia sekä myös suunnitelman jakelua ja säilytystä. Dokumentin tärkeä osa on liitteet, jotka käytännössä sisältävät keskitetyt ja systematisoidut tiedot ja listat ("mitä") kaikista niistä asioista, joista suunnitelma kertoo kussakin luvussaan ("miten"). Näin tämän dokumentin tekstiosuus toimii Kohdeorganisaation tietoturvan kuvauksena ja step-by-step -toimintaohjeena, kun taas liitteet ko. vaiheiden toteutustyökaluina.

3.2.2 Tietoturvapolitiikka, turvallisuuden ja jatkuvuuden hallinnan prosessi

<< Jatkuvuudenhallinta on sidoksissa organisaation strategiaan ja pohjautuu liiketoiminnan ja johtamisen tarpeisiin. Prosessin kattavuuden määrittely kuuluu johdolle. Kuvataan politiikka liiketoiminnan ja IT:n vaatimusten mukaan. >>

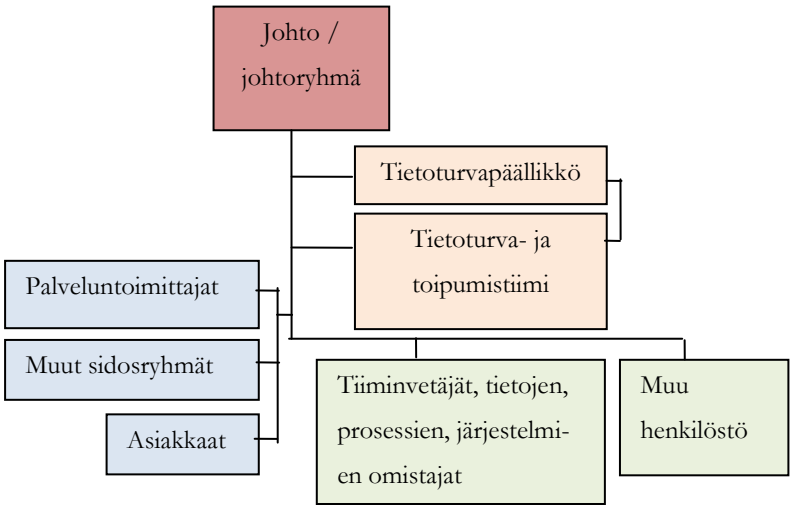
Kohdeorganisaatiossa tietoturvaa ja liiketoiminnan jatkuvuutta hallinnoidaan jatkuvana prosessina, jota esittävät seuraavassa kuvassa PDCA-mallin (plan–do–check–act) mukaiset työvaiheet:



Kuvio 7. PDCA-mallin mukaiset työohjeet (ASQ Quality Press 2004, 390–392)

3.2.3 Tietoturvaorganisaatio, roolit ja vastuut

<< Oletetaan, että tietoturva- ja toipumisorganisaatio ja -vastuut ovat pitkälti tai kokonaan samat, johtuen mm. organisaation koosta ja selkeästä konkreettisesta toiminnasta. Kuvaa eri tavalla jos aiheellista, esim. jos kyseessä on eri tiimit. >>



Kuvio 8. Tietoturvan / jatkuvuussuunnittelun organisaatio

Kaavan mukaan tietoturvaan on osallistuttava koko Kohdeorganisaation henkilöstön (mukaan lukien johto, substanssiomistajat, muu henkilöstö) ja sen palveluntoimittajien, asiakkaiden ja muiden sidosryhmien. Ensisijaiset tietoturvavastuut ovat johdolla ja tietoturvatiimillä, mistä kerrotaan tarkemmin seuraavaksi. Kohdeorganisaation jatkuvuus- ja toipumistoiminnassa tarvittavat Kohdeorganisaation kaikkien tahojen ja henkilöstön yhteystiedot löytyvät Liitteestä 2.7 tämän dokumentin lopusta. Siitä löytyvät myös kaikkien tahojen, oman henkilöstön ja sidosryhmien yhteystiedot.

Toimiva johto

Päävastuu tietoturvasta, liiketoiminnan jatkuvuudesta ja toipumisprosessien toimivuudesta on Kohdeorganisaation johdolla, joka on käynnistänyt, suunnitellut ja perustanut tietoturvallisuuden hallintajärjestelmän, määrännyt sen politiikan ja jatkaa sen kehittämisen ohjausta ja valvontaa strategisten linjausten ja suunnitelmien mukaisesti. Ylin johto on myös jatkuvuudenhallinnan prosessin omistaja, joka määrittelee suojattavat liiketoimintaprosessit ja -alueet, tunnistaa turvaamisen tarpeet ja osoittaa riittävät resurssit niitä edellyttämiin toimiin.

Toipumis- ja tietoturvatiimi

Käytännön vastuu suunnitelmien luonnista ja toteutuksesta on tietoturva- ja toipumistiimillä, jota ohjaa tietoturvapäällikkö. Hän toimii suunnitelmien koordinaattorina, varmistaa niiden ajantasaisuuden, seuraa henkilöstö-, teknologia-, ympäristö- ja muita muutoksia, ideoi ja esittää johdolle ajankohtaiset tarpeet, järjestää tietoturvaan liittyviä koulutuksia ja harjoituksia sekä ohjaa siihen liittyvää dokumentaation päivittämistä ja ajan tasalla pitämistä.

Tiiminvetäjät, tietojen, prosessien, järjestelmien vastuulliset ja omistajat

Liiketoiminnan tavoitteiden toteuttamisen piirissä nämä henkilöt ja tahot toimivat johdon tukena myös tietoturvallisuuden ja jatkuvuuden osalta omilla vastuualueillaan, mihin liittyen heidän tehtäviään ovat:

- Perusturvallisuuden toimeenpano, toipumisvalmius ja valmiussuunnittelu
- Osallistuminen tietoturvallisuuden ja jatkuvuuden suunnitelmien päivittämiseen
- Systemaattinen raportointi johdolle muutoksista sekä kyvystä varmistaa toiminta
- Teknisten turvallisuustavoitteiden määrittäminen niiden vastuukohdilleen,

Muu henkilöstö

Henkilöstö osallistuu toimintaan oman roolinsa ja työnkuvansa mukaisesti sekä esimiesten, johdon ja tietoturvatiimin määritysten ja ohjeiden mukaan. Se myös osallistuu tietoturva- ja -jatkuvuudenharjoituksiin ja -koulutuksiin. Tärkeää, että jokaisella on oma-aloitteinen ja yrittäjämäinen (ideointi, havainnot jne.) lähestymistapa tietoturvan(kin) osalta.

Ulkoisten ja muiden palveluiden toimittajat, asiakkaat ja muut sidosryhmät

Kohdeorganisaation toiminta on varsin verkostoitunutta, sen kumppanit ja palveluntoimittajat takaavat organisaation palveluiden ja toiminnan tuottamisen. Samalla organisaatio tarjoaa palveluita lukuisille asiakkaille. Tämän johdosta ko. sidosryhmillä on suuri (ja palveluntarjoajilla ratkaiseva) merkitys organisaation tietoturva- ja jatkavuuden hallinnalle. Siksi sidosryhmät ja niiden omat tietoturvallisuusasiat ovat mukana Kohdeorganisaation jatkuvuussuunnittelussa. Lisäksi sidosryhmät huomioidaan tämän suunnitelman tiedotusosiossa.

3.2.4 Suojattavat kohteet

Suojattava kohde on mikä tahansa asia, jolla on arvoa organisaatiolle ja joka sen vuoksi edellyttää suojaamista. Suojattavat kohteet määräävät pitkälle tietoturvallisuuden hallintajärjestelmän ja jatkuvuuden toiminnan kattavuuden ja rajat. Kaikki merkittävät kohteet luetellaan ja yksilöidään tässä suunnitelmassa selkeästi ja luetteloiden ylläpidosta huolehditaan systemaattisesti päivittämällä ne tapahtuvien muutosten mukaisesti tietoturvatiimin voimin tai sen ohjeiden perusteella. Luettelo sisältää kaikki tiedot, joita tarvitaan katastrofista toipumiseen, mukaan lukien kohteen tyyppi, tallennusmuoto, sijainti, varmuuskopiotiedot, lisenssitiedot, omistajat, tärkeys ja arvo liiketoiminnalle.

Nämä tiedot saadaan palveluntuottajilta, järjestelmien-, tietojen- ja prosessien omistajilta, finanssitahoilta, tiiminvetäjiltä. Suojattavien kohteiden tunnistamisen ja luettelemisen yhteydessä tehdään kohteiden dokumentaation kartoitus ja päivitys. Puuttuvat tai vajanaiset dokumentit luodaan (esim. liiketoiminnan ydinprosessien kuvaukset), täy-

dennetään, systematisoidaan, niiden sijainnit keskitetään ja varmuuskopioidaan. Suojauskohteet on lueteltu tyypeittäin Liitteessä 2.1.

Suojattaviin kohteisiin kuuluvat:

- *Palvelut* ja niihin liittyvä *sopimukset* ja sitoumukset: tietojenkäsittely- ja tietoliikennepalvelut, yleishyödylliset palvelut, mukaan lukien Kohdeorganisaation asiakkailleen tarjoamat ja organisaation saamat palvelut
- *Prosessit*: liiketoiminnan ja tietohallinnon ydin- ja tukiprosessit
- *Laitteisto*: tietotekniikkalaitteistot ja - komponentit, tietoliikennelaitteistot, ja verkkoyhteydet, siirrettävät tietovälineet ja muut laitteistot ja vastaavat (esim. virtuaalipalvelimet),
- *Sovellukset ja ohjelmistot*: sovellusohjelmisto, järjestelmäohjelmisto, kehitystyökalut ja apuohjelmat
- *Tieto*: tietokannat ja tiedostot, järjestelmädokumentointi, tutkimustieto, käyttäjän käsikirjat, opetusmateriaali, käyttö- ja tukiohjeistot, liiketoiminnan jatkuvuussuunnitelmat, varajärjestelyt, kirjausketjut ja arkistoitu informaatio
- *Henkilöstöresurssit:* ihmiset ja heidän pätevyytensä, taitonsa ja kokemuksensa
- *Aineettomat tekijät*: organisaation maine ja imago
- *Tukitoimet ja -tahot*: toimisto- tms. rakennukset jne.

3.2.5 Riskien arviointi

Riskit kohdistuvat suojattaviin *kohteisiin*, joita on käsitelty, eli lueteltu, luokiteltu, priorisoitu ja arvioitu edellisen luvun kuvauksen mukaisesti ja tulokset on kirjoitettu Liitteeseen 2.1. Seuraavassa on tarkoitus tunnistaa ja arvioida kunkin kohteen *riskit* ja niiden *tasot*, jotta olisi mahdollista tunnistaa ja valita (tai luoda) tarkoituksenmukaiset ja perustellut turvamekanismit. Riskitaso määräytyy suojattavan kohteen arvon, kohteeseen kohdistaman uhan todennäköisyyden, kohteen haavoittuvuuden, ja suojausmekanismien perusteella. Näin riskien tason arvioinnissa suojattavien *kohteiden lista* (Liite 2.1) toimii pohjana, jonka päälle on kehitetty *riskienhallinnan työkalu*, Liite 2.2. Se on taulukko, jossa on lista riskeistä – ensisijaisesti suojattaviin kohdekohtaisiin liittyviä, mutta myös ”vapaamuotoisia” ja tuloksena riskitasot omassa sarakkeessaan.

Uhkien tunnistus ja todennäköisyyden arviointi

Uhka on riskin potentiaalinen aiheuttaja. Uhka saattaa vahingoittaa suojattavia kohteita, kuten tietoa, prosesseja ja järjestelmiä ja sitä kautta organisaatioita. Uhkien tunnistamiseen ja toteutumisen todennäköisyyden arvioimiseen tarvittavia lähtötietoja saadaan organisaation suojattavien kohteiden omistajilta tai käyttäjiltä, henkilöstöltä, toimitilajohdolta ja tietoturva-asiantuntijoilta, lakitaholta ja muilta organisaatioilta, esim. vakuutusyhtiöiltä ja viranomaisilta. Merkitykselliset uhat vaihtelevat jatkuvasti, erityisesti jos liiketoimintaympäristö tai tietojärjestelmät muuttuvat. Uhat merkitään riskienhallinnan työkalun (Liite 2.2) *Uhka*-sarakkeeseen. Uhkien tunnistamisen jälkeen arvioidaan kunkin niistä toteutumisen todennäköisyys ja vaikutus määrällisen tai laadullisen arviointimenetelmän avulla. Esimerkiksi uhan toteutumisen osalta se voi olla: ei mahdollinen, epätodennäköinen, todennäköinen, varma.

Turvamekanismien tunnistus

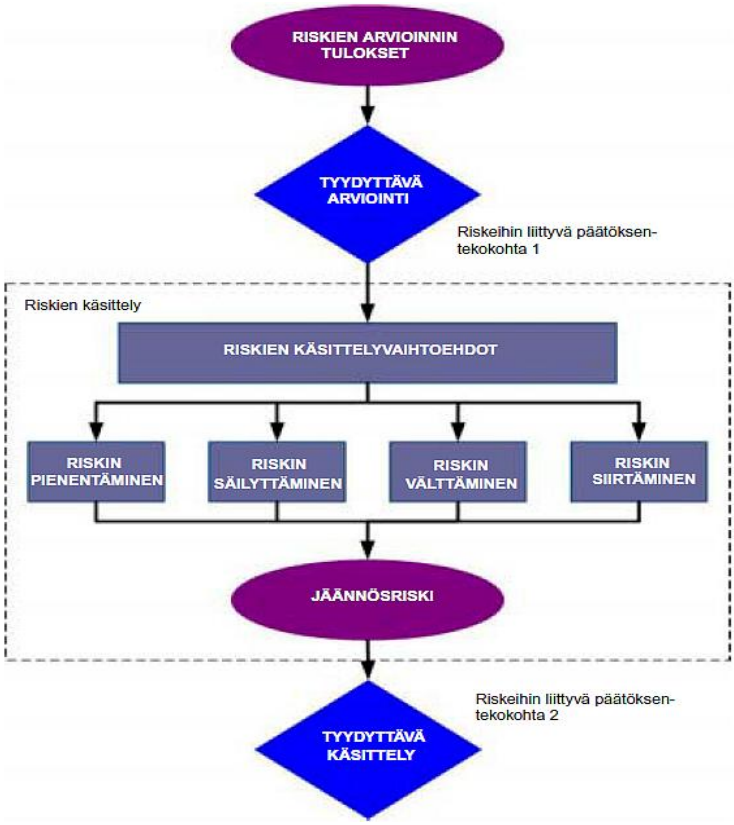
Riskien arvioinnissa hyödynnetään organisaatiossa tunnistettuja turvamekanismeja. Turvamekanismi on käytäntö, menettelytapa, looginen tai tekninen ratkaisu, väline tai niistä rakentama kokonaisuus, jonka avulla toteutetaan tietoturvaan liittyvät toimet ja kontrollointi. Käytössä olevien turvamekanismien tunnistamisen yhteydessä tarkistetaan, että ne toimivat oikein. Jos puutteita löytyy, ne korjataan. Tunnistetut turvamekanismit luetellaan (Liite 2.3). Riskikohtaiset turvamekanismit merkitään riskienhallinnan työkalun (Liite 2.2) *Turvamekanismi(TM)*-sarakkeeseen ja niiden toteutusastetta *TM-toteutus* -sarakkeeseen.

Riskien vaikutusten arviointi ja riskitasojen määrittely

Kun suojattavat kohteet ja uhat on tunnistettu, uhkatodennäköisyydet arvioitu ja olemassa olevien turvamekanismien tunnistus on tehty, suoritetaan riskien vaikutusten arviointi. Tulokseksi saadaan päivitetyt riskiluettelon riskien *tasot*, jotka merkitään riskienhallinnan työkalun (Liite 2.2) *Riskitaso*-sarakkeeseen. Se on *riskien arvioinnin* tärkeimpiä tuloksia riskien käsittelyä varten (ks. alaluku).

3.2.6 Riskien käsittely

Tässä riskienhallinnan prosessin vaiheessa käsitellään kustannustehokkaat tavat ja toimet, joilla on mahdollista hallita riskejä. Riskien käsittelyyn on käytettävissä neljä vaihtoehtoa: riskin pienentäminen, säilyttäminen (hyväksyntä), välttäminen ja siirtäminen. Seuraava kuva esittää riskien käsittelytoimintaa.



Kuvio 9. Riskien käsittely (Tietoturvastandardi 2700x 2009, 42)

Riskin pienentäminen

Riskitasoa alennetaan valitsemalla turvamekanismit siten, että jäännösriski voidaan uudelleen arvioitaessa todeta hyväksyttäväksi. Käytännössä tässä vaiheessa tehdään *nykyisten* turvamekanismien ja *jatkokehittämistarpeiden* kartoitus, jonka seurauksena päätetään mahdollisten uusien turvamekanismien luomisesta, olemassa olevien parantamisesta sekä päällekkäisyyksien ja turhien mekanismien poistamisesta. Tämän vaiheen tuloksena saadaan mahdollisten turvamekanismien luettelo sekä tiedot niiden kustannuksista, hyödyistä ja toteuttamisen tärkeysjärjestyksestä (Liite 2.3).

Riskin säilyttäminen

Jos riskitaso täyttää riskin hyväksyntäkriteerit, muita turvamekanismeja ei tarvitse toteuttaa ja riski voidaan päättää säilyttää. Päätökset riskin säilyttämisestä ilman lisätoimenpiteitä perustuvat riskien vaikutuksen arviointiin ja ne merkitään riskienhallinnan työkaluun (Liite 2.2).

Riskin välttäminen

Tiettyä riskiä aiheuttavaa toimintaa tai olosuhteita vältetään. Jos tunnistetut riskit katsotaan liian suuriksi tai riskien muiden käsittelyvaihtoehtojen kustannukset ovat hyötyjä suuremmat, voidaan päättää välttää riski kokonaan vetäytymällä suunnitellusta tai käynnissä olevasta toiminnasta tai toiminnoista tai muuttamalla olosuhteita, joissa toimintaa suoritetaan. Päätökset ja käsittelyn tulokset merkitään riskienhallinnan työkaluun (Liite 2.2).

Riskin siirto

Organisaatiossa riski siirretään toiselle osapuolelle (lähinnä palveluntarjoajalle), joka riskien vaikutuksen arvioinnin perusteella pystyy tehokkaimmin hallitsemaan kyseistä riskiä. Riskin siirto tarkoittaa päätöstä jakaa tietyt riskit organisaation ulkopuolisten tahojen kanssa. Riskin siirto voi aiheuttaa uusia riskejä tai muuttaa aiempia tunnistettuja riskejä. Tämän vuoksi saatetaan tarvita uutta riskien käsittelyä. Siirto voidaan tehdä esimerkiksi vakuutuksella, joka tukee seurauksia tai tekemällä sopimus sellaisen kumppanin kanssa, jonka roolina on tarkkailla tietojärjestelmää ja pysäyttää hyökkäys välittömillä toimenpiteillä ennen kuin se aiheuttaa määritellyn tasoisen vahingon. Päätökset ja käsittelyn tulokset merkitään riskienhallinnan työkaluun (Liite 2.2).

3.2.7 Riskinanalyysin tulokset

Tässä vaiheessa riskit on sekä *tunnistettu* (kohteet arvoineen, uhat todennäköisyyksineen, nykyiset turvamekanismit) että *käsitelty* (riskien siirto, säilyttäminen, välttäminen, pienentäminen turvamekanismien kehityskartoituksineen). Seuraavaksi luodaan *riskien kä-*

sittelysuunnitelma (Liite 2.4), määritetään jäännösriskit, päätetään riskien hyväksynnästä ja tulokset päivitetään *riskienhallinnan työkaluun* (Liite 2.2).

Riskien käsittelysuunnitelma

Joillakin riskin käsittelytavoilla voidaan käsitellä tehokkaasti useampaa kuin yhtä riskiä (esim. tietoturvakoulutuksen ja -tietoisuuden avulla). Riskien käsittelysuunnitelma määritellään ja siinä selkeästi yksilöidään, missä tärkeysjärjestyksessä yksittäiset riskien käsittelytoimenpiteet toteutetaan ja millainen on toimenpiteiden aikataulu. Tärkeysjärjestys määritetään eri tavoin, kuten riskien luokittelun ja kustannus-hyötyanalyysin avulla. Silloin Kohdeorganisaation johto päättää turvamekanismien toteuttamisen kustannusten tasapainottamisesta ja budjettivarauksista. Käsittelysuunnitelma on kuvattu Liitteessä 2.4.

Jäännösriskit

Jäännösriski on riskien käsittelyn jälkeen jäljellä oleva riski. Kun riskien käsittelysuunnitelma on määritelty, täytyy määrittää jäännösriskit. Tämä tarkoittaa riskien arvioinnin päivittämistä tai toistamista siten, että arvioinnissa otetaan huomioon ehdotettujen riskien käsittelytapojen odotetut vaikutukset. Mikäli jäännösriski ei edelleenkään täytä organisaation riskin hyväksyntäkriteerejä, saattaa olla tarpeen toistaa riskien käsittely ennen siirtymistä riskin hyväksyntään. Jäännösriskiä myös pyritään esiarvioimaan riskien käsittelysuunnitelmassa (Liite 2.4).

Tietoturvariskien hyväksyntä

Riskien hyväksymisestä päätetään ja tämä päätös sekä vastuu siitä kirjataan. Riskien käsittelysuunnitelma kuvaa, miten arvioituja riskejä käsitellään niin, että ne saadaan täyttämään riskin hyväksyntäkriteerit. Vastuullinen johto katselmoi ja hyväksyy ehdotetut riskien käsittelysuunnitelmat ja jäljelle jäävät jäännösriskit sekä kirjaa kaikki hyväksyntään liittyvät ehdot. Tulokseksi saadaan luettelo hyväksytyistä riskeistä ja perustelut sellaisille riskeille, jotka eivät ole organisaation tavanomaisten riskin hyväksyntäkriteerien

mukaisia (Liite 2.5). Tätä informaatiota käytetään mm. liiketoiminnan toipumissuunnittelussa (ks. ko. luku alempana).

Riskin hyväksyntäkriteerit

Riskin hyväksyntäkriteerit laaditaan ja määritellään. Riskin hyväksyntäkriteerit riippuvat usein organisaation toimintaperiaatteista, tavoitteista, päämääristä ja sidosryhmien näkemyksistä.

3.2.8 Riskikohtaiset käsittelykuvaukset ja toipumissuunnitelmat

Kun kaikki riskit on tunnistettu ja arvioitu käyttäen riskienhallinnan työkalua (Liite 2.2), niistä jokaisesta (ainakin merkittävimmistä) luodaan tarkempi *käsittelykuvaus* sekä *toipumissuunnitelma*, joka riskin toteutuessa esittää ohjeet ja toimenpiteet normaaliin tilaan palaamiseksi.

Eri kriisitilanteissa, eri kohteilla ja riskitoteutuksissa on omat toipumistoimenpiteensä. Esim. toimistotilojen tulipalo tai tärkeän loppukohdeorganisaatiolle toimitettavan palvelun osa (ohjelmisto, komponentti tms.) vaativat aivan erilaisia toipumistoimia. Osassa tapauksista kuitenkin saattaa olla samanlainen toipumismenettely - joko kokonaan tai suurilta osin. Seuraava luku esittää juuri sellaista toipumissuunnitelman esimerkkiä osana "perusriskitapauksen" käsittelykuvausta. Se kuvaa sitä toimintajärjestystä ja niitä toimenpiteitä, jotka pitää suorittaa vahingon sattuessa.

RISKI: PERUSTAPAUS / ESIMERKKI

Todennäköisyys
Keskitaso

Vaikutustaso
Suuri

Todennäköinen skenaario

Esim.: maailmanlaajuinen tai keskitetysti Kohdeorganisaation ympäristöihin/palveluihin/IT-järjestelmiin suunnattu virus- tai muu hyökkäys, joka lamauttaa kaikki palvelimet ja palvelun toimittaminen kohdeorgranisaatiolle keskeytyy

Vaikutusalue

Kaikki konesalitoiminnot, mahdollisesti myös toimisto- ja käyttäjälaitteet (ml. ainakin osa työasemista)

Ennaltaehkäisevät toimenpiteet ja valmistelut

Ennakoivat toimenpiteet ko. riskiä ja siihen liittyvää toimintaa koskien on suoritettu ylempänä riskienhallintaan liittyvissä yläluvuissa kuvattujen menettelyjen ja niiden saamien tulosten mukaan.

Resurssit

Konesalipalvelun toimittaja, tietoturvatiimi, <<*lisää tai muokkaa tarpeen mukaan*>>

Rajoitteet

<<*rajoitteet tähän*>>

Riskikohtaisen toipumissuunnitelman aktivointi

Toipumisvaiheen aktivoinnista vastaa aina tietotuva-/toipumistiimi.
<<*aktivoinnin kriteerit tähän*>>

Toipumissuunnitelman viimeinen testaus ja päivitys

<<*ko. tiedot tähän ja Liitteeseen 2.6*>>

Varsinainen toipumissuunnitelma

Seuraavassa on esitetty "perustapaus"-riskin toipumissuunnitelman päävaiheet. Kriisitilanteessa toimitaan niiden mukaan. << *Laajenna, tarkenna, muuta järjestystä ko. vaiheiden osalta jokaisessa riskikohtaisessa toipumissuunnitelmassa tarpeiden ja tarkoitusten mukaan; määrittele vastuulliset, aikarajat jne.* >>

1. Tilanteen tunnistaminen
2. Toipumisryhmän hälyttäminen ja mobilisointi
3. Henkilöstön hälyttäminen
4. Tapahtumien analysointi
5. Käytössä olevien resurssien määritteleminen
6. Roolien ja vastuiden jakaminen
7. Liiketoimintavaikutusten kartoitus
8. Ennalta määrättyjen toimenpiteiden tekeminen
9. Vahinkojen määrän rajoittaminen
10. Vaikutukset henkilöihin; sitten ydintoimintaan, tiloihin, laitteistoon yms.
11. Vahinkojen arviointi
12. Ennalta määrättyjen toimenpiteiden suoritukset
13. Yksityiskohtaisen palauttamissuunnitelman valmistelu
14. Normaalijärjestelmään palautumisen edellyttämät hankinnat ja kunnostustoimenpiteet
15. Tarkennettujen toipumistoimien käynnistäminen ja suorittaminen
16. Palautumisprosessin valvonta ja tapahtumien kirjaaminen
17. Tarvittavien osapuolten informointi ja tiedotussuunnitelma (kriteerit, ajoitus, riippuvuudet, kohderyhmät ja niiden järjestys, ulkoisen ja sisäisen tiedottamisen sisällöt, tiedotuskanavat ja -periaatteet, vastuut ja valtuudet)
18. Toimintojen johtamisen palauttaminen normaalille johdolle (tarvittaessa)
19. Palautumisvaiheen raportin valmistelu
20. Tilanteen ja suoritettujen toimenpiteiden analyysi ja jälkihoito
21. Syiden selvitys ja parannukset toimintatapoihin
22. Toipumis- ja jatkuvuussuunnitelmien ja muiden tarvittavien dokumenttien päivittäminen

RISKI: XX

<<Kuvaa edellä olevan esimerkin mukaan jokaisen merkittävän riskin käsittelykuvaus, ml. toipumissuunnitelma. >>

3.2.9 Liiketoiminnan jatkuvuussuunnitelman laadinnan jälkeinen toiminta

Auditointi, testaus, uudelleenarviointi, päivitys

Liiketoiminnan jatkuvuussuunnitelman toimivuuden ja tehokkuuden varmistamiseksi sitä auditoidaan (esim. sisäisesti) ja päivitetään kokonaisuudessaan sekä testataan riskikohtaisia toipumissuunnitelmia säännöllisesti, vähintään kerran vuodessa. Tällä toiminnalla varmistetaan, että kaikki tietoruva- ja toipumistiimin jäsenet ja muut olennaiset henkilöstön jäsenet ovat tietoisia suunnitelmasta ja liiketoiminnan jatkuvuuteen ja tietoturvallisuuteen liittyvistä vastuistaan sekä tietävät roolinsa otettaessa suunnitelma käyttöön. Liiketoiminnan jatkuvuussuunnitelman auditoinnin ja riskikohtaisten toipumissuunnitelmien testauksen aikatauluista (Liite 2.6) ilmenee, miten ja milloin kutakin suunnitelman osaa tarkistetaan ja testataan. Testaamisessa käytetään eri tekniikoita varmistamaan, että suunnitelma toimii myös todellisuudessa. Testaustekniikoihin sisältyy esim. eri vaihtoehtojen pöytätestausta, simulaatioita, toimittajien laitteiden ja palvelujen testausta sekä kokonaisia harjoituksia. Näitä tekniikoita sovelletaan kyseisen suunnitelman kannalta olennaisella tavalla. Testien tulokset kirjataan ja tarvittaessa ryhdytään toimenpiteisiin, joilla parannetaan suunnitelmia.

Jatkuvuussuunnitelman säännöllistä katselmusta varten nimetty vastuuhenkilö on tietoturvapäällikkö. Sen jälkeen, kun on tunnistettu liiketoimintajärjestelyjen muutokset, jotka eivät vielä näy liiketoiminnan jatkuvuussuunnitelmissa, seuraa suunnitelman asianmukainen päivitys. Tämä virallinen muutoksenvalvontaprosessi varmistaa sen, että päivitetty suunnitelma tulee jakeluun ja se vahvistetaan kokonaissuunnitelman säännöllisellä katselmuksella. Esimerkkejä muutoksista, joiden yhteydessä päivitetään liiketoiminnan jatkuvuussuunnitelmia, ovat palveluntarjoajien muutokset, uusien laitteiden hankkiminen, järjestelmien päivitykset sekä muutokset henkilöstössä, liiketoimintastrategiassa, osoitteissa ja puhelinnumeroissa, sijainnissa, palveluissa ja resursseissa, lainsäädännössä, sopimusosapuolissa, toimittajissa ja avainasiakkaissa, prosesseissa sekä riskeissä. Jatkuvuussuunnitelman auditoinnin tuloksena saadaan raportti ja ehdotukset jakokehittelyyn (mm. riskienhallinnan osalta) sekä päivityksiin. Toipumissuunnitelmien testauksen tietoja on esitetty Liitteessä 2.6.

Koulutus

Jatkuvuussuunnitelmasta, sen käsittelemästä riskienhallinnasta, riskeistä ja niihin liittyvistä toipumissuunnitelmista pidetään säännöllisiä koulutustilaisuuksia koko Kohdeorganisaation henkilöstölle ja muille sidosryhmille. Samoin sitä esitetään uusille työntekijöille työsuhteen alussa. Kaikki tietoturva-/toipumistiimin jäsenet ja heidän varajäsenet koulutetaan sen lisäksi jatkuvuussuunnitelman auditointien, päivittämisten ja toipumissuunnitelmien testaamisen yhteydessä. Koulutuksessa otetaan huomioon erilaiset kohderyhmät. Koulutusten suunnittelusta, toteutuksesta, dokumentoinnista ja raportoinnista vastaa tietoturvapäällikkö.

Suunnitelman jakelu ja säilytys

Tämä suunnitelmaa säilytetään…<<*tiedot säilyttämisestä (ml. varmuuskopio) ja jakelusta*>>

4 Pohdinta (diskussio): yhteenveto ja johtopäätökset

Tämä luku kertoo tutkimuksen yhteenvedosta ja johtopäätöksistä. Ensiksi käsitellään aiheenvalinnan merkittävyyttä nykytietämyksen kannalta. Seuraavaksi käydään läpi yhteenvedot tutkimisongelmasta, -kysymyksistä, -tavoitteista sekä valituista metodeista. Sen jälkeen esitetään tutkimustulokset koskien tietoperustaa, käytäntöä eli empiriaa sekä kokonaisuudessaan (ml. toimintamallin osalta). Tämän jälkeen pohditaan tutkimuksen luotettavuutta, siirrettävyyttä ja hyödynnettävyyttä. Lisäksi esitetään ehdotuksia jatkotutkimukseksi. Luvun lopuksi tarkastellaan tutkimustekijän oppimista ja kehittymistä opinnäytetyöprosessin aikana.

4.1 Aihevalinnan merkittävyys nykytietämyksen kannalta

Seuraavassa esitetään valittuun aiheeseen liittyvät huomiot:

Työelämää hyödyntävä ja kehittävä

Aihevalinta ja sen pohjalta suoritettu tutkimus tuloksineen auttaa kohde- tai oikeastaan mitä tahansa organisaatiota arviomaan oman tietoturvansa nykytilaa, käsittelemään riskejä ja luomaan toiminnan jatkuvuussuunnitelma, mikä jatkossa edesauttaa toimimista oikein kestävän operoinnin, johtavuuden ja laadun takaamiseksi.

Tekijän omia ammattiopintoja syventävä

Asia on esitetty alempana tämän luvun viimeisessä alaluvussa.

Ajankohtainen

Tietoturvan merkitys kasvaa päivä päivältä niin pienissä kuin suurissakin organisaatioissa. Tietoturvasta on huolissaan niin asiakas kuin organisaatiokin. Aihe on erittäin ajankohtainen nykyisessä yritysmaailmassa, varsinkin IT-alalla (joka tavalla tai toisella on nykyään mukana kaikilla aloilla). Liiketoiminnan on mahdoton kehittyä ilman kestävää ja vahvaa tietoturvatietämystä ja sen avuksi tehtyä jatkuvuudensuunnitelmaa, joka tukee liiketoiminnan jatkuvuutta ja vastaa tietoturvallisuuden parhaita käytäntöjä sekä tärkeimpiä standardeja. Tietoturvan huipputason osaajista on jatkuva pula sekä Suomessa että maailmalla, mikä on näkyvästi esillä alan ja yleisissä medioissa ja työpaikkailmoituksissa.

Uutuusarvoinen

Tietoturvaan liittyviä tutkimuksia on tehty jonkin verran. Tämän tutkimuksen lisäarvo organisaation ja tutkimustoiminnalle on siinä, että tutkimus sisältää tietoturvan ja sen tarkastuksen lisäksi myös siihen liittyvän tärkeän kokonaisuuden eli liiketoiminnan jatkuvuuden. Toiseksi se esittää valmiiksi laadittuja malleja ko. dokumenteista ja niihin liittyviä käytännönläheisesti rakennettuja valmiita työkaluja.

Sopivasti rajattu

Asia on esitetty Johdannon omassa kohdassa *Tutkimuksen rajaus.*

Tutkimuksen tekijää kiinnostava

Tämän tutkimuksen tekijä on muutamien koulu- ja työelämässä vietettyjen vuosien aikana todennut juuri kyseisen alueen tarvitsevan lisää tutkimista ja kehittämistä. Aiheesta tulikin tämän tutkimuksen kohde. Se myös liittyy tutkimuksen tekijän työpaikkaorganisaatioon hankkeeseen, jonka tulokset tulevat vaikuttamaan koko organisaation toimintaan. Näin ollen aiheen valintaan on vaikuttanut sen kiinnostavuus tutkimuksen tekijälle monesta eri syystä: työpaikan, työelämän tarpeiden ja koulutuksen kautta, kuten myös ajankohtaisuuden ja haasteellisuuden takia.

4.2 Yhteenveto tutkimusongelmasta, -kysymyksistä, -tavoitteista ja -metodeista

Tämän työelämälähtöisen tutkimuksen päämääränä ja tarkoituksena oli ratkaista ongelma, joka syntyi kohdeorganisaation toiminnan (liiketoiminta ja IT) tietoturvatehostamistarpeista. Sen ratkaisemiseksi oli tarkoitus tutkia tilanne sekä kehittää ja tarjota toimintamalli, joka kuvaa organisaation tietoturvan nykytilan selvittämistä ja jatkokehittämisen prosesseja sekä näihin liittyviä tekijöitä. Työn seurauksena tulokseksi saatiin tietoturvaan liittyvien toimintojen ja asioiden selkeyttäminen, yhdenmukaistaminen ja keskitetty ohjaus. Lisäksi luotiin käytännön työkaluja, kuten dokumenttimallit ja -pohjat ja niihin liittyvät matriisit, taulukot ja listat.

Tutkimus sisältää teoria- ja empiriaosuudet, joiden avulla se vastaa kahteen tutkimuskysymykseen. Ensimmäisen kysymyksen osalta tutkimus osoittaa asioita, antaa ohjeistusta, esittää työkaluja ja dokumenttimallin, joiden avulla on mahdollista selvittää organisaation nykyinen tietoturvatila ja esittää saatuihin tuloksiin perustuvia ehdotuksia sen jatkokehittämiselle. Toinen kysymys keskittyi organisaation liiketoiminnan jatkuvuuden suunnitteluun, jossa lähdettiin liikkeelle ensimmäisen kysymyksen tuloksia hyödyntä-

mällä. Molemmat kysymykset sisältävät sekä teoriaa että toteutusosuutta. Ensimmäinen tutkimuskysymys K1 oli seuraava: Miten kirjallisuudessa esitetään, kuinka voidaan selvittää organisaation nykytila, sen puutteet, ongelmat ja muutostarpeet, miten ja mitä tuloksia saadaan, miten ja kenelle ne esitetään, miten hyödynnetään, ja mitä vaatimuksia näille kaikille asetetaan?

Yllämainittuun kysymykseen liittyen tavoitteena oli esittää tutkittujen kirjallisuuslähteiden pohjalta mainittuja asioita niin, että niitä voidaan hyödyntää käytännössä. Toisena tavoitteena oli kuvata menetelmä, toimintamalli eli prosessi ja eteneminen, jonka mukaan tietoturvan arviointi pitää tapahtua. Kolmannen tavoitteen tarkoitus oli selvittää tarvittavat ja riittävät tietolähteet, mitä ko. arvioinnissa pitää käyttää ja mitkä asiat toimivat arvioinnin perustana ja kriteereinä. Neljäntenä tavoitteena oli saada käsitys siitä, mitä tuloksia pitäisi saada, missä muodossa, kenelle ja miten ne esitetään ja jatkokäsitellään.

Toinen tutkimuskysymys oli seuraava: Miten nykyteorian ja -vaatimusten pohjalta toteutetaan käytännössä seuraavat asiat: miten tietoturvan arvioinnin jatkeeksi suunnitellaan liiketoiminnan jatkuvuutta, mitä ko. suunnitelma pitää sisällään, miten sitä käytetään ja mitä vaaditaan, jotta lopputuloksena organisaatio saisi käyttöönsä tehokkaat pelastustyökalut ja jatkuvasti uusiutuvan ja parannettavan prosessin eikä pelkkää dokumentaatiokansiota.

Tämän kysymyksen tavoitteena oli samoin kuin edellisessä kysymyksessä esittää tutkittujen kirjallisuuslähteiden pohjalta K2-kysymyksessä ja sen seuraavissa tavoitteissa mainitut asiat niin, että niitä voi hyödyntää käytännössä. Toiseksi tavoitteena oli esittää, miten voi selvittää ja valmistella organisaation liiketoiminnan jatkuvuussuunnitelmaa varten sen rakenne ja pääosat, mm. tietoturvapolitiikka ja -organisaatio, vastuut, toiminnot, suojattavat kohteet, riskienhallinta jne. Kolmantena tavoitteena oli kuvata työkalut ja dokumentit, joiden avulla suunnitelmasta saadaan aikaan toimiva, selvä ja hyödyllinen. Neljäntenä tavoitteena oli esittää valmis suunnitelmaesimerkki, josta ilmenee jatkuvuussuunnittelun malli sekä käynnistettävät ja suoritettavat toimenpiteet kertasuorituksina ja myös prosesseina.

Tässä työssä tutkimusmenetelminä käytettiin aiheen kirjallisuuden katsausta (kansainvälisiä ja kotimaisia standardeja, parhaita käytäntöjä, julkishallintoa ja VAHTI-suosituksia, sekä ajankohtaista kirjallisuutta), niiden analysointia ja hyödyntämistä valmiiden dokumenttimallien ja niiden liitteiden muodossa.

Nämä sisältävät lähestymistavat, toteutumisprosessien kuvaukset, sekä niihin liittyvät työkalut, kuten dokumenttipohjat ja lomakkeet. Näiden avulla kohdeorganisaatiolle esitettiin keinot tarkastaa kohteen tietoturvaa ja suunnitella liiketoiminnan jatkuvuutta. Tutkimus on tyypiltään kvalitatiivinen eli laadullinen tapaustutkimus, jossa käytetään myös toimintatutkimuksellista otetta.

4.3 Yhteenveto tutkimustuloksista

Tämä tutkimustulosten yhteenveto sisältää kolme osaa, jolloin saatu yhteenveto esitetään ensin tietoperustasta (kirjallisuus ja teoria), tämän jälkeen toteutuksesta (empiria) ja lopuksi esitetään niiden yhteiseksi tulokseksi saatu tietoturvan kehittämisen toimintamalli. Näin tutkimuksen keskeinen tulos on organisaation (ensisijaisesti PAVE) tietoturvan tehostaminen, sisältäen mm. tietoturvan tarkastusprosessin ja -raportin, sekä toiminnan jatkuvuuden prosessin ja suunnitelman - sekä raporttiin ja suunnitelmaan liittyvien prosessien parantamisen ja päivittämisen. Tutkimuksen empiriaosuus sisältää valitun aiheen toteutuksen reaalityöelämän tapauksessa, nykyaikaisen organisaation piirissä, mikä antaa varmasti lisäarvoa ko. tutkimukselle. Työ ei rajoitu siis pelkästään kirjallisuuden lähteiden käsittelyyn ja olettamuksiin, vaan niiden avulla kehitetty toimintamalli lähtee käsittelemään nykyorganisaation ajankohtaista näkökulmaa tietoturvaan, sisältää mallin parannusten toteuttamiselle sekä kuvaa esimerkein käytännön toteutusta.

Yhteenveto tietoperustaan liittyvistä tutkimustuloksista

Kysymykseen K1 ja sen tavoitteisiin liittyen tutkimuksessa saatiin tietoperustan eli kirjallisuuskatsauksen perusteella seuraavia tuloksia:

- tiedot organisaation nykytietoturvatasosta, sen parannusehdotuksista, muutostoimenpiteistä, puutteista ja ongelmista
- selvitys siitä, mitä ja miten tuloksia saadaan, miten niitä hyödynnetään ja kenelle esitetään
- selvitys kansainvälisestä normistosta ja ohjeistuksesta
- selvitys kansallisesta lainsäädännöstä
- esitetyt käsitykset tietoturvan johtamisesta ja hallinnasta
- selvitys tietoturvallisuuden rooleista ja vastuista
- tiedot tietoturvan standardeista ja viitekehyksistä
- selvitys tarkastuksen prosessista, ml. suunnittelu ja alustava tutkimus, arviointisuunnitelman laadinta, tarkastuksen tietolähteet (evidenssit), arviointiperusteet (kriteerit), tarkastuksen kohteet, tietoturvan tarkastettavat osa-alueet, kenttävaihe
- selvitys tuloksista ja niiden jatkokäsittelystä

Kysymykseen K2 ja sen tavoitteisiin liittyen tutkimuksessa saatiin tietoperustan eli kirjallisuuskatsauksen perusteella seuraavia tuloksia:

- selvitys liiketoiminnan jatkuvuussuunnittelun termistöstä
- selvitys jatkuvuussuunnittelun tavoitteista ja hyödyistä
- katsaus jatkuvuussuunnittelun standardeihin ja vastuihin
- selvitys jatkuvuussuunnitelmassa käytettävistä tietolähteistä
- ohjeistus laatimisen vaiheista ja sisällöstä
- selvitys testauksesta ja jatkokäsittelystä

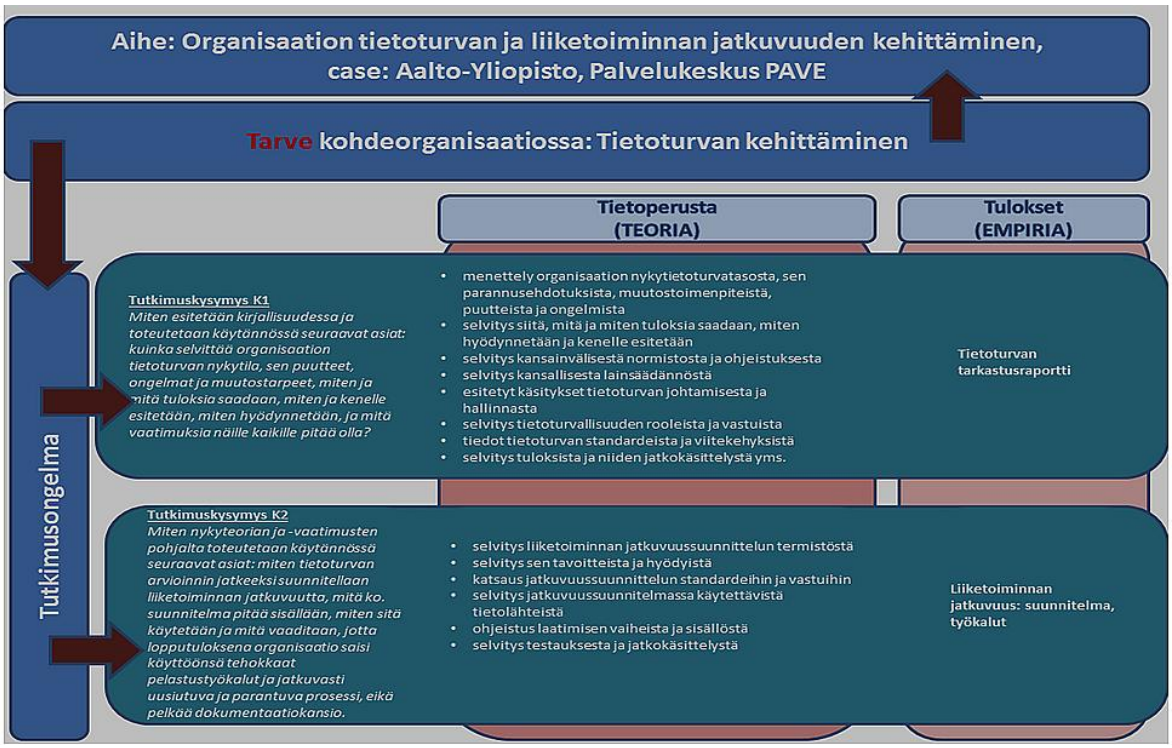
Yhteenveto empiiriseen tutkimukseen liittyvistä tuloksista

Kysymyksiin K1 ja K2 sekä niiden tavoitteisiin liittyen tutkimuksessa saatiin empirian osalta seuraavanlaisia tuloksia:

- organisaation tietoturvatarkastuksen raporttimalli
- liiketoiminnan jatkuvuuden suunnitelmamalli työkaluineen

Yhteenveto yhteistulokseksi saadusta tietoturvan kehittämisen toimintamallista

Yhteistulosten yhteenvedoksi voi todeta, että tutkimuksen ongelma ja kohdeorganisaation tarve tuli ratkaistua, tutkimuskysymyksiin saatiin tarvittavat ja riittävät vastaukset, kysymysten ja tutkimuksen tavoitteet on saavutettu. Seuraava kuva esittää tutkimuksen keskeisimmät tulokset, jossa mm. peilataan tietoturvaperustan alueita empiriaan tutkimusongelman ja -kysymysten rajoissa.



Kuvio 10. Tutkimuksen tulokset, aikaansaatu toimintamalli.

4.4 Tutkimuksen luotettavuus, siirrettävyys ja hyödynnettävyys

Kvalitatiivisessa eli laadullisessa tutkimuksessa *luotettavuutta* pohtiessa keskitytään tarkastelemaan tutkimuksen uskottavuutta ja siirrettävyyttä (Haaga-Helia 2013, 32).

Tämän tutkimuksen *uskottavuuden* ja sitä kautta luotettavuuden perustana on se, että tutkimusta ja sen tuloksia on lähdetty tekemään lähtien käytännön tarpeista eli reaalielämän organisaation tavoitteista ko. alueen osalta. Tulokset on hyväksytty kohdeorganisaatiossa, mikä osoittaa sen, että tarvittavat tulokset ja asetetut päämäärät on saavu-

tettu tarpeellisella tasolla. Toiseksi luotettavuuden todentaa se fakta, että tietoperustana on käytetty korkealaatuisen kotimaisen ja kansainvälisen kirjallisuuden lisäksi alan tärkeimpiä viimeisimpiä standardeja, parhaita suosituksia ja viitekehyksiä.

Tutkimuksen *hyödynnettävyys* lähtee myös kohdeorganisaatiosta, jossa sen tulokset eli erityisesti empirian toteutus tarkastusprosessin ja -raportin sekä liiketoimintajatkuvuuden suunnitelman muodossa on siis todettu toimiviksi ratkaisuiksi. Lisäksi toteutuksessa on alusta asti korostettu prosessinomaista lähestymistapaa, jolloin empirian tulokset ovat ikään kuin automaattisesti kehittyviä ja reaalielämän muutoksia tukevia.

Tutkimuksen *siirrettävyys* toteutuu siten, että alusta asti on pyritty luomaan sellainen toimintamalli, joka ei rajoitu tietyn tai tietyntyyppisen organisaation ominaispiirteiseen toimintaan, organisaatiotyyppiin tai esim. toiminta-alaan. Näin tuloksena saatuja dokumenttimalleja työkaluineen pääsee käyttämään jopa melkein sellaisinaan missä tahansa organisaatiossa.

4.5 Suositukset, kehittämis- ja jatkotoimenpide-ehdotukset

Tietoturva ja osana sitä *organisaation tietoturvan kehittäminen* on aiheena aika laaja ja pitkäjänteinen. Siksi on vaikeaa syventyä kerralla sen kaikkiin tekijöihin ja osa-aiheisiin huomioiden kaikki näkökulmat ja niiden vaikutukset ko. tutkimuksen lopputulokseen. Tutkimuksen aikana saadut tiedot ja tulokset antavat tutkijalle aihetta esittää seuraavia jatkotutkimusehdotuksia.

Tämä tutkimus pitää sisällään toimintamallin ja siihen kuuluvat määrittelyt ja toteutuksen. Olosuhteiden, tarkoituksen ja valitun rajauksen takia tutkimus ei tässä toteutuksessa ulotu aiheen tarkasteluun aivan kaikista näkökulmista. Näin jatkotutkimuksen kohde voisi olla tilanne, jossa käytetään toisenlaisia käytäntöjä, suosituksia ja standardeja ja sitä kautta saatuja työkaluja (muut kuin tutkimuksessa mainitut). Toinen jatkotutkimuksen lähestymistapa voisi olla sellainen, jossa painopiste tietoturvan tarkastuksessa ja jatkuvuuden suunnittelussa olisi enemmän teknisessä toteutuksessa, ml. tekniset prosessit, ohjelmistot, toteutukset. Kolmas jatkotutkimuskohde on suunnattu niille organisaatioille, joille esim. jatkuvuussuunnittelun toteuttamisen kustannuksilla on suurempi merki-

tys: tällöin tutkimuksen avulla otettaisiin selvää, miten saavutetut hyödyt vastaavat investointeja.

4.6 Tutkimustekijän oppiminen ja kehittyminen opinnäytetyöprosessin aikana

Tässä tutkimuksen ja opinnäytetyön viimeisessä alaluvussa kuvataan lyhyesti tämän työn vaikutusta ja tärkeyttä sen tekijän ammatillisen oppimisen ja kehittymisen kannalta.

Tutkimuksen ideoinnin, valmistelun, toteutuksen ja jälkikäsittelyn aikana työn tekijä on saanut hyvän mahdollisuuden kokonaisvaltaisesti käyttää niitä taitoja, joita tarvitaan asiantuntijatehtävissä työelämässä. Näitä taitoja ovat mm. luova ongelmanratkaisukyky, tiedonhankinta ja kriittinen arviointi, analysointi, systematisointi, jäsentäminen, esittäminen, valmiin tuloksen tuotteistaminen. Tekijän mielestä opinnäytetyön tavoite on onnistuttu saavuttamaan, mukaan lukien tavoite, jonka muukaan tekijän pitäisi työn aikana kehittää ja osoittaa valmiuksia soveltaa tietojaan ja taitojaan ammattiopintoihin liittyvässä käytännön asiantuntijatehtävässä (Asetus ammattikorkeakouluista 352/2003).

Tehdessään opinnäytetyötä tekijä on oppinut tuottamaan ammatillisesti käyttökelpoista tietoa ja hyödyntämään sitä käytännössä. Aalto/PAVE:n casen avulla on onnistuttu varmistamaan ammattikorkeakoulun opinnäytetyön työelämälähtöisyys ja tulosten sovellettavuus käytännön ongelmatilanteisiin. Näin ammatillisen kasvun lisäksi tutkimuksen tekijä voi hyödyntää työtään ja siinä hankittua osaamista mm. työnhaussa ja tulevissa tehtävissään, koska opinnäytetyön suunnittelu, laatiminen ja esittäminen perehdyttivät tekijää oman alansa tiedontuottamisprosessiin.

Lopuksi tekijä haluaisi kiittää kaikkia osapuolia ja ihmisiä jotka olivat mukana, tukivat ja ohjasivat tekijää opinnäytetyön prosessin aikana: koulussa, työpaikalla, ystäväpiirissä, sekä erikseen tietoperustan kirjoittajia ja alan ammattilaisia. Heidän avulla tekijästä on (toivon mukaan) tullut pätevämpi osaaja. Kiitos!

Lähteet

Alppisara, L. 2012. Jatkuvuuden hallinta IT-palveluliiketoiminnassa. Luettavissa: https://jyx.jyu.fi/dspace/bitstream/handle/123456789/38110/URN:NBN:fi:jyu-201206271971.pdf?sequence=1. Luettu 19.08.2013

Calder, A. & Watkins, S. 2012. IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Fifth edition. Kogan Page.

COSO. 2013. Sisäisen valvonnan viitekehys COSO uudistunut. Luettavissa: http://www.codeofconduct.fi/sisaisen-valvonnan-viitekehys-coso-uudistunut/. Luettu: 24.07.2013.

HAAGA-HELIA ammattikorkeakoulu 2010. Raporttien ulkoasu ja lähteisiin viittaaminen. MyNet. Opiskelu. Opinnäytetyö amk. Raportointiohjeet. Luettavissa: http://www.haaga-helia.fi. Luettu: 10.04.2013.

HAAGA-HELIA ammattikorkeakoulu 2013.
Ammattikorkeakoulututkinnon opinnäytetyön sisältö ja menetelmät. Raportointityöryhmän ohje. Luettavissa: Opiskelijan extranet > Opiskelu > Opinnäytetyö amk > Raportointiohjeet. Luettu 10.04.2013.

Haatainen, T., Rajakylä, M. 2003. Valtioneuvoston asetus ammattikorkeakouluista 352/2003. Helsinki. Luettavissa: http://www.finlex.fi/fi/laki/alkup/2003/20030352. Luettu 23.04.2013

Hakala, M. 2006. Tietoturvallisuuden käsikirja. Jyväskylä. Docendo Finland Oy.

Haren, V. 2007. Foundations of IT service management: based on ITIL V3. Zaltbommel. The Netherlands.

Holopainen, A., Koivu, E., Kuuluvainen, A., Lappalainen, K., Leppiniemi, J., Mikola, M. & Vehmas, K. 2006. Sisäinen tarkastus. Tallinna.

Iivari, M., Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Tietosanoma. Helsinki.

Julkisen hallinnon tietohallinnon neuvottelukunta JUHTA. Tervetuloa JHS-järjestelmän verkkopalveluun. Luettavissa: http://www.jhs-suositukset.fi/web/guest JHS suositukset. Luettu: 13.6.2013.

Jyväskylän yliopisto. Laadullinen tutkimus. Luettavis-sa:https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus. Luettu: 14.7.2013.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Edita Publishing Oy. Helsinki.

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Talentum Media Oy. Helsinki.

Myrskylän Kunta. 2012. Sisäisen valvonnan ohje. Luettavissa: http://www.myrskyla.fi/index.php?id=29. Luettu 01.08.2013.

Nancy, R. 2004. The Quality Toolbox. Luettavissa: http://asq.org/learn-about-quality/project-planning-tools/overview/pdca-cycle.html. Luettu: 03.05.2013.

Nurmi, K. 2011. Tietoturvallisuuden hallinnan suunnittelu ja toteutus. Luettavissa: http://www.tietoturvatalkoot.fi/Projektiopas.pdf. Luettu: 07.07.2013.

Pickett, S. 2003. The Internal Auditing Handbook. Second edition. John Wiley & Sons. United States.

Pk-yrityksen riskienhallinta. 2000-2009. Yrityksen riskien kartoittaminen. Luettavissa: http://www.pk-rh.fi/tyovalineet/yrityksen-riskien-kartoittaminen.html. Luettu: 04.05.2013

Puhakainen, P. 2010. Suomen turvallisuusalan vuosikirja 2009. Forssan kirjapaino Oy. Forssa.

Sisäiset tarkastajat ry. 2012. Sisäisen tarkastuksen ammattistandardit. Luettavissa: https://na.theiia.org/standardsguidance/Public%20Documents/IPPF%202013%20Finnish.pdf. Luettu: 29.06.2013.

Tietoturvastandardi 2700x –perhe. 2009. SFS-ISO/IEC. Suomen standardisoimisliitto. Helsinki.

VAHTI 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. VAHTI 7/2003. Edita Prima. Helsinki.

VAHTI 2006. Tietoturvallisuuden arviointi valtionhallinnossa. VAHTI 8/2006. Edita Prima. Helsinki.

VAHTI 2007-2013. Tietoturvallisuus. Luettavissa: http://ta.ramk.fi/VAHTI/Sivusto/kayttajan_ohje/011_johdanto1.htm. Luettu: 08.07.2013.

VAHTI 2011. Johdon tietoturvaopas. VAHTI 2/2011. Juvenes Print. Helsinki.

Liitteet

Liite 1. Sanasto

BS 7799 -standardi - Merkitys on vähenemässä pikku hiljaa, sillä sen on sivuuttanut nykyiset 2700x -standardit.

COBIT - Control Objectives for Information and related Technology -viitekehystä voidaan hyödyntää määriteltäessä tietojenkäsittelyn liiketoiminnallisia tavoitteita ja sitä, miten niiden saavuttamista voidaan mitata. COBIT määrittelee tietoturvallisuuden kannalta tärkeitä prosesseja, jotka tuottavat yrityksille tarpeellista informaatiota.

COSO - Tunnetuin sisäisen valvonnan viitekehyksistä, riskinhallinnanmalli. Mallilla on viisi komponenttia: valvontaympäristö, riskien arviointi, valvontatoiminnot, informaatio ja kommunikaatio, seuranta. Viimeisin päivitetty versio on julkaistu toukokuussa 2013, jonka tarkoituksena selkeyttää mallia.

GAISP - Generally Accepted Information Security Principles esittää eri järjestelmäturvallisuuden periaatteita. Viitekehys on pääpainotteisesti tarkoitettu tietolähteeksi järjestelmien ja laitteiden valmistajille sekä käyttäjille. GAISP:n tavoitteena on yhdistää julkisen ja yksityisen sektorin tietoturvaperiaatteet koko maailmassa.

Help Desk (service d) - Tukikeskus on neuvontaa antava yksikkö, joka palvelee asiakkaita esim. konehuollossa.

Henkilöstö - Tehtäviin kuuluu mm. tiedon käsittely, siirtäminen ja säilyttäminen tietoturvaohjeita noudattaen, sekä omien salasanojen hallinta ja turvallinen käyttö. Kunkin työntekijän tulee myös itse huolehtia omasta tietoisuudestaan liittyen tietoturvapolitiikkaan. Jotta tämä onnistuisi, tulisi työntekijän osallistua tietoturvallisuuskoulutuksiin.

IIA - International Standards for the Professional Practice of Internal Auditing on kansainvälinen ammattistandardien johdanto, jonka tarkoituksena on toteuttaa organisaation sisällä tapahtuvaa tarkastusta. Ammattistandardi kuvaa periaatteet, miksi sisäinen tarkastus tehdään, määrittää ajatusmallin tarkastettavien tehtävin suorittamiselle ja kehittämiselle, luo pohjan sisäisen tarkastuksen tuloksen arvioinnille, parantaa toiminnallisten prosessien kehittämistä ja avaa käsitteistöä.

ISF - Information Security Forum kuuluu Kansainväliseen järjestöön, joka on julkaissut Standard of Good Practice for Information Security. Standardin tehtävänä on auttaa käytännönläheisesti tiedonkäsittely-prosessien riskienhallintaa. Standardi on jaettu viiteen tärkeään osa-alueeseen, jossa kukin osa-alue esittää siihen kuuluvia tietoturva-asioita: tietoturvallisuuden hallinta organisaatiotasolla, liiketoimintakriittiset järjestelmät, tietojärjestelmät, tietoverkot, järjestelmäkehitys.

ISO 2700x -standardit - Nämä standardit ovat oleellisimpia ja laajemmin levinneitä ympäri maailmaa. Puhutaan kuitenkin nykyään yleisemmästä ISO 27001 -standardista, joka kattaa tietoturvajohtamis- ja hallintajärjestelmien perustamisen, toteuttamisen, käyttämisen, valvomisen, arvioimisen, huoltamisen ja parantamisen. Standardi auttaa suojaamaan kaikki tietoturva-asiat: tiedot, asiakirjat, koneet, verkot jne. ISO 27001 on

perustettu kansainvälisessä standardointiorganisaatiossa, jota käytetään sertifioinnissa. ISO 27001 korvaa entisen BS 7799 -standardin ja sen monia ominaisuuksia hyödynnetään muiden standardien nojalla, kuten ISO/IEC 17799:2005, ISO 9001 yms.

ITIL - Information Technology Infrastructure Library on suunniteltu kattamaan IT:n tärkeimmät palvelutuotannon toimintatavat. Viitekehyksen prosessit ja palvelut pyrkivät tukemaan tietoturvallisuutta. Yksi tärkeimmistä ja suurimmista prosesseista on tietoturvallisuuden johtaminen, jossa määritellään tietoturvallisuuden taso, missä taas pyritään ehkäisemään riskitilanteita ja korjataan jo aiheutuneita vahinkoja. ITIL pyrkii säännöllisesti tarkastamaan tietoturvallisuuden nykytilan ja raportoimaan siitä. Ko. periaatteissa ja linjauksissa ITIL ei eroa paljoa ISO 2700x -standardien vaatimuksista.

JHS-suositukset - Julkisen hallinnon suositukset kuuluvat valtion- ja kunnallishallinnon tietohallintoon. Kuvaavat yhtenäistä menettelytapaa, määrittelyä tai ohjetta. JHS-järjestelmän painopistealueet: tietojärjestelmien yhteentoimivuus, yhteisten tietovarantojen hyödyntäminen, asiointikäyttöliittymät, tietojen käsittelyyn liittyvä tietoturva ja tietosuoja, palvelujen kehittämistä tukevat hyvät käytännöt.

Järjestelmän pääkäyttäjä - Toimivan tietoturvan toimintaympäristön edellytyksenä on järjestelmän pääkäyttäjän valitseminen. Järjestelmän pääkäyttäjä vastaa systeemien ja sovellusten toimivuudesta ja siitä, että sen tuottama ja käyttämä tieto on varmasti luotettavaa. Pääkäyttäjä saa hallita sovelluksiin liittyviä tietoturvallisuuden käyttöoikeuksia, mutta ei saa päättää niistä. Käyttöoikeuksista voivat päättää vain järjestelmän, tiedon tai prosessin omistaja. Lisäksi järjestelmien pääkäyttäjät ovat vastuussa järjestelmien päivityksistä ja ylläpidosta. Laki yksityisyyden suojasta tulee ottaa huomioon tilanteissa, joissa käsitellään henkilötietoja, esim. sähköpostia. Järjestelmien pääkäyttäjät kuuluvat yleensä tietohallintoon.

NIST - National Institute of Standards and Technology on yhdysvaltalainen organisaatio, joka antaa erilaisia suosituksia ja kuvaa menetelmiä, joilla voidaan vaikuttaa organisaation riskienhallintaan.

OECD - Organisation for Economic Cooperation and Development eli Taloudellisen yhteis-työn ja kehityksen järjestö on ensimmäisiä tietojärjestelmien ja -verkkojen ohjeistusten tekijöitä. Ko. ohjeistuksen tarkoituksena on nostaa etusijalle turvallisuussuunnittelu ja -hallinto, jolloin organisaatiossa tullaan ymmärtämään turvallisuuden tarve. Ohjeistus sisältää yhdeksän periaatetta, joita ovat turvallisuustietoisuus, vastatoimet, vastuullisuus, eettisyys, riskien arviointi, demokratia, turvallisuuden hallinta, turvallisuuden suunnittelu ja uudelleenarviointi.

OLA - Operational Level Agreement on hankintasopimus, jossa määritellään organisaation sisäosastojen väliset vastuut ja päätetään hyödykkeistä ja palveluista, joita toimitetaan.

Prosessin omistaja - Jokaisella liiketoiminnan prosessilla on omistaja, joka vastaa kyseisestä prosessista sekä siitä, että siinä tietoturvallisuus on huomioitu. Prosessin omistajien tehtäviin tietoturvan osalta kuuluu mm. riskikartoitusten tekeminen, prosessin suojaustavasta päättäminen, tietoturvallisuuden ja liiketoiminnan tavoitteiden saavutta-

minen, henkilöstön tietoturvan osaamisen varmistaminen ja ko. asioihin liittyen säännöllinen raportointi ja jatkuva seuranta.

Sarbanes-Oxley Act eli SOX - Kyseinen säännös ohjaa, kuinka taloudellista tietoa tulisi käsitellä organisaatiossa. Säännös ohjaa säilyttämään kaikki tilinpäätöksiä koskevat tiedot missä tahansa muodossa seuraavan seitsemän vuoden ajan. SOX-säännös on saanut alkunsa Yhdysvalloissa, eikä se koske suoraan suomalaisia yrityksiä. Se koskee vain niitä yrityksiä, joiden nimi on Yhdysvaltojen pörssissä SEC:ssä sekä joitakin suomalaisia tytäryhtiöitä, jotka toimivat ulkomailla ja joiden toiminta koskettaa koko organisaatiota. Se sisältää hyviä lähestymistapoja ja käytäntöjä, joiden käyttö on hyödyllistä ja suositeltava tietoturvatyössä.

Sisäinen tarkastus - Pyrkii estämään toiminnan epäkohtia sekä turvaamaan toiminta-edellytyksiä. Varsinainen sisäisen tarkastuksen tehtävä on arvioida mm. tietoturvallisuuden tasoa ja tarkastella organisaation toimintaa tietoturvapolitiikkaan nojaten. Sisäinen tarkastus raportoi kaikki havaintonsa organisaation johdolle. Ulkoisen tarkastuksen pää-tehtävään kuuluu tilintarkastus, eli organisaation tilinpäätöksen, kirjanpidon sekä yhtiön hallinnon tarkastaminen.

SLA - Service Level Agreement on palvelutasosopimus ulkoisen palveluntarjoajan ja organisaation välillä. Siinä käsitellään vastuita palveluiden tuottamisessa.

SVTSL-tietosuojalaki - Määrittelee kenellä on oikeus käsitellä arkaluonteista tietoa, tunnistamistietoja.

Tietohallinto - Tärkeimpiä tehtäviä on toteuttaa tietoturvallisuuden tekninen puoli ja ylläpito, mutta se ei saa päättää järjestelmien tai tietojen suojaustasosta. Siitä päättävät tiedon, prosessien ja järjestelmien omistajat. Tietohallinto yleensä vastaa myös mm. laitetilojen suojaamisesta, tiedonsiirron turvallisuudesta, lokitiedostojen keräämisestä ja säilyttämisestä sekä kulunvalvonnasta ja operatiivisen toiminnon monitoroinnista. Lokitietojen avulla voidaan valvoa organisaation toimintaa ja raportoida siitä organisaation liikkeenjohdolle. Raportoinnissa tulisi ottaa huomioon tunnistamistietojen käsittelyä koskevat määräykset.

Tietojen omistajat - Vastaavat tiedosta, sen laadusta ja käyttötavoista. Yleisesti tiedon omistaja on johtaja tai jonkin tahoinen päällikkö tms. vastaava, vaikka hän ei välttämättä olekaan tiedon tuottaja. Tiedon omistaja kontrolloi, että tieto on luotettavaa ja päättä itse sen, kenellä on oikeus tarkastella ja muokata sitä. Tiedon omistajan on otettava huomioon lainsäädäntöön kuuluva mm. henkilötietolaki, laki yksityisyyden suojasta työelämässä ja SVTSL-tietosuojalaki, jotka määrittelevät kenellä on oikeus käsitellä arkaluonteista tietoa, tunnistamistietoja.

Tietoturvaorganisaatio - Ryhmä, joka on vastuussa mm. tietoturvan operatiivisesta toiminnasta, ja joka yleensä laatii ja turvaohjeet muille liiketoimintayksiköille ja valvoo niiden noudattamista sekä raportoi omalle tai ylimmälle johdolle. Johto taas päättää kuka kuuluu tietoturvaorganisaatioon ja mahdollistaa tarvittavat resurssit tehtävien suorittamista varten.

Tietoturvapäällikkö - Laatii yksikön johtajien kanssa toimintaohjeet, joita jokainen yksikkö noudattaa. Johdon tulee tiedottaa henkilöstölle tietoturva-asioista ja antaa myös heille mahdollisuuden osallistua niiden valmisteluun. Tällöin tietoturvapolitiikka toimii oikein ja asetetut tavoitteet ovat saavutettavissa.

Ulkoinen sidosryhmä - Oma roolinsa organisaatiossa. Johtotaso tai tietoturvapäällikkö vastaa niistä, sillä hänen täytyy osata arvioida ulkopuolisten toimijoiden pätevyys ja työkokemus. Tärkeintä ulkopuolelta ostettavan palvelun tai toiminnon osalta on arvioida oikein tietoturvariskit ja ohjeistaa oman organisaation henkilöstöä.

VAHTI - Valtionhallinnon tietoturvallisuuden johtoryhmä. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä.

Viestintävirasto CERT - Computer Emergency Response Team listaavat verkkosivuillaan tietoa uusista uhista ja julkaisevat ohjeet niiden ennaltaehkäisemisestä ja korjaamisesta.

Liite 2. Liiketoiminnan jatkuvuuden työvälineet (sarja alaliitteitä)
Liite 2.1. Suojattavat kohteet - luettelot ja arviointi

Viimeksi päivitetty: nimi ja pp.kk.vvvv

Muutos: xxx

Arvot&skaalat:

Suojaustaso: 1,2,3,4,5 (1 ylin)

Arvio laadullinen: Korkea, Keskitaso, Matala

Suojattava KOHDE	**Suojaustaso / tärkeysluokka (tärkein ylin)**	**Sijainti**	**Dokumentin sijainti (url, polku, tms)**	**Varmuuskopio (url, polku, tms)**	**Omistaja (rooli tai nimi)**	**Arvo määrällinen (esim Eur)**	**Arvo laadullinen (esim. 'Korkea')**	**Haavoittuvuudet ja riippuvuudet**
Palvelin XX	1	IT-toimittaja1-konesali	http://aalto/docs/HW&virtuals/PalvelinXX-operontiohje.ppt		TH päällikkö	999	Korkea	
Cisco-reititin	1							
Työasemat	3	Toimisto/käyttäjät				20 kpl	Keskitaso	

Liite 2.2. Riskienhallinnan työkalu

Viimeksi päivitetty: nimi ja pp.kk.vvvv

Muutos: xxx

Arvot&skaalat:

Kohteen tärkeysluokka: 1,2,3,4,5 (1 ylin)

Uhan todennäköisyys: Korkea, Keskitaso, Matala

TM-toteutus: Ei mahdollinen, Ei (ei toteutettu), Osittain (toteutettu), Kyllä (täysin toteutettu)

Riskitaso: 1,2,3,4,5 (1 ylin)

Riski	Kohde	Kohteen tärkeys-luokka	Kohteen tyyppi	Uhka	Uhan todennä-köisyys	Turvamekanismi (TM)	TM-toteutus	Riskin vaikutukset	Riskitaso (korkein ylin)
Konesalitoimittaja lopettaa sopimus	Konesalipalvelut, IT-toimittaja1	1	Organisaation saama palvelu	Toimittaja poistuu	pieni	Puitesopimus toisen ko-nesalipalveluntarjoajan kanssa	Ei	Organisaation toimittamat palvelut ei toimi kokonaan	1
		-		Luonnonilmiöt	pieni	Toimitaan kotoa käsin; IT-toimittaja1-SLA:ssa huomi-oitu; Toisen toimittajan kanssa puitesopimus alkaa toimia 3:n päivän sisällä	Osittain	Organisaation toimittamat palvelut tai osa niistä ei toimi	4

Liite 2.3. Turvamekanismit

Viimeksi päivitetty: nimi ja pp.kk.vvvv

Muutos: xxx

Turvamekanismi	Luotu	Muokattu	Muutokset	Vastuu
Tietoturvallisuutta koskevien vastuiden jako	On ollut aina	pp.kk.vvvv	Tarkennettu ja lueteltu jatkuvuussuunnitel-maan	Toimitusjohtaja

Turvamekanismit, jatkokehittämistarpeiden kartoitus

Ohjeet: tehdään nykyisten turvamekanismien (edellinen taulukko) jatkokehittämistarpeiden kartoitus, jonka seurauksena päätetään mahdollisten uusien turvamekanismien luomisesta, olemassa olevien parantamisesta, päällekkäisyyksien ja turhien mekanismien poistamisesta. Tämän vaiheen tuloksena saadaan mahdollisten turvamekanismien luettelo sekä tiedot niiden kustannuksista, hyödyistä ja toteuttamisen tärkeysjärjestyksestä.

Turvamekanismi	Uusi vai muokattava vanha (mikä)	Valmiusaika, päämäärä	Muutokset tai hyödyt (jos uusi)	Vastuu

Liite 2.4. Riskien käsittelysuunnitelma

Viimeksi päivitetty: nimi ja pp.kk.vvvv

Muutos: xxx

Joillakin riskin käsittelytavoilla voidaan käsitellä tehokkaasti useampaa kuin yhtä riskiä (esim. tietoturvakoulutuksen ja -tietoisuuden avulla). Riskien käsittelysuunnitelma määritellään ja siinä selkeästi yksilöidään, missä tärkeysjärjestyksessä yksittäiset riskien käsittelytoimenpiteet toteutetaan ja millainen on

toimenpiteiden aikataulu. Tärkeysjärjestys määritetään eri tavoin, kuten riskien luokittelun ja kustannus-hyötyanalyysin avulla. Silloin Asiakkaan johto päättää turvamekanismien toteuttamisen kustannusten tasapainottamisesta ja budjettivarauksista.

	Prio/nro (ylin korkein)	Riskin käsittelyn päätös ja toimenpiteet	Valmiusaika, pp.kk.vvv	Muutokset (jos vanha riksi) tai hyödyt (jos uusi)	Vastuu	Muutos päivitetty Riskienhallinnan työkaluun, pp.kk.vvv	Arvioitu jäännösriski

Liite 2.5. Luettelo hyväksytyistä riskeistä

Viimeksi päivitetty: nimi ja pp.kk.vvvv

Muutos: xxx

Hyväksytty riski	Perustelu	Kenen päätös	Päätösaika, pp.kk.vvvv	Päivitetty Riskienhallinnan työkaluun, pp.kk.vvv	Huomiot

Liite 2.6. Toipumissuunnitelmien testaus

Viimeksi päivitetty: nimi ja pp.kk.vvvv

Muutos: xxx

Jatkuvuussuunnitelma osa / Riksi / Toipumissuunnitelma	Laajuus tai testauskohteet	Liittyvät dokumentit ja raportit	Testaustavat ja -tiheys	Suoritusajankohta pp.kk.vvvv	Vastuullinen	Tulokset / Parantamisohjeet
Riskienhallinta	Ks. suunnitelman ko. osa	Tämä suunnitelma	Joka tammikuu vuosittain	pp.kk.vvvv	Tietoturvapäällikkö	Ks. päivitetty Riskienhallinnan työkalu
Tulipalo	Toimistotilat	Tämä suunnitelma; testauksen raportti: N:\Aalto\docs\tietoturvatiimi\ToipuminenTulipa	Pöytätestaus, kerran vuodessa	pp.kk.vvvv	Rimma Tarkka	Ks. ko. raportti

		loTest.docx				

Liite 2.7. Yhteystiedot

Viimeksi päivitetty: nimi ja pp.kk.vvvv

Muutos: xxx

Nimi, puhelinnumero, sähköpostiosoite	**Rooli, organisaatio, vastuu**	**Varahenkilö: nimi puhelinnumero, sähköpostiosoite**	**Varahenkilö: organisaatio, vastuu, rooli**	**Huomiot**