Elina Pollari

TIETOTURVARISKIEN HALLINTA ORGANISAATIOISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Pollari, Elina
Tietoturvan ja tietoturvariskien hallinta organisaatioissa
Jyväskylä: Jyväskylän yliopisto, 2021, 54 s.
Tietojärjestelmätiede, Pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tässä tutkimuksessa tarkastellaan tietoturvariskien hallintaa organisaatioissa. Tutkimuksen tavoitteena on tunnistaa ne keskeiset tekijät, jotka yrityksen on huomioitava oman tietoturvallisuuden hallinnassa ja yritykseen kohdistuvien tietoturvariskien hallinnassa.

Tutkimus on toteutettu kirjallisuuskatsauksena, jossa aiemman kirjallisuuden perusteella on pyritty löytämään aiheeseen liittyviä yhteisiä tekijöitä, joiden voidaan katsoa olevan keskeinen osa yrityksen tietoturvan ja tietoturvariskien hallinnan suunnittelussa ja toteuttamisessa. Tutkimuksessa käydään läpi useiden eri tutkijoiden ja kirjoittajien teoksia. Aiempien tutkimusten vertailulla pyritään löytämään yhteisiä tekijöitä eri tutkijoiden välillä. Näiden yhtäläisyyksien avulla pyritään löytämään ne kohdat, joita laajimmin pidetään aiheen kannalta keskeisimpinä toimintatapoina tai ns. parhaina käytänteinä. Tutkimuskysymykseen on pyritty vastaamaan vertailemalla kirjallisuutta niin tietoturvariskien tutkimusten, tietoturvariskien hallinnan standardien ja viitekehysten kautta kuin myös muun tietoturva käytänteiden hallintaa käsittelevän kirjallisuuden kautta.

Tutkimuskysymykseen on vastattu kuvaamalla tietoturvan- ja tietoturvariskien hallinnan kannalta keskeiset toimet, joita yrityksessä tarvitsee suorittaa, sekä avaamalla mitä toimintoja eri osa-alueet pitävät sisällään ja mihin yrityksen tulee kiinnittää huomiota. Tämän tutkimuksen yhtenä havaintona on riskien arvioinnin tärkeyden korostaminen miltei jokaisessa läpi käydyssä kirjallisuudessa. Tarkasteltaessa erikseen jokaista tietoturvan hallinnan osa-aluetta, on miltei jokaisen prosessin alussa suositeltu riskien arviointia. Riskien arviointi antaa yritykselle näkemyksen siitä, millaisia ovat juuri kyseistä organisaatiota uhkaavat riskit. Riskien tunnistamisen jälkeen voidaan lähteä suunnittelemaan niitä toimenpiteitä, joilla yritykset voivat kehittää itselleen toimivan riskienhallintastrategian.

Asiasanat: Riski, Riskienhallinta, Tietoturvariski, Tietoturvan hallinta, Riskienhallinnan elinkaari, Tietoturvan elinkaari, Tietoturva käytänteet

ABSTRACT

Pollari, Elina
Information security and informationsecurity risk management in organisations
Jyväskylä: University of Jyväskylä, 2021, 54 p.
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

This study examines information security and informationsecurity risk management in organizations. The aim of the study is to identify the key factors that a company must take into account in managing its own information security and in managing information security risks in the company.

The study has been carried out as a theoretical study, in which, based on the previous literature, an attempt has been made to find common factors related to the topic, which can be considered a key part in the planning and implementation of a company's information security and security risk management. The study goes through several different research and written literature. A comparison of previous studies seeks to find common factors between different researchers. These similarities aim to identify those points that are most widely considered to be the most important courses of action on the subject. An attempt has been made to answer the research question by comparing the literature through the literature on information security research, information security risk management and information security policy management.

The research question has been answered by describing the key actions that the company needs to perform in terms of information security and information security risk management, as well as by opening up what functions the different areas include and what the company should pay attention to.

One findings of this study is the emphasis on the importance of risk assessment in almost every literature reviewed. When looking at each aspect of security management separately, a risk assessment is recommended at the beginning of almost every process. The risk assessment gives the company an idea of the risks facing the organization in question. Once the risks have been identified, it is possible to start planning the measures that the company has to hedge against the risks.

Keywords: Risk, Risk Management, Security Management, Risk Management Lifecycle, Security Lifecycle, Information security policy

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Stephen V. Flowerdayn ja Tite Tuyikezen (2016) artikkelissa todetaan organisaatioiden tietoturvan tarpeen perustuvan siihen tosiasiaan, että organisaatiot ovat nykyään yhä enemmän riippuvaisia tietotekniikasta (IT). IT tukee organisaatioiden jokapäiväistä toimintaa. Doughty ja Griego (2005) toteavat, että "tietotekniikkaa olisi pidettävä keinona lisätä organisaation päätöksentekoprosessia tukevan tiedon saatavuutta, nopeutta ja kattavuutta". Riippuvuus tietotekniikasta on kuitenkin valitettavasti lisännyt mahdollisia uhkia organisaatioiden tietovaroille (Flowerday, S., Tuyikeze, T., 2016).

Toisin kuin monet muut liiketoiminnan haasteet, tietoturvan riskienhallinta on edelleen ongelma, johon ei ole helppoa ratkaisua. Se vaatii johdolta jatkuvaa huomiota, kykyä sietää huonoja uutisia sekä järjestelmällistä ja selkeää viestintää. Vaikka keskeisiä tietoturvauhkia on selvitetty kattavasti lukuisissa erinomaisissa lähteissä, yritysjohdon tueksi soveltuvaa tietoturvan hallinnan aineistoa on edelleenkin saatavilla vähänlaisesti (ICC, 2015).

Perinteisesti tietoturvan hallinta on nähty hyvin teknisestä näkökulmasta. Tutkimusten mukaan kuitenkin suurin osa toteutuneista turvallisuusrikkomuksista johtuu organisaation henkilökunnan väärinkäytöksistä. Tästä voi vetää johtopäätöksen, että tietoturvan hallinnan pitää kattaa laajemmat osa-alueet organisaatiossa kuin vain tekninen turva. Organisaatioilla tulee olla kyky hallita teknisen puolen lisäksi myös henkilöstön kykyä toimia tietoturvallisesti omassa työssään. Tietoturvan hallinta liittyy ensisijaisesti strategisiin, taktisiin ja operatiivisiin kysymyksiin, jotka liittyvät organisaation tietoturvaohjelman suunnitteluun, analysointiin, toteuttamiseen ja ylläpitoon (Choobineh, J., Dhillon, G., Grimaila M.R., Rees, J. 2007). Organisaatioille tämä tarkoittaa sitä, että niiden tulee pystyä arvioimaan oma tilanteensa ja suunnitella organisaation tarpeisiin sopivat turvallisuuskäytännöt, joihin henkilökunta sitoutuu.

Yrityksillä voi kuitenkin olla haasteita ymmärtää tietoturvariskien hallinnan merkitystä, sillä tietoturvariskien auditointi ja hallinta ei ole käsitteenä selkeä kaikille. Lisäksi käsitteiden ymmärtäminen voi olla haastavaa, sillä ne tapahtuvat hyvin vahvasti abstraktilla tasolla, jolloin auditoinnin käsinkosketeltavaa merkitystä ei välttämättä nähdä organisaatioissa tärkeäksi. Aiemmassa

kirjallisuudessa tietoturvan hallinta ja tietoturvariskien hallinta on usein kirjoitettu toisistaan erillään. Tietoturvan hallinta sisältää myös tietoturvariskien hallinnan; riskien ymmärtämisen avulla voidaan paremmin rakentaa tietoturvallisuutta organisaatioissa. Tämä innoitti minua tutkimaan, kuinka yritykset voivat kehittää itselleen toimivan strategian hallita tietoturvariskejä.

2 TUTKIMUSMENETELMÄT

Tutkimukseen kuuluu yhtenä keskeisenä kysymyksenä tieteellisen metodin arviointi. Tähän on monia perusteita. Yhtäältä metodia edellytetään joidenkin mukaan, koska peremmiltään tutkimus on järjestelmällistä ja järkiperäistä tiedonhankintaa. Tieteenfilosofian oppikirjan mukaan, tieteellisen tutkimuksen järjestelmällisyys ja järkiperäisyys toteutuvat vain siten, että tiede käyttää tieteellistä menetelmää. Tutkimuksessa on noudatettava tieteelliseen työhön kuuluvia periaatteita – menetelmän tulee ohjata tutkimusta. (Haaparanta, L., Niiniluoto, I. 1986. s. 11–12) Toisaalta ei ole yhtä ”tieteellistä menetelmää” (Siponen et al. 2021) ja arvaus, erehdys ja sattuma näyttelevät myös osaa isossa osassa tieteellisiä löydöksiä (Siponen & Klaavuniemi 2020).

Tämä tutkimus toteutetaan teoreettisen tutkimuksen menetelmillä aikaisempien tutkimusten ja kirjallisuuden pohjalta suoritettavana kirjallisuuskatsauksena. Kuvaileva kirjallisuuskatsaus on yksi yleisimmin käytetyistä kirjallisuuskatsauksen perustyypeistä. Sitä voi luonnehtia yleiskatsaukseksi ilman tiukkoja ja tarkkoja sääntöjä. Käytetyt aineistot ovat laajoja ja aineiston valintaa eivät rajaa metodiset säännöt. Tutkittava ilmiö pystytään kuitenkin kuvaamaan laaja-alaisesti ja tarvittaessa luokittelemaan tutkittavan ilmiön ominaisuuksia. Tutkimuskysymykset ovat väljempiä kuin systemaattisessa katsauksessa tai meta-analyysissä. Kuvaileva katsaus – joskus nimityksenä on traditionaalinen kirjallisuuskatsaus – toimii itsenäisenä metodina, mutta sen katsotaan myös tarjoavan uusia tutkittavia ilmiöitä systemaattista kirjallisuuskatsausta varten. Metodisesti kevyin kirjallisuuskatsauksen muoto on narratiivinen kirjallisuuskatsaus. Sen avulla pystytään antamaan laaja kuva käsiteltävästä aiheesta, tai kuvailla käsiteltävän aiheen historiaa ja kehityskulkua. Kuvailevana tutkimustekniikkana narratiivinen katsaus auttaa ajantasaistamaan tutkimustietoa, mutta ei tarjoa varsinaista analyyttisintä tulosta. (Salminen, A. 2001. s.6) Erityisesti tietojärjestelmätieteen menetelmäluokitteluissa tässä käytetty kirjallisuuskatsaus on luonteeltaan käsiteanalyyttista tutkimusta (Siponen 2002; Järvinen 2004)

Käytettävä kirjallisuus koostuu tieteellisistä artikkeleista tutkimuksista sekä teoksista. Kirjallisuutta on kerätty mm. Google Scholarin kautta, Jyväskylän yliopiston JykDok tietokannasta sekä tieteellisiä artikkeleita julkaisevien yhteisöjen verkkosivuilta kuten IEEE. Kirjallisuuden ja tutkimusten kautta pyritään rakentamaan selkeä näkemys tietoturvariskien hallinnasta organisaatioissa.

Aiheeni on tietoturvariskien hallinta yrityksessä, miten organisaatiossa voidaan kehittää sille sopiva tietoturvariskien hallintastrategia? Riskienhallinta on kriittinen osa tietoturvaa. Se keskittyy tunnistamaan, analysoimaan ja varautumaan riskeihin, jotka ovat ominaisia kullekin yhtiölle. Teoksia ja tutkimuksia on haettu seuraavilla hakusanoilla: tietoturvariskien hallinta, information security risk management, tietoturva, information security, riskienhallinta, risk management, tietoturvan hallinta, information security management.

.

3 RISKIN MÄÄRITELMÄ

Tietotekniikka liittyy nykyään tiiviisti lähes kaikkeen yhteiskunnan, yritysten ja yksityisten ihmisten toimintoihin. Ihmiset joutuvat luottamaan erilaisten tietoteknisten laitteiden toimivuuteen ja käytön turvallisuuteen. Tietoverkkoihin liitettyjä laitteita löytyy jatkuvasti yhä enemmän, sillä nykyteknologian avulla mikrosiruja voidaan asentaa yhä pienempiin laitteisiin. Mitä laajemmin tietotekniikka on käytössä, on sitäkin tärkeämpää ymmärtää siihen kohdistuvat riski (Myllynen, 2002).

Riskien hallinnan näkökulmasta on oleellista ymmärtää mitä käsitteellä riski tarkoitetaan. Koska riski on abstrakti käsite, sille löytyy useita erilaisia tulkintoja. Tässä työssä riskiä tarkastellaan tieturvallisuuden näkökulmasta. Evan Wheelerin (2011, s. 22) mukaan "tietoturva-alalla riskien hallinta liittyy arkaluonteisiin tietoihin ja kriittisiin resursseihin liittyvien riskien hallinnasta". Oxford Learner's Dictionary (2020) selittää riskin olevan "mahdollisuus, että jotain pahaa tapahtuu jossain vaiheessa tulevaisuudessa; tilanne, joka voi olla vaarallinen tai jolla voi olla huono tulos”. IRM (Institute of Risk Management) käyttää ISO / IEC-opasta 73 riskin määrittelemiseksi seuraavasti: "Riskit voidaan määritellä tapahtuman todennäköisyyden ja sen seurausten yhdistelmänä" (IRM, 2002). Vladimirov, Gavrilenko & Michaijlowski käyttävät riskien tulkintaan NIST Specials Publication 800–30 määrettä: “Riski riippuu todennäköisyydestä, jonka mukaan tietty uhka käyttää tiettyä mahdollista haavoittuvuutta sekä kyseisen haittatapahtuman seurauksista organisaatiolle. “(Vladimirov, Gavrilenko, Michajlowski. 2014 s.288).

Riskeille löytyy paljon enemmän määritelmiä, mutta yksi yhteinen asia kaikille niille on. Kaikki tulkinnat ehdottavat, että vaikutus tapahtuman jälkeen on negatiivinen. Riskin ottaminen voi johtaa myös positiiviseen lopputulokseen. Esimerkiksi arvan ostaminen on riski, mutta saatat päätyä voittamaan paljon rahaa. Mutta Hopkin myös toteaa, että yleensä riskit määritellään parhaiten keskittymällä riskeihin tapahtumina (Hopkin, P. 2017 s.15–17) Eri standardit määrittelevät riskit hieman toisistaan poiketen. Hopkin on listannut muutamien yleisimpien standardien määritelmät riskeistä:

- ISO Guide 73/ ISO 31000 - Epävarmuuden vaikutus kohteisiin. Vaikutus voi olla positiivinen, negatiivinen tai poikkeama odotetusta. Riski kuvataan usein tapahtumalla, olosuhteiden muutoksella tai seurauksena
- Institute of Risk Management (IRM) - Riski on tapahtuman todennäköisyyden ja sen seurausten yhdistelmä. Seuraukset voivat vaihdella positiivisista negatiivisiin
- Orange Book from HM Treasury- Epävarmuus lopputuloksesta altistus alueella, joka johtuu vaikutuksen ja mahdollisen tapahtuman todennäköisyyden yhdistelmästä

- Institute of Internal Auditor - Epävarmuus tapahtumasta, jolla voi olla vaikutusta tavoitteiden saavuttamiseen. Riski mitataan seurausten ja todennäköisyyden perusteella. (Hopkin, P. 2017 s.16)

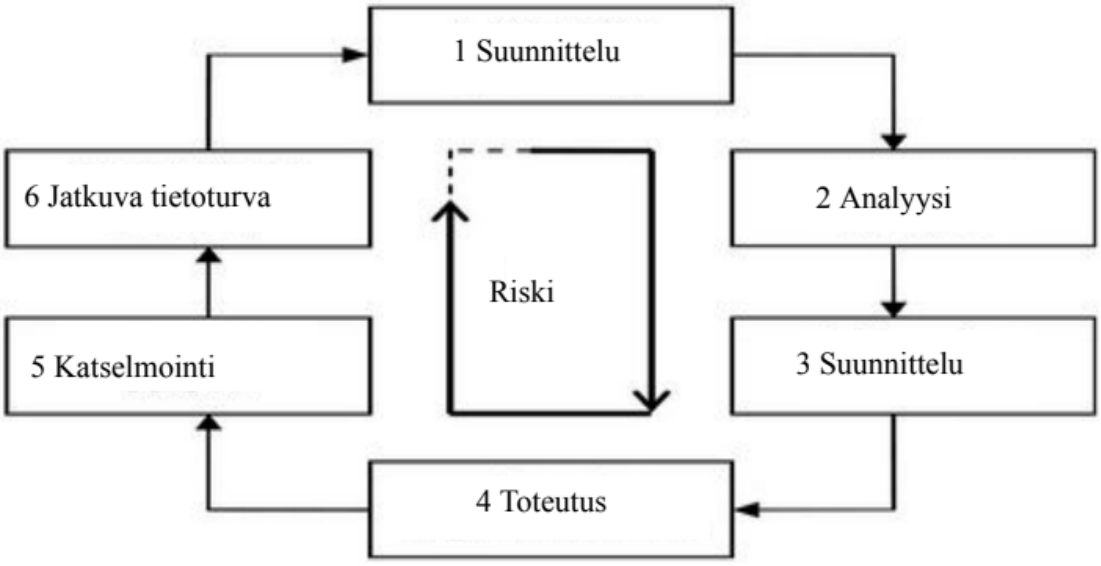
4 TIETOTURVA ORGANISAATIOISSA

Tietoturvan tavoitteena on oltava resurssien luottamuksellisuuden, eheyden, saatavuuden ja vastuullisuuden varmistaminen. Haluttu varmuuden taso vaihtelee organisaatioiden, toimialojen ja ehkä jopa saman organisaation osastojen välillä. Ei ole olemassa yhtä ainoaa lähestymistapaa tai standardia, joka koskisi kaikkia. Tietoturva-ammattilaisten tulee tietää kuinka mitata organisaation riskinsietokykyä, soveltaa turvallisuusstandardien takana olevaa tarkoitusta kussakin tilanteessa ja tasapainottaa valvonnan kustannukset potentiaalisen riskialtistuksen vähentämiseen (Wheeler, E. 2011. s. 29).

Yrityksillä esiintyy jonkin verran haluttomuutta käyttää rahaa tietoturvan hallintaan, sillä arvon asettaminen turvallisuudelle on vaikeaa. Aiheesta on tehty tutkimuksia, joiden mukaan arvo voidaan laskea rahallisen menetyksen kautta. Esimerkiksi yrityksen internet tietoturvaloukkauksesta ilmoittaminen alentaa osakkeiden arvoa keskimäärin 2,1 % kahden päivän sisällä ilmoituksen tekemisestä (Goodman, S., Straub, W. S., Baskerville R. 2008. s.viii).

4.1 Tietoturvan elinkaari

Raggadin (2010, s. 68) mukaan tietoturvan elinkaari käsittää kuusi vaihetta.



KUVIO 1 Tietoturvan elinkaari

- Suunnittelu: suunnittelu on perusta turvallisuusohjelmien kehittämiselle. Suunnittelun tulisi olla ylemmän johdon hyväksymä, sen on noudatettava yrityksen turvallisuuspolitiikkaa ja noudatettava organisaation strategista suunnitelmaa (Raggad, 2010, s.69).
- Analyysi: Turvallisuusanalyysin tavoitteena on tietoturvan elinkaaren aikana määritellä suojausvaatimukset, joita tarvitaan kohdetietojen riittävään suojaamiseen (Raggad, 2010, s. 75).
- Muotoilu: Suojauksen muotoilun tarkoituksena on suunnitella tietoturva kohdetiedoille määriteltyjen turvallisuustavoitteiden saavuttamiseksi (Raggad, 2010, s.93).
- Toteutus: Tämä vaihe koostuu riskilähtöisen turvallisuusohjelman toteuttamisesta (Raggag, 2010, s.99).
- Katselmointi: Tämän vaiheen tarkoituksena on varmistaa, että kohdetietojen omistaja hyväksyy ehdotetun turvallisuussuunnitelman (Raggad, 2010, s. 100).
- Jatkuva tietoturva: Tarkoittaa jatkuvaa seuranta, jonka tarkoituksena on varmistaa, että turvallisuusriski pysyy hyväksytyllä tasolla (Raggad, 2010, s. 101).

4.2 C-I-A-A mallin vaatimukset

Tietoturvan hallinta suojelee tiedon neljää eri elementtiä C-I-A-A mallin mukaisesti. Nämä elementit ovat tiedon luottamuksellisuus, eheys, saatavuus ja aitous.

C-I-A-A mallin elementit:

- Luottamuksellisuus (engl. Confidentiality): Varmuus siitä, että tietoja ei paljasteta luvattomille henkilöille, prosesseille tai laitteille.
- Aitous/autenttisuus (engl. Integrity): Suojaus tietojen luvattomalta luomiselta, muokkaamiselta tai tuhoamiselta
- Saatavuus (engl. Availability): Reaaliajassa tai tietyssä määritellyssä ajassa luotettava pääsy tietopalveluihin luotettaville käyttäjille
- Vastuullisuus (engl. Accountability): Toiminnan jäljittäminen tai kyky jäljittää toiminnasta vastuulliset osapuolet (Wheeler, 2011, s.31)

C-I-A-A malli ei sisällä käsitteitä "pääsyn hallinta" (engl. access control) sekä autentikointi (engl. authentication), sillä ne ovat Wheelerin (2011, s 31–32) mukaan keinoja saavuttaa turvallisuutta sen sijaan, että ne olisivat itse tietoturvassa tarkoitettuja tiedolle asetettuja vaatimuksia.

Erityisesti tietoturvan hallinnassa annetaan painoarvoa yhteiskunnallisesti merkittäville asioille kuten yksityisyyden, digitaalisen identiteetin ja henkisen omaisuuden suojaamiselle. Tietoturvan hallinta sisältää dynaamisia mittausjärjestelmiä, joiden avulla suojellaan dataa, tietoa ja tietojärjestelmiä luvattomalta

käytöltä tai tahattomilta keskeytyksiltä. Luvaton käyttö tai tahattomat keskeytykset voivat johtua ihmisen aiheuttamasta toiminnasta tai luonnollisista uhista. Näille systemaattisille teknisille ja organisatorisille menetelmille on käytössä monia eri kategorioita. Tietoturvan varmistaminen on erottamattomasti sidoksissa riskienhallintaprosessiin; täydellistä turvallisuutta ei ole, ja turvallisuuspolitiikassa ja prosessissa on priorisoitava ja hallittava riski riippuen sen todennäköisyydestä ja haittatapahtumien mahdollisista vaikutuksista yritykselle. (Goodman, S., ym. 2008. s.viii).

Organisatorisen näkökulman tutkiminen tietoturvallisuuden hallinnassa voi ottaa useita eri suuntia. Uusia teoria pohjaisia metodeita riskien arvioinnissa pyritään kehittämään, jotta voidaan huomioida tietoturvaan vaikuttavat riskitekijät. Samalla pyritään huomioimaan menetelmiä, joilla riskeihin vastataan sekä luomaan kustannushyöty analyysejä riskien hallinnassa. Organisaatioiden tulee suojautua tiedon menetykseltä huolimatta siitä, onko menetyksen syynä terroristi tai pyörremyrsky. Molemmat voivat yhtä lailla kaataa organisaation tietojärjestelmät. (Goodman, S., ym. 2008. s.6).

4.3 Tietoturvan hallinnan avulla suojellaan yritykselle tärkeää tietoa

Koska tietoturva-alalla tieto tai data on suojattava voimavara, on myös tärkeää saada käsitys niistä ominaisuuksista, joita riskienhallinta yrittää suojata. Yrityksille tietoturvariskien hallinta on välttämätöntä, sillä tieto on yksi arvokkaimmista asioista, joita yrityksillä on. Tietotekniikka kehittyy nopeasti, ja tietoa on hallittava yhä haastavammissa ja monimutkaisemmissa ympäristöissä (Hopkin, 2017, s. 15). Raggadin (2010, s.6) mukaan tiedolla on erityinen merkitys yrityksen liiketoiminnan arvon muodostamisessa. Raggad (2010, s.6) huomauttaa myös, että tiedoille on erityisiä vaatimuksia. Tietojen on oltava tarkkoja, täydellisiä ja ajankohtaisia, jotta niillä voidaan luoda arvoa liiketoiminnassa. Yrityksen hallitsemat tiedot ovat myös kilpailuetujen perusta.

5 RISKIT YRITYKSEN ERI TASOILLA

Yhä useampi yritys toimii nykyään verkossa tai pilvessä. Tämä tarkoittaa sitä, että yhä enemmän arvokasta tietoa liikkuu verkossa. Nykyinen teknologia mahdollistaa yrityksille mahdollisuuden tuottaa uutta, tavoitella uusia markkinoita ja tuottaa tehokkaita ratkaisuja, jotka hyödyttävät asiakasta. Mahdollisuuksien kasvu tarkoittaa yrityksille myös uusia haasteita. Yritysten tulee sopeutua kaikkialle ulottuvien tuotteiden ja palvelujen toimittamiseen tarvittavien viestintäympäristöjen ja tietovirtojen suoriin ja epäsuoriin vaikutuksiin. Yrityksissä on käytössä yhä enemmän tietotekniikkaa. Uusia tietoteknisiä ratkaisuja myös syntyy jatkuvasti ja niitä otetaan käyttöön, ymmärtämättä, että tällöin myös riskit tulee tarkastella uudelleen (ICC, 2015).

5.1 Riskien luokittelu

Riskit vaihtelevat aina kohteen mukaan, eikä itse riski ole aina sama kaikille. Riskit voivat kertyä eri lähteistä, ja niiden vaikutukset vaihtelevat suuresti. Tämä aiheuttaa sen, että riskienhallinnan ajattelun aloittamiseksi sinun on tiedettävä riskit ja niiden vaikutukset yritykseen. Riskien tunteminen on olennaista riskienhallinnassa, joten ne on kuvattava tietoturvan elinkaaren alussa.

Hopkins jakaa riskit neljään luokkaan:

- Noudattamisriskit (tai pakolliset riskit, engl. compliance risks)
- Vaaralliset (tai puhtaat, engl. hazard risks) riskit
- Hallinnan (tai epävarmuuden, engl.control risks) riskit
- Mahdollisuusriskit (tai spekulatiiviset, engl. opportunity risks) riskit (Hopkins, P. 2017. s.17)

Kaikilla näillä riskeillä on erilaiset tulokset ja ominaisuudet. Organisaatiot pyrkivät minimoimaan pakolliset riskit, vähentämään vaarallisia riskejä, hallitsemaan valvontariskejä ja omaksumaan mahdollisuuksien riskit (Hopkins, P. 2017 s.17). Hopkins tarkastelee riskien hallintaa yleisesti liiketoiminnan kannalta, ei vain tietoturvallisuuden näkökulmasta. Hopkinsin riskien jako ilmenee kuitenkin myös tietoturvallisuuden- ja sen riskien hallinnassa.

5.1.1 Compliance risks eli noudattamisriskit

Yritysten toimintaa säädellään useiden eri tahojen kautta. Joillain aloilla valvonta on hyvinkin tiukkaa ja liiketoiminta sektorilla voi olla oma toimintaa tarkastava elin. Toimialoja koskevien alakohtaisen säännöstelyn lisäksi Suomessa astui

voimaan EU:n yleinen asetus GDPR (General Data Protection Regulation) 25.5.2018. Asetuksen myötä yrityksille syntyi erityinen tarve tarkistaa oman yrityksensä tietoturvan taso. GDPR määrittelee tarkasti, kuinka yritysten tulee säilyttää ja käsitellä yksityisten henkilöiden tietoja. Tiedon säilyttämistä ja käsittelyä koskevien säädösten mukana tuli myös tiedon turvaamiseen liittyviä vastuita. GDPR myös määrittelee yrityksille tiedonantovelvollisuuden, jos yrityksen tietoturvaa on loukattu, tai jos asiakkaiden henkilökohtaisia tietoja on vuotanut julkisuuteen. Tietoturvarikkomuksista voidaan määrätä myös sakkoja, jotka voivat olla liiketoiminnasta riippuen todella mittavia. (EU:n GDPR info, 2020)

Deloitten (2020) tekemästä tutkimuksesta käy ilmi, että noudattamisriskit ovat yksi kolmesta eniten huolestuttavimmista riskeistä seuraavan kahden vuoden aikana. Erityisesti organisaatioilla oli huoli tiukentuvien sääntöjen ja määräysten vaikutuksesta liiketoiminnan kuluihin, mutta myös vaadittavan dokumentoinnin sekä toiminnan oikeellisuuden osoittamisen aiheuttamista kustannuksista.

5.1.2 Hazard risks eli vaaralliset riskit

Vaaralliset riskit ovat ehkä riskeistä helpoiten ymmärrettävissä, vaaralliset riskit ovat suuri uhka yrityksen liiketoiminnan kannalta. Hopkin (2017, s. 42) toteaakin, että "vaarallisten riskien esiintymislaajuus tulee tunnistaa tarkasti. Vaaralliset riskit voivat aiheuttaa suunnittelemattomia keskeytyksiä organisaation toiminnassa". Valtiovarainministeriö (2010) listaa näiden riskien liittyvän erityisesti toiminnan tavoitteisiin, toiminnan suunnitteluun ja organisointiin, päätösten toimeenpanoon, henkilöstöön, prosesseihin, hankintoihin, sopimuksiin, laatuun, asiakkaisiin, toimitiloihin, työvälineisiin, teknologiaan, tiedonhallintaan, tietojärjestelmiin ja tietoturvaan.

5.1.3 Control risks eli hallinnan riskit

Raggard (2010, s. 283) jakaa organisaation teknisen arkkitehtuurin neljään osaan. Jokaisella osalla on omat vaatimukset riskien suhteen.

- Fyysinen turvallisuus liittyy esteisiin, joilla estetään tietotekniikan ja laitteiden luvaton käyttäminen. Hyökkäyksen sattuessa, sen onnistumisen mahdollisuuden tulisi olla pieni ja kiinnijäämisen riski suuri. Fyysinen turvallisuus kattaa laajasti kulunvalvonnan, fyysisen pääsyn järjestelmään, paloturvallisuuden, apuohjelmien tukemisen, datan kaappaamisen, mobiilit ja kannettavat laitteet jne. (Raggad, 2010, s. 283)

- Verkon turvallisuus - Hyvin suunniteltu ja toteutettu verkkoarkkitehtuuri takaa hyvin saatavilla olevan, turvallisen, skaalautuvan, hallittavan ja luotettavan palvelun. Jos yrityksellä on useita verkkoja, tulee jokaisen niistä toimivuus tarkastella erikseen. Lisäksi tulee varmistua siitä, että

tärkeimmät verkon osat ovat suojattuja turvattomilta verkoilta. Yrityksen sisäinen verkkopuolustus tulisi toteuttaa verkon suunnittelun, langattoman verkon turvallisuuden ja turvallisuusprotokollien avulla, jotta vain luotettavat ja tunnistetut tietokoneet voivat kirjautua verkkoon. (Raggad, 2010, s. 283)

- Sovellusten turvallisuus - Sovellukset ovat olemassa kaikkialla yrityksen systeemeissä, joten kun arvioidaan sovelluksen turvallisuutta, tulee ajatella koko organisaation ympäristöä. Sovellusten turvallisuus tulisi toteuttaa siten, että sovellusta käytettäessä sillä on vain hyvin vähän oikeuksia muuhun ympäristöön. Lisäksi sovellusten tulisi olla niin hyvin suojattu, että niihin kohdistuu mahdollisimman vähän altistumista. (Raggad, 2010, s. 283)

- Datan turvallisuus. Data on yrityksen tärkein resurssi, sillä tuottaa yrityksen tiedot. Yleensä asiakastasolla data on säilötty paikallisesti ja on hyvin altis hyökkäyksille. Dataa voidaan suojata erilaisin kryptografian menetelmin, mutta suosituin suojauskeino on yhä varmuuskopioiden ottaminen. (Raggad, 2010, s. 283)

5.1.4 Kyberturvallisuus riskit

Raggardin (2010) tekemässä jaossa ei ole erikseen korostettu kyberturvallisuus riskejä. Deloitten (2020) tekemän tutkimuksen mukaan kyberturvallisuus riskit ovat kuitenkin alati kasvavaa uhka yrityksille. Tutkimukseen vastanneista yrityksistä 41 % oli sitä mieltä, että kyberturvallisuus riskit ovat yksi kolmesta suurimmasta riskistä tulevaisuudessa. Näistä 16 % katsoi kyberturvallisuus riskien olevan kaikkein suurin huolenaihe tulevaisuudessa. Tästä huolimatta ainoastaan 32 % vastaajista katsoi yrityksen olevan hyvin tai erittäin hyvin varautunut kyberturvallisuus riskeihin.

Deloitten (2020) tutkimuksesta selviää myös, että yrityksillä on haasteita erilaisten kyberturvariskien hallinnassa. Organisaatiot kokivat onnistuvansa parhaiten (51 %) häirintä hyökkäysten hallinnassa, seuraavaksi tulivat taloudellisten menetysten ja petosten hallinta (51%), asiakkaista johtuvat kyberturvariskit (47%) ja arkaluontoisen datan menetys (46%). Muilla kyberturvallisuus riskeillä hallinta koettiin vähemmän onnistuneeksi. Vain 38 % organisaatioista koki hallitsevansa organisaation sisäpuolelta tulevat uhat. Seuraavaksi eniten koettiin pystyä hallitsemaan kolmannen osapuolen aiheuttamia riskejä 35 %, valtion taholta tulevia riskejä 35 %, hakkereiden hyökkäyksiä 33 % ja tuhoisia hyökkäyksiä 36 %.

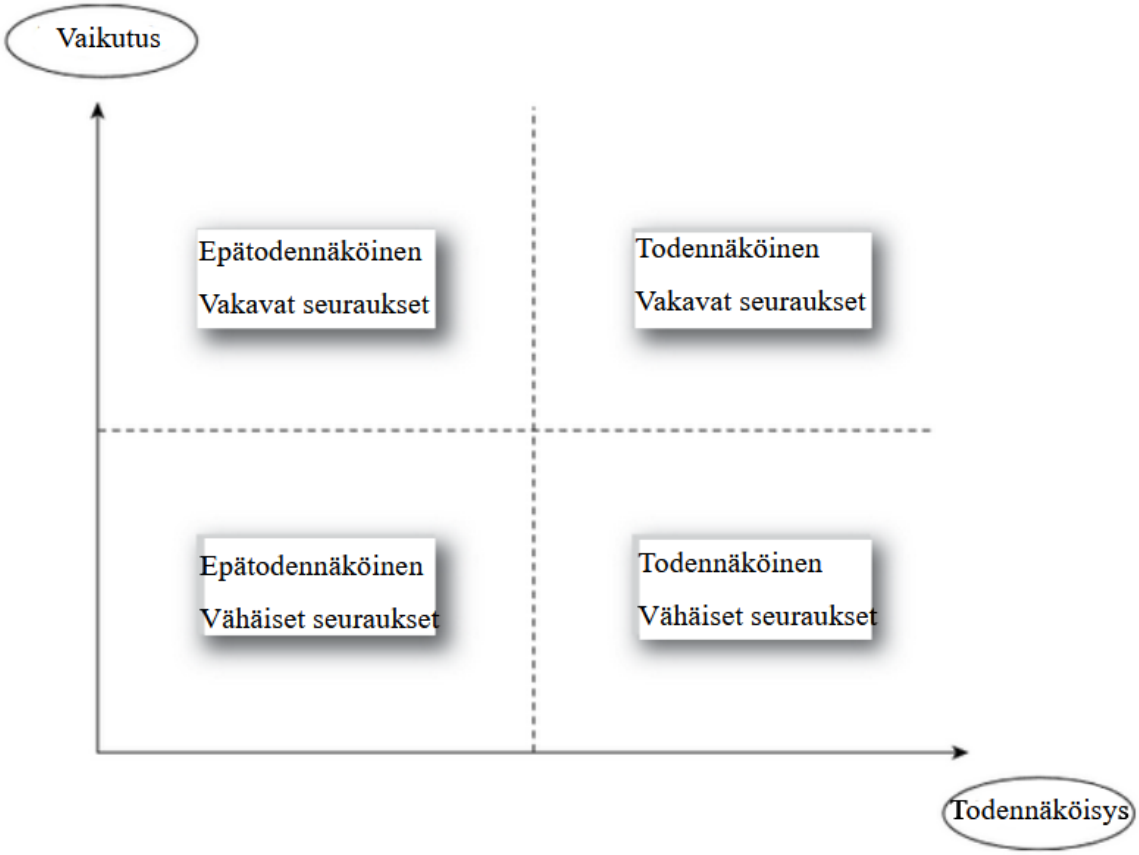
5.2 Riskiherkkyys

Riskiherkkyydellä tarkoitetaan sitä, millainen vaikutus riskillä olisi toteutuessaan organisaation liiketoimintaan. Riskin herkkyyttä arvioitaessa tulee huomioida tarkasteltavan resurssien yleiskuva, toiminnot ja ominaisuudet, siihen liittyvien tietojen (datan) tietoturva luokitus, kriittisyys organisaation toiminnan kannalta, resursseihin liittyvät lait ja määräykset sekä käyttäjäyhteisö. Wheeler huomauttaa myös, että korkean herkkyyden resursseja tulisi arvioida useammin kuin matalan riskin resursseja (Wheeler, E. 2011. s. 65).

Riskin taso	Kriteerit
Matala	Matalan tason riskin suhteen tehdyt kompromissit ovat yleensä rajoitettuja ja yleisesti hyväksyttäviä organisaatiolle. Matalan tason riskeillä on yleensä vähäiset vaikutukset rahallisesti sekä toiminnan kannalta. Vaikutuksiltaan vähäinen organisaation normaaleihin toimintoihin.
Kohtalainen	Kohtalaiseen riskiin liittyvät kompromissit ovat marginaalisesti hyväksyttävissä. Riskillä voi olla joitain seurauksia rahallisesti, toiminnan tai maineen kannalta. Normaalit toiminnot voivat heikentyä huomattavasti, lisäksi riski voi vaikuttaa myös niiden velvoitteiden hoitamiseen joista on sovittu sopimuksilla jonkin osapuolen kanssa.
Korkea	Korkeatasoiseen riskiin liittyviä kompromisseja ei voida hyväksyä. Ne johtavat huomattaviin rahallisiin, tuotannollisiin ja maineeseen liittyviin menetyksiin. Kyky suorittaa normaaleita toimintoja heikkenee huomattavasti. Voi johtaa siihen, ettei voida noudattaa voimassa olevia lakeja. Myös yleinen luottamus yritykseen voi kärsiä.

KUVIO 2 Riskin herkkyystasoa kuvaava kaavio

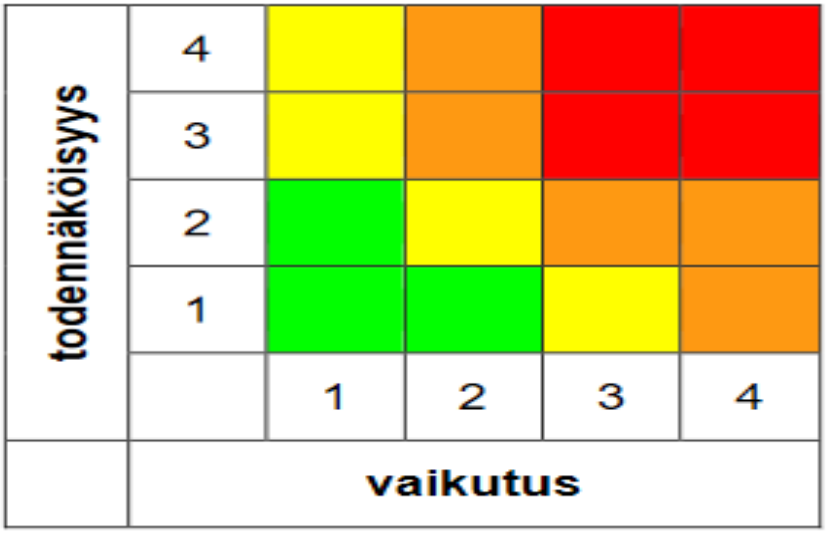
Wheeler (2011, s. 65) tarjoaa asteikon yrityksen riskiherkkyyden arvioimiseksi. Ymmärrettävästi yritykset haluavat välttää korkean tason riskit.



KUVIO 3 Riskin todennäköisyyttä ja vaikutusta kuvaava kaavio

Hopkin tuo uuden ulottuvuuden riskiherkkyyden arviointiin. Hän toteaa, että myös riskin todennäköisyys ja vaikutuksen merkitys tulisi ottaa huomioon (Hopkin, 2017, s. 21.) Hän sanoo myös, että nämä voidaan parhaiten osoittaa käyttämällä riskimatriisia. Hän painottaa matriisin käyttöä arvioinnissa. ”Riskimatriiseja voidaan tuottaa monissa muodoissa. Riippumatta siitä, missä muodossa riskimatriisia käytetään, se on erittäin arvokas työkalu riskienhallinnan ammattilaiselle " (Hopkin, 2017, s. 21).

Valtiovarainministeriö (2010) suosittelee vastaavan riskimatriisin käyttöä kuin Hopkin. Valtiovarainministeriön matriisisissa riskin kriittisyyttä on korostettu värein, jotka auttava hahmottamaan riskin merkittävyyttä ja tarvittavia toimenpiteitä.



KUVIO 4 Valtiovarainministeriön riskimatriisi

Riskitasosta voidaan johtaa käsittelyn tarve, joka on esitetty kuviossa 5.

Taso	Käsittelyn tarve
Kriittinen riski (riskiluku 9-16)	• vaatii yleensä välittömiä toimia • edellyttää jatkuvaa seurantaa
Merkittävä riski (riskiluku 4-8)	• tehtävä suunnitelma riskin pienentämiseksi • seurattava
Kohtalainen riski (riskiluku 3-4)	• ei välttämättä tarvita toimenteitä • seurattava riskiä ja sen mahdollista kehittymistä
Matala riski (riskiluku 1-2)	• ei vaadi akuutteja toimenpiteitä

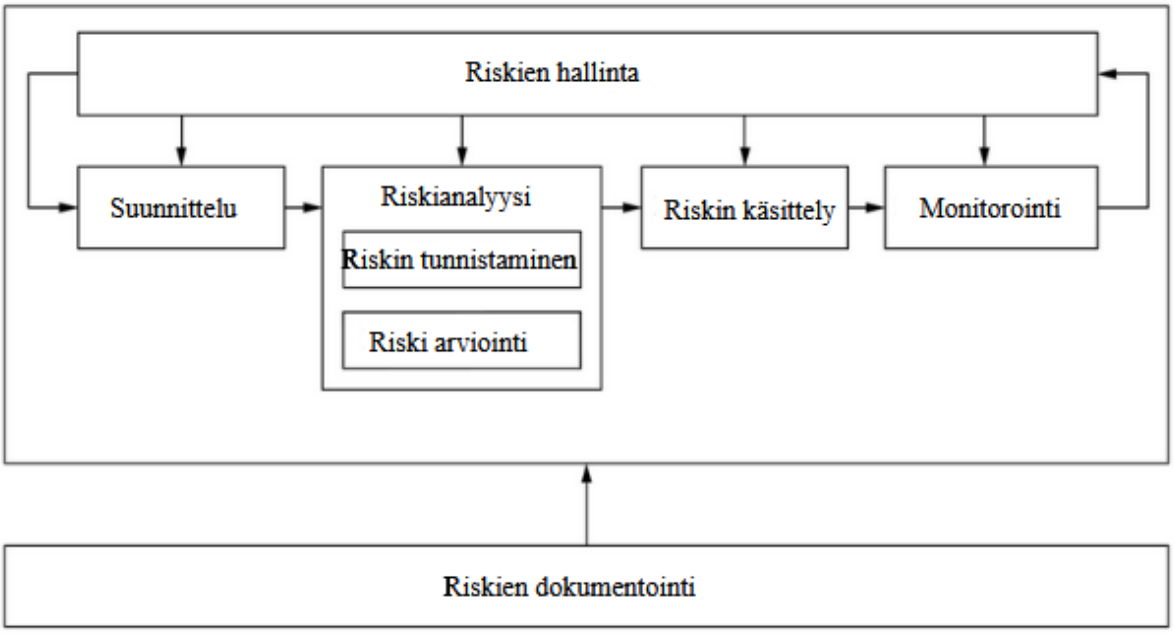
KUVIO 5 Valtiovarainministeriön riskin käsittelyn tarve

6 RISKIEN HALLINTA

Tämän tutkimuksen kannalta riskien hallinta on keskeisessä roolissa. Jotta organisaatio voi lähteä rakentamaan itselleen tietoturva käytänteitä, sen tulee tunnistaa ne riskit, jotka ovat mahdollisia yrityksen liiketoiminnalle. Tämän tutkimuksen kannalta riskienhallinnan elinkaarella on keskeinen merkitys, sillä tavoitteena on lisätä yritysten ymmärrystä siitä, että riskienhallinta ei ole kertaluontoinen projekti ja että vaaditaan muutakin kuin vain teknisiä ratkaisuja. Riskit muuttuvat ajan myötä ja uusia riskejä tulee esille kiihtyvään tahtiin. Riskienhallinnan tulisi tällöin olla jatkuva osa yrityksen toimintaa.

Wheeler (2011, s.44) toteaa, että riski on liikkuva kohde. Tällä tarkoitetaan sitä, että riskit muuttuvat aina ja niillä on uudet muodot. Tämä aiheuttaa riskienhallinnan olevan, kuten tietoturvan hallinta, jatkuva ja iteratiivinen prosessi. Riskien hallinta prosessina on monivaiheinen ja se on voitava tarvittaessa uudelleen arvioida, kun riskit muuttuvat. Riskien hallinnan prosessi alkaa oman omaisuuden arvioinnista, sekä omaisuuden tai riskin herkkyyden arvioimisesta. Tämän toiminnan tavoitteena on tunnistaa yrityksen toiminnan kannalta kriittiset resurssit, joita tulee suojella. (Wheeler, 2011, s.44)

Tämän jälkeen pyritään tunnistamaan keskeisiin resursseihin kohdistuvat uhat ja haavoittuvuudet, arvioidaan riskialttius, päätetään sopivat riskin lähestymistavat, implementoidaan tarvittavat hallintalaitteet, arvioidaan niiden toimivuus ja lopulta tarkastellaan muutoksia ajan kuluessa (Wheeler, 2011, s.44). Wheeler (2011, s 44) kuitenkin itsekin toteaa, että tämä saattaa kuulostaa yksinkertaiselta, mutta todellisuudessa jokainen vaihe voi olla hyvinkin monimutkainen riippuen yrityksestä tai siitä, kuinka yksityiskohtaisesti asioita tarkastetaan.

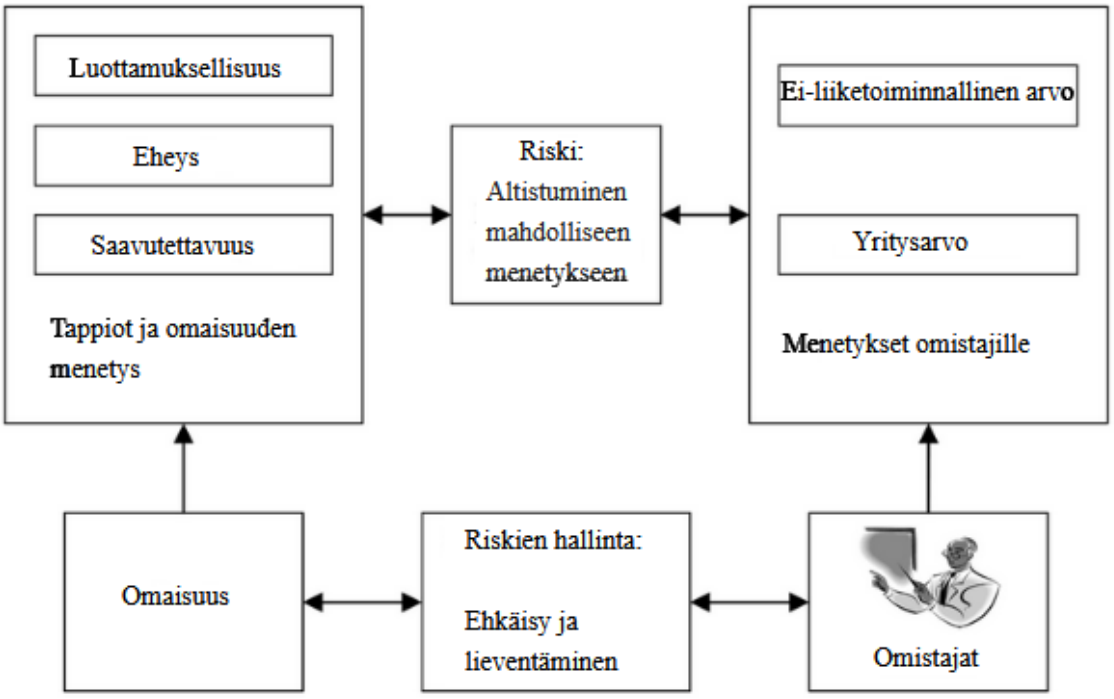


KUVIO 6 Riskinhallinnan elinkaari

Raggad (2010. S. 285) esittää riskienhallinnan elinkaaren hyvin paljon samanlaisena kuin Wheeler. Wheelerin (2011, s.44) kuviossa riskienhallinta on jatkuvaa ja vaikuttaa jokaisessa riskienhallinnan elinkaaren vaiheessa. Riskien suunnittelu, riskien analyysi, riskien käsittely sekä riskien monitorointi ovat erillisiä vaiheita, jotka seuraavat toisiaan. Dokumentointi kattaa koko elinkaaren, sisältäen myös riskien hallinnan. Raggadin mallissa riskianalyysi käsittää riskien tunnistamisen, sekä arvioinnin.
Wheeler (2011, s.46) tarjoaa myös työnkulun riskienhallinnan elinkaarelle, jossa esitetään vaiheet ja tarvittava henkilöstö. Wheelerin mallissa huomioidaan myös jokaisessa prosessin vaiheessa tarvittavat henkilöt.

6.1 Riskien hallinnan yhteys liiketoimintaan

Riskienhallinnan tavoitteena on maksimoida organisaation tuotos (palvelujen, tuotteiden, tulojen ja niin edelleen) ja minimoida odottamattomien tulosten mahdollisuus. Riskin eliminoinnista ei puhuta, koska se ei ole järkevä tavoite. Jotkut organisaatiot, joilla on alhainen riskinsietokyky, ovat ottaneet asenteen kaikkien tunnistettujen riskien ehkäisemisestä. Vaikka tämä toimintamalli voi vaikuttaa toimivalta, se luo pelon kulttuurin riskien tunnistamiseksi, sillä kaikkien riskien poistamiseksi tarvittavat toimet ovat usein täysin suhteettomia riskin toteutumisen vaikutuksiin. (Wheeler, E. 2011. s. 28–29)

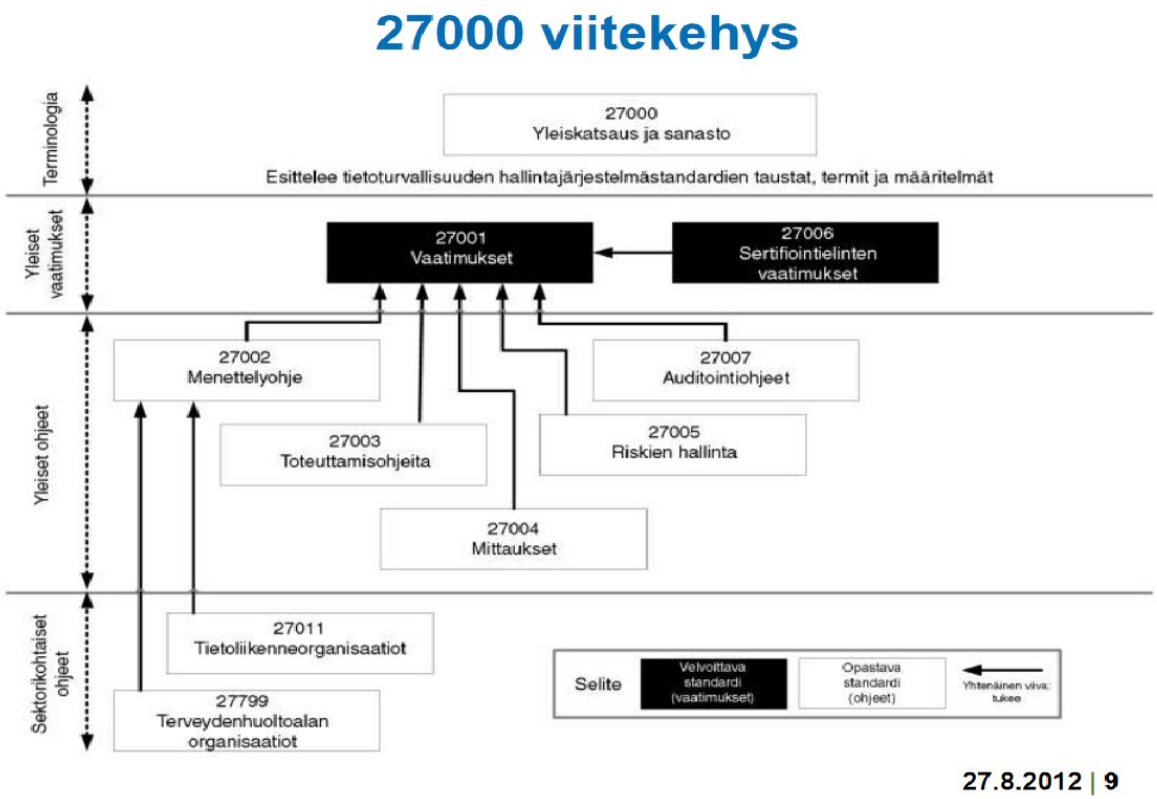


KUVIO 7 Riskinhallinnan yhteys liiketoimintaan

Raggadin (2010, s. 6–287) mukaan riskienhallinnan tarkoitus on hallita riskiä siten, että riski pysyy hyväksyttävän laajuisena. Työ sisältää suunnittelua riskien varalta, riskialttiiden alueiden tunnistamista, riskin hoidon vaihtoehtojen kehittämistä ja koko riskienhallinta ohjelman dokumentointia. Liiketoiminnan näkökulmasta turvallisuuden ei katsota olevan välttämätöntä kannattavuuden kannalta toisin kuin monet tietoturva-alan ammattilaiset ajattelevat sen olevan. Turvallisuusjohtajien on yritettävä määritellä, hallita ja ennustaa epävarmuutta eikä ennakoida sitä (Wheeler, E. 2011. s. 28–29). Riskien hallintaan on saatavilla useita valmiita viitekehyksiä ja standardeja, joita voidaan hyödyntää tietoturvariskien hallinnan suunnittelussa.

6.2 ISO/IEC 27000 Standardiperhe

ISO/IEC 27000 viittaa ISO/IEC standardi perheeseen, jonka yhteinen otsikko on "Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät". Standardit tarjoavat suosituksia ja ohjeita tietoturvan hallintaan, kontrollointiin ja riskeihin eri hallintajärjestelmissä. ISO 27000 sisältää koko ISO/IEC 27000 -standardiperheen yleiskatsauksen, käytetyt määritelmät ja niiden luokitukset sekä yleiset vaatimukset. Yleisiä vaatimuksia määritellään mm. Hallintajärjestelmien luomiselle, toteuttamiselle, käytölle, valvonnalla, katselmoinneille, ylläpidolle ja parannuksille. Standardiperheen keskeisimmät standardit ovat 27001 joka määrää tietoturvan hallintajärjestelmien vaatimukset, sekä 27005 joka määrää riskienhallinnasta. (Suomen standardoimisliitto SFS ry, 2012)



KUVIO 8 ISO 27000 Viitekehys

ISO 27001 valvonta tavoitteet on esitetty oheisessa taulukossa 1.

TAULUKKO 1 ISO 27000 vaatimukset

Tietoturvan osa-alue	Tavoite
Turvallisuuspolitiikka	• Turvallisuuspolitiikan tarkoituksena on tarjota johdolle ohjeita ja tukea tietoturvan hallintaan liiketoiminnan vaatimusten sekä asiaankuuluvien lakien ja asetusten mukaisesti.
Tietoturvan organisointi	• Tavoitteena on hallita tietoturvaa organisaation sisällä. • Hallita organisaation niiden tilojen turvallisuutta, jossa käsitellään ja muokataan tietoa ja joihin on pääsy jollain kolmannella osapuolella.
Omaisuuden hallinta	• Tavoitteena on saavuttaa ja ylläpitää soveltuva suojaus organisaation omaisuuteen

	• Varmistaa, että tiedolle on sopivan tason suojaus
Henkilöstöresurssien turvallisuus	• Tavoitteena on, että työntekijät sopimuskumppanit ja kolmannet osapuolet ymmärtävät omat velvollisuutensa, ovat soveltuvia heille valittuihin rooleihin. • Vähentää varastamisen, petoksen tain väärinkäytösten riskiä. • Varmistaa, että osapuolet ovat tietoisia tietoturvauhista ja ymmärtävät omat vastuut ja velvollisuudet, sekä että heillä on oikeat välineet voidakseen tukea organisaation turvallisuus politiikkaa omassa työssään. • Vähentää inhimillisten virheiden riskiä. • Varmistaa, että osapuolet lähtiessään toimivat sovittujen sääntöjen mukaan.
Ympäristön fyysinen turvallisuus	• Tavoitteena on estää luvaton pääsy, vahingot, häirintä organisaation tiloissa tai tietovaroissa. • Estää menetykset, vahingot, varkaudet, luvaton tietojen muuttaminen tai muu häirintä koskien yrityksen tieto- tai fyysistä omaisuutta.
Kommunikaatio ja operaatioiden hallinta	• Tavoitteena on varmistaa tietojenkäsittelyn oikea ja turvallinen toiminta. • Ottaa käyttöön ja ylläpitää asianmukaista tietoturvan ja palvelujen toimittamisen tasoa kolmansien osapuolten palvelujen toimitussopimusten mukaisesti. • Minimoida järjestelmien kaatumisen riski • Suojella ohjelmistojen ja tietojen eheyttä • Suojella tietojen ja niiden käsittelyyn liittyvän laitteiston eheyttä ja saatavuutta • Suojella tietoja verkossa ja sitä tukevan infrastruktuurin suojaaminen • Estää omaisuuden luvaton paljastaminen, muuttaminen, poistaminen tai tuhoaminen sekä liiketoiminnan keskeyttäminen • Ylläpitää organisaation sisällä ja ulkopuolisten tahojen kanssa yhteisten tietojen ja ohjelmistojen turvallisuutta • Varmistaa sähköisen kaupankäynnin palvelut sekä niiden turvallinen käyttäminen • Luvattoman tiedon käsittelyn havaitseminen
Pääsyn hallinta	• Tavoitteena on kontrolloida pääsyä tietoihin

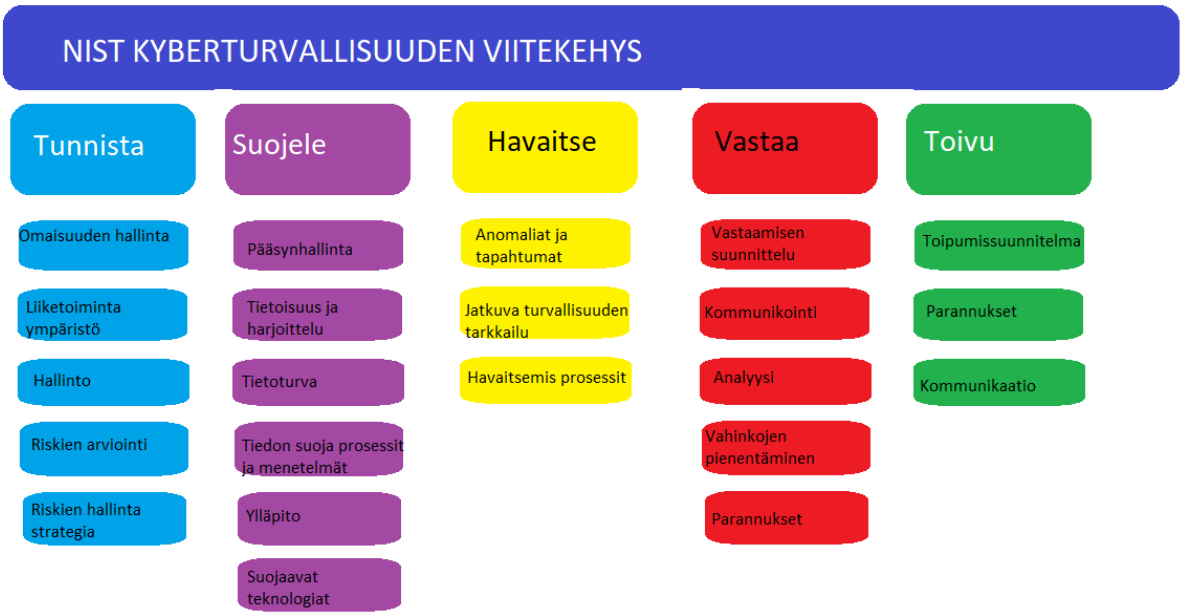
	• Mahdollistaa sallittu pääsy ja estää luvaton pääsy tietojärjestelmiin • Estää luvaton pääsy verkkopalveluihin • Estää Luvaton pääsy operatiivisiin järjestelmiin • Estää luvaton pääsy sovellusjärjestelmissä oleviin tietoihin • Varmistaa tietoturva mobiililaitteiden käytössä ja etätöiden aikana
Tietojärjestelmien hankinta, kehitys ja ylläpito sekä etätyötilat	• Tavoitteena on varmistaa, että turvallisuus on olennainen osa tietojärjestelmiä • Estää virheiden, menetysten, luvattomien muutosten tai tietojen väärinkäyttö sovelluksissa • Tietojen luottamuksellisuuden, aitouden tai eheyden suojaaminen salauksella. • Varmistaa järjestelmätietojen turvallisuus. • Ylläpitää sovellusjärjestelmän ohjelmistojen ja tietojen turvallisuutta • Vähentää julkaistujen teknisten haavoittuvuuksien käytöstä aiheutuvia riskejä
Tietoturvan tapahtuman hallinta	• Tavoitteena on varmistaa, että tietoturvatapahtumista ja heikkouksista kommunikoidaan siten, että mahdollistetaan oikea-aikaiset korjaavat toimenpiteet. • Varmistaa johdonmukainen ja tehokas lähestymistapa tietoturvatapahtumien hallinnassa
Liiketoiminnan jatkuvuuden hallinta	• Tavoitteena on torjua liiketoiminnan keskeytykset ja suojata kriittiset liiketoimintaprosessit tietojärjestelmien merkittävien vikojen tai katastrofien vaikutuksilta ja varmistamaan niiden jatkuminen ajoissa.
Vaatimustenmukaisuus	• Tavoitteena on välttää lakien, asetusten, sopimusvelvotteiden sekä turvallisuusvaatimusten rikkominen • Varmistaa, että järjestelmät ovat organisaation tietoturvakäytäntöjen ja -standardien mukaisia. • Maksimoida tietojärjestelmien auditointiprosessin tehokkuus.

6.3 NIST

NIST:n (National Institute of Standards and Technology) kehittämä riskienhallintakehys (engl. Risk Management Framework) kuvaa tarkkaa ja jäsenneltyä prosessia, joka integroi tietoturva- ja riskienhallinta toimet järjestelmän kehittämisen elinkaareen. Jatkuva seuranta on kriittinen osa riskienhallintaprosessia. Lisäksi organisaation yleistä turvallisuusarkkitehtuuria ja siihen liittyvää turvallisuus ohjelmaa seurataan sen varmistamiseksi, että organisaationlaajuinen toiminta pysyy hyväksyttävällä riskitasolla tapahtuneista muutoksista huolimatta. Ajankohtainen, asiaankuuluva ja tarkka tieto on elintärkeää, varsinkin kun resursseja on rajoitetusti ja yritysten on priorisoitava työnsä. (National Institute of Standards and Technology, 2011) NIST:in viitekehys on suunniteltu kyberturvallisuuden ylläpitämiseen, mutta kuten jo tämän tutkimuksen alussa on todettu, tietoturva on yhä enemmän riippuvainen tietotekniikasta (Flowerday ym. 2016) on tämän viitekehyksen käyttäminen tietoturvariskien hallintaan perusteltua.

Viitekehys sisältää viisi keskeistä kriittistä aluetta:

- Tunnista (engl. Identify): olemassa olevaa dataa tutkimalla voidaan tunnistaa ja arvioida riskejä.
- Suojele (engl. Protect): Elementit, joiden avulla liiketoimintaa voidaan suojata
- Havaitse (engl. Detect): Tietoisuus ongelmista, kun niitä ilmenee
- Vastaa (engl. Respond): Perusasiat, jotka tulee huolehtia, jotta ongelmaan voidaan vastata riittävällä tasolla
- Toivu (engl. Recover): Mitä toimia on tehtävä, jotta voidaan toipua datan menetyksestä. (Ifsecglobal,2021)



KUVIO 9 NIST kyberturvallisuuden viitekehys Ifsec Globalin mallia mukaillen

6.3.1 NIST julkaisut

NIST on julkaissut useita turvastandardeja ja ohjeita tietoturvariskien hallintaan. NIST:in julkaisujen käsitteet ja periaatteet pyrkivät olemaan yhdenmukaisia ISO ja IEC standardien kanssa. NIST:in julkaisut muodostavat yhdessä kattavan ohjeistukset tietoturvariskien hallintaan.

6.3.2 NIST 800-39

NIST Erikoisjulkaisu 800–39, Tietoturvariskin hallinta, organisaation, mission ja informaatiojärjestelmän näkökulma (engl. Managing Information Security Risk: Organization, Mission, and Information System View). NIST 800-39 on "lippulaiva" NIST:in julkaisemien tietoturva standardien ja ohjeiden julkaisusarjassa. Julkaisun tarkoituksena on tarjota ohjeet integroituun, organisaation laajuiseen toimintaan, jonka avulla voidaan hallita organisaation toimintaan liittyviin tietoturvariskeihin. Erikoisjulkaisu 800–39 tarjoaa jäsennellyn, mutta joustavan lähestymistavan riskien hallintaan, joka on tarkoituksellisesti laajapohjaista, sisältää yksityiskohtaiset tiedot riskien arvioimisesta, niihin reagoimisesta ja seurannasta jatkuvasti muiden tukevien NIST-tietoturvastandardien ja -ohjeiden avulla. Julkaisun tarkoituksena ei ole korvata tai vähentää muita riskeihin liittyviä toimintoja, ohjelmia, prosesseja tai lähestymistapoja, joita organisaatiot ovat toteuttaneet tai aikovat toteuttaa muussa lainsäädännössä, direktiiveissä, politiikoissa, ohjelmallisissa aloitteissa tarkoitetuilla riskinhallinnan aloilla, tai tehtävän tai liiketoiminnan vaatimukset. Pikemminkin kuvatut riskienhallintaohjeet

täydentävät ja niitä tulisi käyttää osana kattavampaa yritysriskien hallintaohjelmaa (ERM). (National Institute of Standards and Technology, 2011B)

6.3.3 NIST 800-37

NIST Erikoisjulkaisu 800–37 versio 2, Riskienhallinnan viitekehys tietojärjestelmille ja organisaatioille; Järjestelmän elinkaari käytäntö turvallisuuden ja yksityisyyden suojaamiseksi (englanniksi Risk Management Framework for Information Systems and Organizations; A System Life Cycle Approach for Security and Privacy. Revision2). Julkaisussa kuvataan riskienhallinnan viitekehys ja annetaan ohjeet riskienhallintajärjestelmän soveltamiseksi tietojärjestelmiin ja organisaatioon. Viitekehys tarjoaa kurinalaisen, jäsennellyn ja joustavan prosessin tietoturvariskien hallintaan. Se kattaa tietoturvaluokituksen tekemisen, hallinnan, toteutuksen ja arvioinnin jatkuvan seurannan. Viitekehys sisältää toimia, joiden avulla organisaatiot voivat toteuttaa viitekehyksen riittävällä riskinhallinnan tasolla. Viitekehys tukee lähes reaaliaikaista riskienhallintaa ja jatkuvaa tietojärjestelmää sekä perusvalvontaa toteuttamalla jatkuvia seurantaprosesseja. Viitekehyksen avulla voidaan tuottaa johtoportaalle tarvittavat tiedot tietoturvaa koskevien päätösten tekoon. Riskienhallinta viitekehyksen tehtävien suorittaminen yhdistää olennaiset riskienhallintaprosessit järjestelmätasolla riskienhallintaprosesseihin organisaatiotasolla. Lisäksi se vahvistaa vastuullisuutta ja luotettavuutta organisaation tietojärjestelmissä toteutetuista hallinta- ja valvontatoimista. (National Institute of Standards and Technology, 2018)

6.4 Katakri

Katakri on Kansallisen turvallisuusviranomaisen ylläpitämä turvallisuusauditointikriteeristö. Vuonna 2015 julkaistu kolmas versio uudisti Katakrin aikaisemman rakenteen ja pääpaino siirtyi turvallisuusluokitellun tiedon tietoturvallisuuteen. Katakrin neljännen version päivitys alkoi 2020 ja siinä on huomioitu myös digitaalisen tiedon käsittelyn kehittyminen. Katakri ei itsessään aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Katakria voidaan käyttää auditointityökaluna arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. (Kansallinen turvallisuusviranomainen, 2020)

Katakri on jaettu kolmeen osa-alueeseen. Turvallisuusjohtamista koskevassa (T) osa-alueessa pyritään varmistamaan, että organisaatiolla on toimiva tietoturvan hallintajärjestelmä sekä riittävät henkilöstöturvallisuuden menettelyt turvallisuusluokiteltujen tietojen suojaamiseen. Turvallisuusjohtamisen osa-alue kattaa hallinnollisen tietoturvallisuuden ja henkilöstöturvallisuuden. (Kansallinen turvallisuusviranomainen, 2020

Fyysistä turvallisuutta käsittelevässä (F) kuvataan fyysistä käyttöympäristöä koskevat turvallisuus vaatimukset. Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten turvatoimien toteuttamista siten, että estetään luvaton pääsy turvallisuusluokiteltuihin tietoihin. (Kansallinen turvallisuusviranomainen, 2020

Teknistä tietoturvallisuutta koskevassa (I) osa-alueessa kuvataan tekniselle tietojenkäsittely-ympäristölle asetetut vaatimukset. Teknisen tietoturvallisuuden osa-alueessa kuvataan vaatimukset, joita soveltamalla pyritään varmistamaan järjestelyjen riittävyys. Vaatimukset on jaettu tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden osioihin. (Kansallinen turvallisuusviranomainen, 2020)

7 RISKIEN ARVIOINTIPROSESSI

Riskien arviointi (engl. risk assessment) on prosessi, jolla löydetään ja dokumentoidaan organisaation toimintaympäristöön kohdistuvat riskit (Goodman, S., ym. 2008. s. 6). Riskien arviointi on yksi keskeisimmistä komponenteista yrityksen riskienhallinta prosessissa. Riskien arviointia käytetään tunnistamaan, arvioimaan ja priorisoimaan riskejä yrityksen operatiivisessa liiketoiminnassa. Riskien arvioinnin tarkoituksena on tuottaa tietoa päätöksen tekijöille ja tukea riskien kohtaamisen määrittelyä. Riskinarvioinnit ovat keskeinen osa tehokasta riskienhallintaa ja helpottavat päätöksentekoa kaikilla kolmella riskienhallinta hierarkian tasolla, mukaan lukien organisaatiotaso, tehtävä- / liiketoimintaprosessitaso ja tietojärjestelmätaso. (National Institute of Standards and Technology, 2012)

Deloitten (2020) tutkimuksen mukaa ne yritykset, jotka kokivat operatiivisten riskien hallinnan olevan yrityksessä hyvin hallittu, käytti ensisijaisena menetelmänä riskien arviointia (63 %).

IT järjestelmän komponentit			Riskien arviointi komponentit
Ihmiset		Ihmiset organisaation sisällä	Luotettu henkilökunta Muu henkilöstö
		Organisaation ulkopuoliset ihmiset	Ihmiset luotetuissa organisaatioissa Tuntemattomat ihmiset
Toimintamallit		toimintamallit	IT ja liikentoiminnan normaalit menettelytavat IT ja liiketoiminnan tärkeiden toimintojen toimintamallit
Data/ Tieto		Data/ Tieto	Tiedon lähettäminen Tiedon käsittely Tiedon säilyttäminen
Ohjelmat		Ohjelmat	Sovellukset Käyttöjärjestelmät Turvallisuus komponentit
Laitteisto		Laitteisto	Järjestelmät ja oheislaitteet Turvallisuuteen liittyvät laitteet
Verkko		Verkon komponentit	Intranetin komponentit Internetin tai DMZ komponentit

KUVIO 10 IT systeemiin liittyvät komponentit

Goodman ym. (2002. s. 77) lähestyvät riskien arviointia kuvaamalla IT systeemiin ja siihen liittyvään riskiarviontiin liittyvät komponentit kuvan 1. mukaan. Kuvan 1. Mukainen luokittelumalli tarjoaa yhden lähestymistavan riskien arviointiin

kuvaamalla IT-järjestelmien vakiokomponentit ja tarkastelemalla niitä riskien tunnistamisen näkökulmasta. (Goodman, S., ym. 2008. s.77)

Raggadin mukaan riskiarviointi sisältää riskin tason määrittelyn, sekä sen toteutumisen todennäköisyyden sekä mahdollisen vaikutuksen organisaation toimintaan. Riskien arviointia tarvitaan, jotta voidaan priorisoida kaikki riskien hoitoon suunnitellut toimet. Arvioitua riskin määrää verrataan odotettuihin hyötyihin ennen minkään riskihoidon hyväksymistä (Raggad, B, 2010, s. 285).

Talabis, M ja Martin J. esittävät yrityksestä saatavan tiedon toimivan tehokkaana riskinarvioinnin kulmakivenä. "Ilman tietoja, jotka tukevat arviointiasi, riskiarvioinnista on hyvin vähän hyötyä, ja tekemäsi arviointi voidaan tulkita pelkäksi arvaukseksi" (Talabis ym., 2013, s. 63)

Wheeler korostaa myös yrityksestä ja sen toiminnasta saatavien tietojen merkitystä. Riskinarviointi on toimintojen päätoiminto, jonka avulla haavoittuvuudet tarkastetaan, kartoitetaan todennäköiset uhat, arvioidaan tietyn ympäristön vakavuus sekä merkitys yritykselle ja määritellään seuraukset. Riskiarvioinnissa olisi myös otettava huomioon haavoittuvuuden omaavan resurssin herkkyystaso. (Wheeler, 2011, s.51)

Vladimirov, Gavrilenko & Michajlowski jakavat riskien arvioinnin kolmeen tasoon: strategiseen, operationaalisen sekä taktiseen tasoon. “Strategisella tasolla tarkoitetaan tarkastettavan kokonaisriskiaseman arviointia, joka on sen erillisten osien epälineaarinen summa. Operatiivinen taso yhdistää kaksi muuta erittelemällä mahdolliset yhteydet erilaisten turvallisuusriskien ja riskityyppien välillä, käsittelemällä kaikki prosessit, joihin vaikutus vaikuttaa, ja ylittämällä rajat teknisten, inhimillisten, prosessi- ja poliittisten virheiden välillä. Kun kaikki kolme tasoa toimivat sopusoinnussa, voidaan luoda realistinen kuva tarkastettavan yrityksen tai organisaation erilaisista riskeistä. (Vladimirov ym. 2014. s.288).

Kirjallisuudesta löytyy useita eri tulkintoja riskien arvioinnista. Kaikkia edellä mainittuja tulkintoja yhdistää kuitenkin yksi yhteinen tekijä. Kaikkien tulkinnassa riskien arvioinnista tulee ilmetä:

- Missä resurssissa haavoittuvuus ilmenee?
- Mikä haavoittuvuus on?
- Mikä on riskin toteutumisen todennäköisyys?
- Mikä vaikutus riskin toteutumisella olisi yritykselle?

Vladimirov ym. (2014, s.288) tulkinta avaa riskin arvioinnissa tarvittavaa laajuutta. He näkevät riskin arvioinnissa olevan välttämätöntä peilata riskin toteutumista koko organisaation tasolla. Tällöin se vaatii, että riskien arvioinnin tekee henkilö, joka ymmärtää yrityksen liiketoiminnan ja toimintaympäristön.

7.1 Assassment vs. evaluation termien käyttö riskien arvioinnissa

Talabis ym. (2013) sekä Wheeler (2011) käyttävät tästä vaiheesta englanninkielistä sanaa *assessment*, kun taas Vladimirov ym. käyttävät sanaa *evaluation*. Suomennettuna molemmat tarkoittavat arviointia, mutta niiden vivahde englanniksi on hieman erilainen. Online Assessment Toolin tutorialin mukaan assessment on enemmänkin jatkuva prosessi, jossa tarkastellaan jonkin asian kehittymistä ja tuetaan kasvua. Kun taas *evaluation* on nykytilan arvio ja myös päätös, jossa asian todetaan olevan tietyllä tavalla. Sanoja kuitenkin yhdistää se, että molemmat vaativat kriteereitä, käyttävät jotain mittausmenetelmiä ja ovat näyttöön perustuvia (Online Assessment Tool, 2020). Tämän työn kannalta sana *assessment* on olennaisempi, sillä työ tarkastelee tietoturvallisuuden- ja riskienhallinnan elinkaarta, jotka molemman ovat jatkuvia prosesseja. Vladimirovin ym. tapa lähestyä aihetta päättyvänä prosessina ei ole tämän työn kannalta kuitenkaan häiritsevää. Riskien tarkastelun vaihe päättyy kaikissa tapauksissa jonkinlaiseen arvioon, myös Talabys ym. sekä Wheelerin lähestymistavassa. Ero on siinä, kuinka vaihe toistuu tulevaisuudessa. Vladimirovin ym. lähestymistapa sopii, jos ajatellaan, että yritys käyttää riskien arviointiin esimerkiksi konsulttia, joka ei välttämättä palaa suorittamaan jatkuvaa riskien hallintaa.

7.2 Riskien arviointi viitekehykset

Riskien arviointia varten on olemassa monia valmiita standardeja ja viitekehyksiä. Hopkin (2017, s.120) korostaa, että riskinarviointi sisältää useita toimintoja sekä, että riskien arviointiin on useita lähestymistapoja. Hopkin (2017, s.120) toteaakin, että yksi keskeisistä päätöksistä on valita, keitä osallistuu riskinarviointiin.

Valittuihin tekniikoihin ja menetelmiin vaikuttaa organisaation yleinen tapa lähestyä riskien arviointia. Tietyt tekniikat edellyttävät tiettyjen henkilöiden osallistumista ja vaativat erityistä lähestymistapaa riskien arviointien suorittamiseen. On tärkeää, että omaksuttu lähestymistapa on sopusoinnussa organisaation kulttuurin kanssa (Hopkin, 2017, s. 120).
Riskien arvioimiseen on olemassa useita metodeja ja viitekehyksiä, joita organisaatiot voivat käyttää riskien arviointia tehdessä.

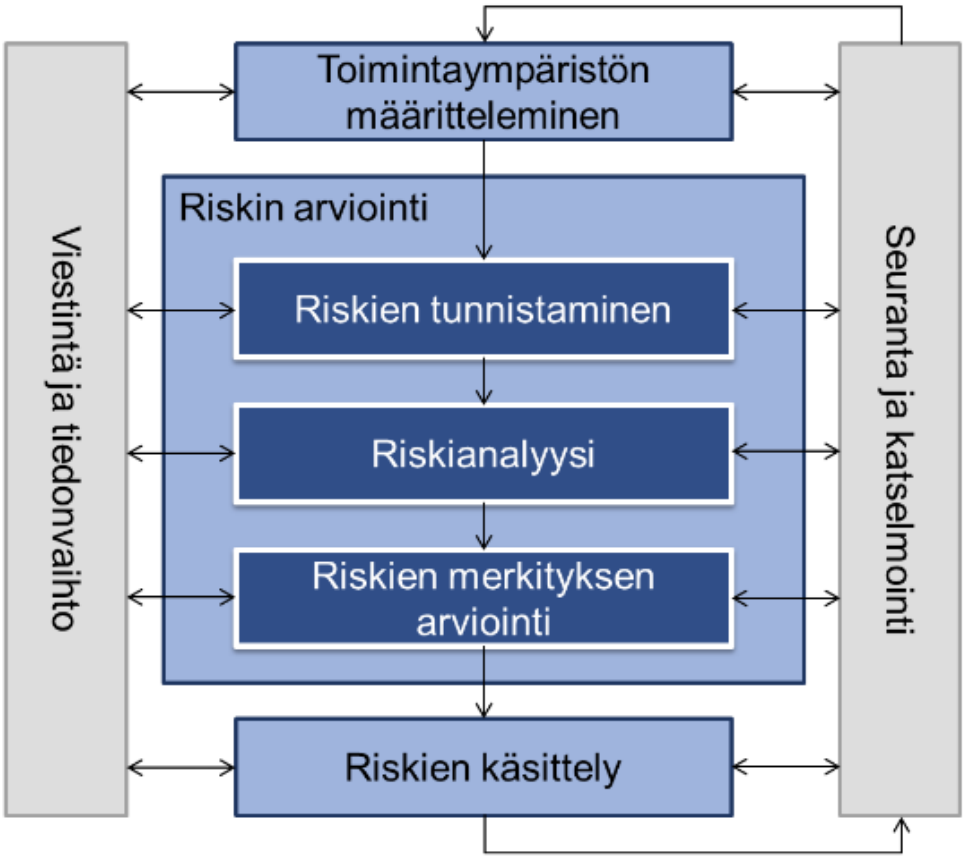
7.3 ISO 27005 ja ISO 31000

ISO 31000 Riskienhallinta on International Standard Organisation (ISO) vuonna 2009 julkaisema standardi, joka on vuosien aikana kehittynyt globaalisti hyväksytyksi (ellei jopa suosituimmaksi) standardiksi riskien hallinnassa. Standardi on hyvin geneerinen, joten se sopii useimpien organisaatioiden käyttöön. ISO

31000 on standardiperhe, joka sisältää useita pienempiä komponentteja, jotka keskittyvät eri riskien hallinnan aspekteihin (Euroopan komissio, 2015).

ISO 31000 standardin erityinen piirre on yhdistää riskienhallinnan viitekehys sekä operatiivinen riskien hallinta prosessi toiminnolla "riskien hallinnan implementointi". Riskienhallinnan viitekehys varmistaa riskien hallinnan jatkuvan sovittamisen organisaation toimintaan. Se noudattaa iteratiivista ja jatkuvaa kehityksen sykliä seuraten yleistä plan-do-check-act (PDCA) sykliä. ISO 31000 käsittää yksitoista periaatetta, tulkiten riskien hallinnan keskeiseksi tehtäväksi kaikilla organisaation tasoilla. Lisäksi riskienhallinnan tulee olla integroitu mahdollisimman läpinäkyvästi kaikkiin organisaation rakenteisiin (Euroopan komissio, 2015).

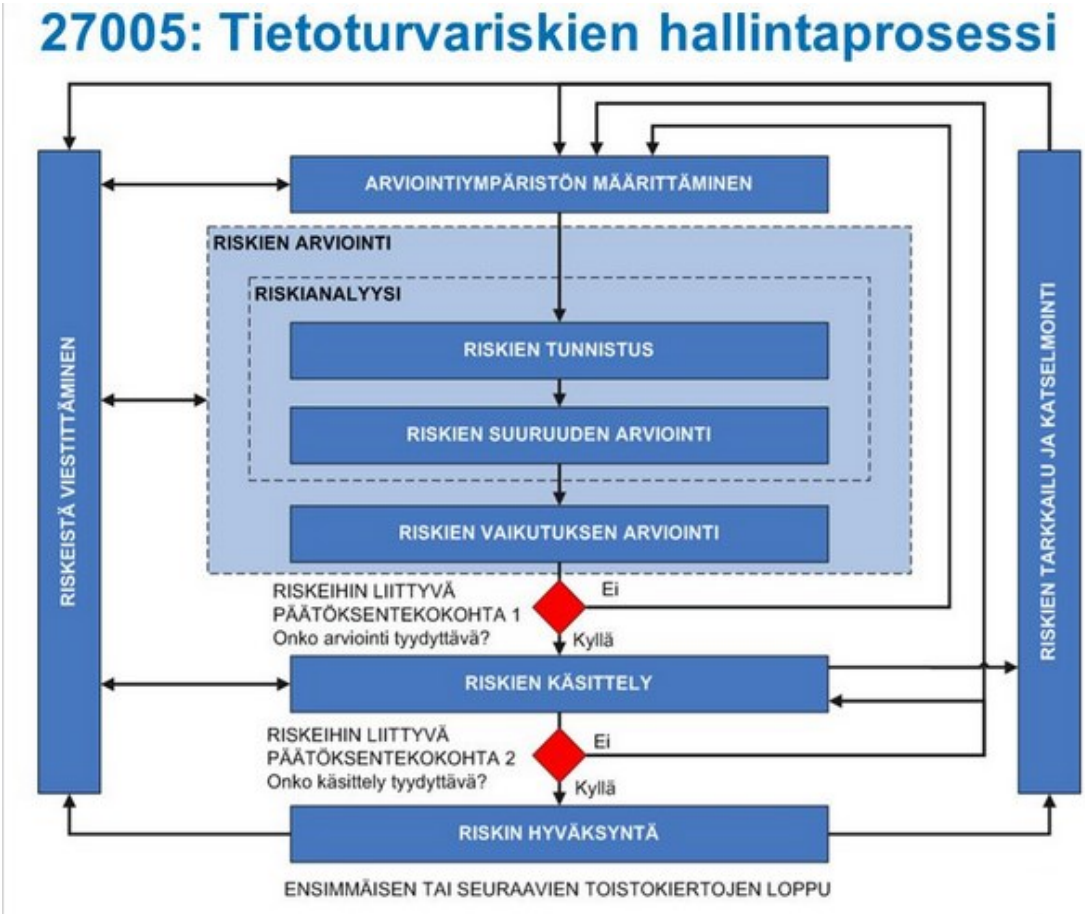
Onnistuakseen riskienhallinta vaatii johdon vahvan sitoutumisen. Tiukka strateginen suunnittelu varmistaa sen, että riskienhallinta on jatkuvasti sisällytetty organisaation rakenteisiin. Organisaation tulee varmistaa että tarvittavat aktiviteetit ovat linjassa riskien hallinnan implementoinnin kanssa. Tällä tarkoitetaan sitä, että toimitaan riskienhallinta käytänteiden mukaan, suoritetaan riskienhallinta prosessia, toimitaan lain ja asetusten vaatimien velvoitteiden mukaisesti, toimitaan yhteistyössä asiaankuuluvien tahojen kanssa sekä kommunikoidaan yleisesti (Euroopan komissio, 2015).



KUVIO 11 Operatiivisten riskien hallinnan viitekehys ISO 31000 mukaan

ISO/IEC 27005 kuuluu ISO 27000 standardi perheeseen. Siinä missä ISO 31000 kuvaa yleisesti riskienhallinnan, ISO 27000 käsittelee lähemmin tietoturvariskeihin liittyviä käsitteitä. ISO 27000 standardiperheen ISO 27005 sisältää erityisesti informaatioturvallisuuden vaatimuksiin soveltuvan ja laajemman riskien hallinta prosessin. ISO 27005 käyttää kuitenkin viittä ISO 31000 standardi perheessä esiteltyä yleistä riskienhallinta elementtiä. (Euroopan komissio, 2015)

ISO 27005 keskeinen päämäärä on riskien organisaation riskien taso sille hyväksyttävälle tasolle tehokkaiden ja oikea-aikaisten prosessien avulla. Riskit, joita ei voida täysin poistaa tullaan huomioimaan juuri riskienhallinnan prosessin aikana. Nämä riskit ovat sellaisia, jotka yrityksen on hyväksyttävä ja sen on tehtävä kaikille osapuolille selväksi, miksi näin on päätetty toimia. Riskien hyväksyminen (engl. Risk Acceptance) on ISO 27005 prosessin viimeinen vaihe (Euroopan komissio, 2015).



KUVIO 12 Tietoturvariskien hallintaprosessi ISO 27005 mukaan

ISO 27005 riskienhallinta prosessissa ensimmäinen askel on arviointiympäristön määrittäminen (engl. Context Establishment). Tässä vaiheessa kerätään kaikki tieto todellisista riskeistä ja luodaan tarpeelliset ehdot viitekehykselle. Samalla tulee päättää millaista riskien hallinnan näkökulmaa tullaan käyttämään. Tämä tarkoittaa myös sitä, että on valittava millä kriteereillä riskejä arvioidaan sekä mikä vaikutus riskeillä on. Lisäksi tulee päättää mikä on se taso

millä riskit hyväksytään. Toinen keskeinen osa on päättää mikä yksikkö organisaatiossa vastaa riskienhallinnasta. Johtotason tuen ja riittävien resurssien varmistaminen on edellytys prosessin onnistumiselle (Euroopan komissio, 2015).

Riskien arviointi käsittää kolme eri vaihetta riskien tunnistaminen (engl. risk identification), Riskin analysointi (engl. risk analysis) ja riskien arvottaminen (engl. risk evaluation). Riskien tunnistamisvaiheessa tarkastellaan, millaisia uhkia organisaatioon kohdistuu, uhkilla tarkoitetaan niin sisäisiä kuin ulkoisia uhkia. Lisäksi tunnistetaan kontekstin luomisvaiheessa päätetyn prosessin soveltamisalan tarkoittamat kohteet (kirjoittajan käännös sanasta assets), joihin liittyvät riskit halutaan tunnistaa. Näihin kohteisiin liittyvät uhat tulee tunnistaa ja onkin tarkasteltava minkä tyyppiset uhat mitäkin kohdetta uhkaa. Kun potentiaaliset uhat on tunnistettu, luodaan lista olemassa olevista ja suunnitelluista hallintatoimenpiteistä. Uhkien lisäksi listataan myös mahdolliset haavoittuvuudet. Tämän jälkeen arvioidaan jokaisen skenaarion potentiaaliset seuraukset organisaatiolle. Seuraukset voivat olla paitsi rahallisia menetyksiä, mutta myös aiheuttaa haittoja organisaation maineelle Riskien analyysivaiheessa keskitytään analysoimaan uhkien potentiaalinsa seurauksia sekä niiden todennäköisyyttä. Riskianalyysissä käytettävät menetelmät tulee olla yhteensopivia kontekstin julistuksessa päätettyjen arviointi kriteerien kanssa (Euroopan komissio, 2015).

Riskin arvottamisen vaiheessa verrataan kaikkien skenaarioiden riskitasoa niihin riskinarviointi kriteereihin, jotka luotiin kontekstin julistamisen vaiheessa. Tällä tavoin voidaan tarkastella riskin kriittisyyttä ja tunnistaa kriittiset riskit organisaation toiminnalle (Euroopan komissio, 2015).

7.4 NIST Special Publication 800–30 ja NIST 800-39

Kuten ISO standardi perheessä, myös NIST viitekehyksessä julkaisut sivuavat toisten NIST julkaisujen toimintamalleja. NIST 800-30 julkaisu keskittyy riskien arviointiin tarjoten yksityiskohtaisen toimintamallin tämän vaiheen suorittamiseen, kun taas NIST-800-39 avaa riskienhallintaa yleisemmällä tasolla kuvaten mm. sitä, kuinka organisaation sisäinen kulttuuri vaikuttaa riskien hallintaan. Riskien arviointi on keskeinen osa organisaation riskienhallintaa. Riskien arviointia käytetään tunnistamaan riskejä, arvioimaan niitä sekä priorisoimaan niiden vaikutus organisaatioon, esimerkiksi sen missioon, toimintaan, julkisuuskuvaan ja maineeseen. (National Institute of Standards and Technology, 2012)

7.5 Muita riskienarviointi viitekehyksiä

Riskien arviointiin löytyy useita viitekehyksiä. Edellä mainittujen ISO/IEC sekä NIST viitekehysten lisäksi löytyy mm.:

- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) from SEI (Software Engineering Institute) and CERT (Computer Emergency Response Team)
- FRAP (Facilitated Risk Assasment Process) Peltier ym.
- SRMD (Security Risk Management Discipline) from Microsoft. (Vladimirov ym. 2014, s.288–289).

Organisaation valitessa sille sopivaa standardia tai viitekehystä, tulee huomioida sen soveltuvuus organisaation toimintaan. Vladimirov ym. (2014. s.289) toteavat, ettei ole aiheellista ottaa käyttöön ja soveltaa kaikkia mahdollisia metodeita, sillä tällöin riskien arvioinnin lopputulos voi olla hämmentävä. Riskien tarkastelussa kannattaa kuitenkin toteuttaa joitain periaatteita, joihin tarkastelussa sitoudutaan.
Hopkinin (2017, s. 120) mukaan riskien tarkastelussa on otettava huomioon neljä kriittistä kysymystä:

- tapahtuman laajuus, jos riski toteutuu;
- tapahtuman vaikutus organisaatioon;
- todennäköisyys riskin toteutumisesta vertailuarvon yläpuolella tai sen yläpuolella;
- hallinnan parantamisen mahdollisuudet

7.6 Riskianalyysi

Riskianalyysin tarkoituksena on tunnistaa riskin ns. herkkyys, ts. se millainen vaikutus riskillä toteutuessaan olisi yritykselle. Riskien analysointi ei kuitenkaan ole niin yksinkertainen prosessi kuin voisi ajatella. Riskianalyysiin liittyy paljon subjektiivisia kokemuksia esimerkiksi siitä mikä riskin hinta toteutuessaan todella voi olla. Riskianalyysin suorittajan tulisi olla tietoinen yrityksen liiketoiminnasta, jotta riskin vaikutusta liiketoiminnalle voidaan arvioida.

Riskianalyysi on tekniikka, jota tietoturva-ammattilaiset käyttävät tietojärjestelmien hallinnan toteutettavuuden selvittämiseen. Silti tekniikka on häiritsevä sekoitus kvantitatiivisia analyysejä, joita sovelletaan tutkittavaan dataan (Baskerville, 1991).
Riskianalyysi on osa riskien hallinnan elinkaarta. Riskien analysoinnissa pyritään ymmärtämään riskiä ja rakentamaan riskien ympärille keinoja hallita niitä. Riskianalyysi pyrkii luomaan ammattimaista tietoa olemassa olevasta tai hankittavasta tietojärjestelmästä (Baskerville, 1991). Riskianalyysin tarkassa kuvauksessa sillä on kaksi ulottuvuutta, ensinnäkin sillä on perinteinen rooli tekniikkana

tai työkaluna tietojärjestelmien suunnittelussa, toisekseen myös riskianalyysiin itseensä liittyvät tekniikat (Baskerville, 1991).

Riskianalyysivaiheessa käytetään erilaisia riskinarviointi työkaluja. Tässä vaiheessa riskin vaikutuksia analysoidaan. Joitakin erilaisia asteikkoja tämän tekemiseen esitettiin luvussa 3. Riskin herkkyyden arvioimiseen voidaan käyttää esimerkiksi Wheelerin riskin herkkyys skaalaa tai Hopkinin riskimatriisia.

Baskerville esittelee FIPS (Federal Information Processing Standards) standardin omaksuman mallin. Malli määrittelee riskin (R) ja riskin esiintymisen todennäköisyyden vuosittain (P), sekä rahallisen menetyksen jos riski toteutuu (C). Tällöin riskin vaikutukset voidaan laskea seuraavasti:

$$R = P \times C$$

Kuten riskinarviointivaiheessa, analyysivaiheessa korostetaan myös suorituskykyisten ihmisten merkitystä. Riskianalyysiryhmä koostuu turvallisuushenkilöstön henkilöstöstä. On toivottavaa, että ryhmän jäsenillä on tekninen pätevyys ja että heillä on ymmärrystä järjestelmän turvallisuudesta ennen riskianalyysiä (Raggad, 2006, s. 319).

Riskianalyysin perustiedot (riskin todennäköisyys ja menetys arviot) ovat erittäin tulkinnanvaraisia, sekä ne ovat usein koottu strukturoimattomilla tutkimuksilla monimutkaisesta organisaatioympäristöstä. Näitä arvoja voidaan manipuloida hyvin positiivisesti ja luoda niiden ympärille muodolliset ja loogiset matemaattiset operaatiot (Baskerville, 1991). Analyysiä suorittavien henkilöiden valinnassa tulee kiinnittää erityistä tarkkuutta, sillä analyysi on lopulta tekijänsä ja tekijän käyttämien laskelmien ja tekniikoiden lopputulos (Baskerville, 1991.; Wheeler, 2011.; Raggad, 2006) Riskianalyysin suorittamiseen voidaan valita useita eri menetelmiä.

Raggad-mallin riskianalyysi ryhmä vastaa seuraavista toimista:

- Tietojen kerääminen riskianalyysiä varten, joka koostuu syvällisistä haastatteluista ja asiakirjojen tarkastelusta.
- Tulosten dokumentointi ja riskianalyysin edellyttämien lomakkeiden täyttäminen.
- Riskianalyysitietojen kokoaminen
- Riskianalyysiraportin kehittäminen. (Raggad, 2006, s.318)

Wheelerin (2017, s.65) mukaan on joitakin vähimmäisvaatimuksia, jotka on kerättävä jokaisesta resurssista:

- Yleinen kuvaus
- Toiminto ja ominaisuudet
- Tietoluokitus
- Kriittisyys organisaatiolle
- Sovellettavat määräykset
- Käyttäjäyhteisö

Kaikki nämä ominaisuudet auttavat selvittämään kunkin omaisuuden tärkeyden organisaatiolle (Wheeler, 2017, s.65).

8 RISKIEN KÄSITTELY

Riskien käsittely tarkoittaa tapaa, jolla riski kohdataan. Raggadin (2006, s.318) mukaan "Turvatoimintojen määritteleminen, valitseminen ja toteuttaminen on prosessi, jolla riskit tuodaan takaisin turvallisuuspolitiikassa määritellylle hyväksyttävälle tasolle. Tähän sisältyy ehdot siitä, mitä pitäisi tehdä, milloin se tulisi suorittaa, kuka on vastuussa, aikataulu ja asiaankuuluvat kustannukset."

Riskihoito on toiminnan tai reaktiostrategian valitseminen jokaiselle analysoidulle riskille. Toimet eroavat toisistaan riskivaikutusten ja vakavuuden mukaan, joten kaikkia riskejä ei voida ratkaista tai käsitellä samalla tavalla.
Hopkin esittelee neljän asteen lähestymistapaa riskihoitoon. Sekä Hopkin (2017, s. 176), Christian Amancei (2011) että Wheeler (2011) käyttävät samaa nelikerroksista asteikkoa. Terminologiassa on pieni ero, mutta neljä peruselementtiä ovat samat.

- Riskien välttäminen - eliminoi epävarmuuden olemalla tekemättä toimia, joita pidetään liiketoiminnan kannalta erittäin riskialttiina. Yleensä kriittisten riskien tapauksessa tätä menetelmää voidaan käyttää riskin välttämiseksi. Hopkin (2017, s.176) kuitenkin toteaa, että valtion voi olla vaikeampi sulkea pois joitain toimia kuin yksityisen sektorin toimijoilla.
- Riskinsiirto - käyttää riskien omistusoikeuden siirtoa tai käyttämällä vakuutuksia, takauksia tai muita sopimuksia, joiden avulla riskiä voidaan jakaa
- Riskin käsittely - riskin käsittelyn (englanniksi treatment) voidaan jatkaa riskialttiin toiminnon suorittamista, mutta siihen kohdistettavien toimien avulla voidaan saada riskitaso sellaiseksi, että se voidaan hyväksyä.
- Riskien hyväksyminen- kaikkia riskejä ei voida estää, joten yrityksellä on oltava hyväksymiskriteerit. Hyväksymiskriteerit riippuvat yrityksen käytänteistä, kiinnostuksen kohteista ja sidosryhmistä.

Kuten Wheeler (2011) toteaa: "Kun riskiryhmä on esitelty, tietoturvaryhmän on yhdessä resurssien omistajan ja ehkä jopa ylimmän johdon jäsenten kanssa neuvoteltava suunnitelmasta riskin pienentämiseksi tai hyväksymiseksi". Raggad (2006) sanoo: "Riskien hyväksyminen on kuitenkin pikemminkin riskienhallinta sääntö kuin riskienhallintastrategia." Tämä tarkoittaa yritykselle, että joka kerta kun uusi ratkaisu otetaan käyttöön, yhtiön tulee tehdä päätöksiä riskin käsittelemisestä. Kuten aikaisemmin on todettu, uusia riskejä tulee jatkuvasti esiin. Yrityksille tämä tarkoittaa, että niiden on oltava jatkuvasti tietoisia uusista tulevista riskeistä.

8.1 Riskien seuranta ja dokumentointi

Kuten edellisessä kappaleessa huomattiin, uusia riskejä tulee melko säännöllisesti esille. Siksi tarvitaan riskien seurantaa. Riskien seuraamisella on iteratiivinen vaikutus yrityksen tietoturvallisuus sykliin. Uuden riskin ilmentyminen voi johtaa riskien uudelleenarviointiin kokonaan tai osittain. Raggad (2006) sanoo: "Se on prosessi, jossa seurataan ja arvioidaan järjestelmällisesti riskin hoitotoimien suoritusta vakiintuneiden mittareiden perusteella ja kehitetään muita riskinhoitovaihtoehtoja tarpeen mukaan. Tämä prosessi tarkastelee muita riskinhallinta toimia, kuten suunnittelua, analysointia ja hoitoa."

Riskien seuranta ei toistu vain riskienhallinnan elinkaaren lisäksi myös tietoturvan elinkaaren aikana. Koska riskinarvioinnissa saattaa olla muutoksia, tämä voi johtaa tietoturvan elinkaaren uudelleen aloittamiseen.

Riskin elinkaaren seurauksena erityisesti analyysit ja hoidot ovat (tai ainakin pitäisi olla) päteviä asiakirjoja. Riskien dokumentointi on lueteltu selkeänä vaiheena riskienhallinnan elinkaaressa; todellisuudessa dokumentointia on suoritettava arviointi- ja analyysivaiheessa koko matkan. Ilman kelvollista dokumentointia on vaikea ajan kuluessa tarkentaa, miksi jokin riski on nostettu korkealle tasolle. Tämä voidaan ratkaista dokumentoimalla perustelut matkan varrella. Tässä dokumentaatiossa on kerättävä kaikki tekijät, jotka otettiin huomioon riskin arvioinnissa ja tehdessä päätöksiä, kuinka riskeihin vastataan (Wheeler, 2017, s.135).

Dokumentoinnilla on tärkeä rooli riskienhallinnan elinkaaressa. Dokumentointi on jatkuva osa elinkaarta, jolloin sen sisältö kattaa kaiken elinkaaren aikana havaitut muutokset ja tehdyt päätökset.

9 HENKILÖSTÖN ROOLI RISKIENHALLINNASSA

Tämä luku käsittelee tietoturvariskien hallintaa tarkastellen henkilöstön merkitystä tietoturvariskien hallinnan näkökulmasta.

On laajasti tiedossa, että yrityksen työntekijät ovat usein heikoin linkki tietoturvariskien hallinnassa. Tietoturvaan liittyvissä tutkimuksissa on annettu liian vähän huomiota ihmisten vaikutukseen tietoturvan kannalta (Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., Giannakopoulos, G. 2014). Metalidou ym. (2014) viittaavat artikkelissaan Cisco Systemsin teettämään tutkimukseen, jossa todetaan, että etätyötä tekevät työntekijät väittävät tuntevansa riskit, mutta saattavat siitä huolimatta aiheuttaa toimillaan tietoturvan vaarantumisen. Huolimatta viimeisimmistä teknologisista tietoturvaratkaisuista käyttäjät omalla toiminnallaan, joko huolimattomuuttaan tai tietämättömyyttään, aiheuttavat tietoturva loukkauksia. Yksi erityinen uhka on ihmisiin kohdistuvat hyökkäykset (engl. Social engineering), jonka avulla työntekijä voidaan saada luovuttamaan tietoja tai asentamaan koneelleen esim. vakoiluohjelman (Metalidou ym. 2014).

Tietoturvariskien hallinta on prosessi ihmisten, käytänteiden ja ohjelmien hallinnoimiseksi tavoitteena toiminnan jatkuvuus samalla kun ylläpidetään strategista linjausta organisaation varsinaisen tehtävän kanssa (Choobineh, J. ym., 2007).

Tietoturvariskien hallinta ja ymmärtäminen on keskeistä yrityksen suunnitellessa omaa strategiaansa. Omaa yritystä koskevien riskien tunnistamisen avulla voidaan rakentaa yrityksen strategiaan ja organisaatiokulttuuriin sopiva malli. Tietoturvallisuuden hallintaan ja johtamiseen löytyy useita eri menetelmiä tai suuntaviivoja:

- TCSEC/Orange Book
- GMITS
- CobiT
- Generally Accepted Information Security Principles (GAISP) 9
- System Security Engineering CMM (SSE-CMM) (Siponen & Willison, 2009)

Artikkellissa Information security management standards: Problems and solutions Siponen & Willison toteavat, ettei näillä menetelmillä ole juurikaan mitään yhteistä. Menetelmät on luotu tukemaan organisaatioiden tietoturvaa tai sertifiointi tarkoituksiin, jotta yrityksen voidaan noudattavan jotain tiettyä menetelmää. Menetelmät ovat organisaatioiden ulkopuolisten komiteoiden laatimia, ja niissä on vahvasti autoritäärinen ote tietoturvan hallintaan. Standardit ovat pyrkineet listaamaan yleisiä tai jopa universaaleja tietoturvakontrolleja, joidenka soveltuvuus/toimivuus kaikkiin eri tilanteisiin erilaisissa organisaatoissa ei ole itsestään selvää (Siponen ym., 2009). Organisaatioille tämä merkitsee sitä, että nämä menetelmät eivät todennäköisesti ole sellaisenaan soveltuvia yrityksen

tarpeisiin. Siponen ym. (2009) myös tuovat esiin sen, että osa esitetyistä menetelmistä suhtautuu tietoturvallisuuteen erittäin puhtaasti tietoturvan tekniseen osaan, IT tuotteiden turvallisuuteen. Organisaatiolle, joka ei toimi selkeästi IT tuotteiden parissa voi olla haastavaa löytää soveltuvaa menetelmää. Tietoturvallisuuden vaatimukset koskevat kuitenkin jokaista organisaatiota, jolloin personoidumpi ratkaisu voi olla tarpeellinen. Riskienhallinta kulttuurin juurruttaminen organisaation toimintaan on kuitenkin vaikeaa ja vain 67 % yrityksistä kokee johtoportaan antavan tähän tarpeeksi tukea (Deloitte, 2010).

9.1 Tietoturvakäytänteet yrityksissä

Vaikka tietoturva käytänteistä on tehty paljon tutkimusta, ei ole olemassa yhtä yhteisymmärrystä siitä, mitä tietoturva käytänteillä tarkoitetaan tai kuinka niitä tulisi kehittää (Paananen, H., Lapke, M., Siponen, M. 2019). Paananen ym. (2019) kirjoittavat, että uudemmassa tietoturva käytänteiden tutkimuksessa tulisi keskittyä enemmän yrityksen tarpeista kumpuavaan tietoturva tarpeisiin, sillä nykyiset tutkimussuunnat eivät tuo selkeää vastausta sille, kuinka asiayhteyteen liittyvät tekijät voitaisiin menestyksekkäästi integroida tietoturva käytänteiden kehitykseen.

Yritykset toimivat tänä päivänä ympäristössä, missä tiedolla on yhä suurempi merkitys. Tietoon kohdistuu jatkuvasti myös uusia uhkia. Tämä pakottaa yritykset etsimään jatkuvasti uusia keinoja suojella tieto pääomaansa. Monet tietoturvan johtamisen teokset korostavat tietoturva käytäntöjen merkitystä ja tietoturva standardeissa ne kuvataan pakolliseksi osaksi tietoturvan hallintaa. Tietoturva käytäntöjen kehittämiseen on tarjolla useita metodeja, mutta niiden kyky ratkaista yksittäisen yrityksen tietoturva käytänteiden kehittämistä ei ole täysin selkeää (Paananen ym. 2019).

9.2 Puutteellinen tietoturvaosaaminen aiheuttaa riskejä

Henkilöstön toiminnalla ja tietoturva osaamisella on merkitystä organisaation kykyyn hallita siihen kohdistuvia tietoturvariskejä (Choobineh ym. 2007.; Metalidou, E., Marangi, C., Panagiotis, T., Eberhagen, N., Skourlas, C., Giannakopulos, G. 2015). Yrityksistä jopa 70 % katsoo, että ammattimaisen riskienhallinta henkilöstön palkkaaminen on heille tärkeää seuraavan kahden vuoden aikana. Lisäksi 54 % yrityksistä katsoo, että myös riskienhallintaa ymmärtävälle operatiiviselle liiketoiminnan osaamiselle on kysyntää. (Deloitte, 2020)

Bodie & Lashkari (2012) jakavat ne tekijät, jotka vaikuttavat toetoturvallisuuten kahteen pääkategoriaan: ihmisten vaikutukseen sekä organisaation vaikutukseen. Bodie ym. (2012) toteavat ihmisten vaikutuksen olevan näistä kahdesta tärkeämpi. Ihmisten vaikutukset on jaettu kahteen alakategoriaan: 1) tekijät, jotka kuuluvat johdolle, lähinnä työkuorman jakamisen sekä heikosti hallittu

henkilöstön hankinta, sekä 2) tekijät jotka johtuvat loppukäyttäjästä (tässä tapauksessa tarkoitetaan henkilöstöä), kuten, tietojen puute, vaaralliset uskomukset, vaaralliset toimintatavat, pätevyyden puute teknologian käytössä, motivaation puute (Bodie ym., 2012).

Motivaation puute

"Henkilöstöä pitää motivoida, jotta he omaksuvat halutun käytöksen ja toimintatavat. Johdon tehtävä on havaita mikä henkilöstöä motivoi" (Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. 2010). Motivaatiota kuitenkin löytyy, kun turvallisuuteen liittyviä asioita jaetaan ja käyttäjät otetaan mukaan päätöksentekoon (Koh, K., Ruighaver, A.B, Maynard, S. & Ahmad, A. 2005).

Tietoisuuden puute

Tietoisuuden puutteella tarkoitetaan sitä, että käyttäjällä ei ole yleistä tietämystä erilaisista hyökkäyksistä. Käyttäjät eivät esimerkiksi osaa havaita koneeseen asennettua vakoiluohjelmaa tai he eivät ymmärrä miksi tarvitaan vahva salasana tunnistautumiseen. He eivät mahdollisesti osaa puolustautua identiteettivarkauksilta, sosiaaliselta hakkeroinnilta (kirjoittajan käännös sanasta social engineering) tai he eivät ymmärrä kuinka estää muita käyttämästä omaa tietokonettaan. (Metalidou ym. 2015)

Uskomukset

Metalidou ym. (2015) viittaavat uskomuksiin lähinnä vaarallisina tai haitallisina uskomuksina. Käyttäjän saattavat esimerkiksi uskoa, ettei antivirus ohjelmiston asentamisesta ole hyötyä tai he ovat valmiit avaamaan kaikki heille sähköpostitse saapuvat linkit.

Teknologioiden taitamaton käyttäminen

Yleisimpiä esimerkkejä teknologioiden taitamattomasta käytöstä ovat mm. Luvattomat konfiguroinnit, muiden käyttäjien salasanojen käyttäminen tai paikkaansa pitämättömän tiedon hakeminen (Metalidou ym. 2015). Kuitenkin "antamalla ihmisille tietoa tietoturvan perusteista, kuten uhkista ja riskeistä sekä heidän oman toimintansa seurauksista voidaan lopulta saavuttaa jatkuvaa muutosta ja kehitystä haluttuun suuntaan" (Ngo, L., 2008).

Tietotekniikkan liittyvät riskit

Badie ym. (2012) esittävät useiden muiden tutkijoiden tekemien tutkimusten perusteella 13 hyökkäystä, jotka kattavat kaikki tietoturvan riskitekijät, ja lopulta määriteltiin "9 tekijää, jotka voivat kattaa kaikki riskit tärkeimpinä tekijöinä". Nämä tekijät ovat: Liian suuret käyttöoikeudet, virheet ja puutteet, palvelunestohyökkäykset, sosiaalinen hakkerointi (kirjoittajan käännös sanasta social engineering), luvaton käyttö, henkilöllisyysvarkaudet, tietojenkalastelu, haittaohjelmat ja luvaton kopiointi.

9.3 Tietoturvakäytäntöjen rakentamisen yhteys riskien hallintaan

Ymmärtämällä yrityksen liiketoimintaa kohdistuvia riskejä, voidaan rakentaa yrityksen toiminnan kannalta kriittisten tietojen ympärille teknisiä suojia sekä käytänteitä, joilla tietojen turvaaminen on mahdollista. Kuten Metalidou ym.

(2014) toteavat, ihmisillä on keskeinen rooli tietoturvariskien hallinnan näkökulmasta. Useilla organisaatioilla voi olla arvokkaita tietoja sekä palveluita sellaisen ihmisen hallinnassa, jotka eivät ymmärrä niiden arvoa, eivätkä tällöin osaa suojata niitä riittävällä tavalla. Tietoturvakäytänteiden avulla huolehditaan siitä, että henkilöstö toimii tiettyjen periaatteiden mukaan. Ennalta sovittujen, yhteneväisten toimintamallien avulla voidaan vähentää ja näin ollen hallita tietoturvariskejä.

10 JOHTOPÄÄTÖKSET JA KESKUSTELU

Tutkimuskysymykseni oli, miten organisaatioissa voidaan hallita tietoturvariskejä. Tietoturvallisuuden ja tietoturvallisuusriskien hallinta saattaa aluksi kuulostaa yksinkertaiselta, mutta kun asiaa tutkii paremmin sen huomaa olevan moniulotteinen ja vaativa kokonaisuus, jonka hallinta on kaikkea muuta kuin yksinkertaista. Aiheesta on kirjoitettu runsaasti kirjallisuutta, mutta niiden painopiste on usein jonkin kapeamman yksityiskohdan alla tarkasteltavana. Esimerkiksi ISO ja NIST viitekehykset jakautuvat useampaan eri julkaisuun, jossa keskitytään yhteen tietoturvallisuuden osa-alueeseen. Aiheen laajuuden huomioiden tämä on luonnollisesti tarpeen, mutta hyvä ymmärrys ja yleiskuva organisaatioiden tietoturvariskien hallinnasta on kuitenkin tarpeellinen, jotta osaa hahmottaa sen merkityksen kokonaisuuden kannalta. Organisaation näkökulmasta löytyy monia asioita ja yksityiskohtia, jotka on otettava huomioon voidakseen hallita tietoturvaa ja tietoturvariskejä. Riskien luonteen vuoksi kenttä muuttuu jatkuvasti ja tämä pakottaa tutkijat ja yritykset seuraamaan riskien kehitystä jatkuvasti.

Tässä tutkimuksessa tietoturvan ja tietoturvariskien hallinta sitoutuvat toisiinsa molempien elämänkaaren kautta. Näihin liittyvät osa-alueet sivuavat toisiaan ja vaativat aina jotakin toisen elinkaaren vaiheesta. Tutkimus nostaa esille keskeiset asiat ja menetelmät, joita yritykset voivat hyödyntää yrityksen tietoturvan ja tietoturvariskien hallinnassa. Tutkimus tehtiin kirjallisuuskatsauksena, jossa pyrittiin löytämään ne keskeiset tekijät, jotka organisaatioiden tulee huomioida tieturvariskien hallinnassa. Useimmat tutkijoiden sekä standardoimisliittojen tietoturvariskien hallinta noudattaa kaavaa riskin tunnistus- riskin arviointi- tehtävät toimenpiteet- implementointi- toisto. Toisto korostuu kaikissa tutkimuksissa ja kirjoissa. Tietoturva on lajina sen luontoinen, että se muuttuu aina. Tämän vuoksi organisaatio ei voi kerran riskiarviointimenettelyn ja siihen liittyvien päätösten jälkeen vain unohtaa prosessia, vaan se joudutaan tekemään aina uudelleen jonkin ajan kuluttua.

Keskeinen osa riskien hallintaa on riskien tunnistaminen. Riskien tunnistaminen vaatii sitä suorittavalta henkilöltä paitsi teknistä osaamista, myös ymmärrystä kyseisen organisaation liiketoiminnasta. Riskien tunnistaminen sekä niiden vaikutusten analysointi on keskeinen osa tietoturvariskien hallintaa. Näiden toimenpiteiden jälkeen voidaan arvioida mitkä riskit on hyväksyttäviä ja mille on tehtävä mahdollisesti joitain välittömiä toimenpiteitä.

Toinen keskeinen tekijä on myös noussut esiin ja se on yrityksen henkilöstön rooli tietoturvan ja tietoturva riskien hallinnassa. Organisaatioissa työskentelee aina luonnollisia henkilöitä. Vaikka teknisesti on varauduttu monenlaisiin uhkiin, voi inhimillinen virhe kaataa koko järjestelmän. Tietoturvariskien kannalta on oleellista, että henkilöstölle on luotu yrityksen toimintaa tukevat tietoturvakäytänteet, joita henkilöstö sitoutuu noudattamaan. Tähän liittyy myös vahvasti se, että johdon on oltava sitoutunut rakentamaan henkilöstölle ympäristö, jossa he voivat työskennellä tietoturvallisesti.

Aiheen laajuudesta johtuen tässä tutkielmassa ei keskitytty yksittäisten toimenpiteiden (esim. riskianalyysi) yksityiskohtaiseen kuvaamiseen. Tutkimuksen tavoitteena oli enneminkin tuoda esiin ne keskeiset tehtävät, mitkä yrityksessä tulee huomioida, sekä antaa suuntaviivoja niihin toimintamalleihin ja viitekehyksiin, joita voidaan käyttää. Samalla tässä tutkimuksessa tuli esiin se, että erilaiset yritykset tarvitsevat erilaisia toimintatapoja eikä jossain onnistunut tapa toimia välttämättä sovi kaikille yrityksille. Tämä osaltaan tekee tietoturvariskien hallinnasta yhä vaikeampaa, sillä tekijöiden on tunnettava myös kohde organisaatio.

Tutkimuksen tekemisen aikaan eräässä yrityksessä tapahtui tietomurto. Yrityksen omistajan sähköpostiin murtauduttiin ja sitä kautta lähetettiin työntekijälle viesti siirtää huomattava summa rahaa tietylle tilille. Vasta siirron tehtyään työntekijä huomasi lähettäjän tiedoissa jotain outoa ja tajusi, ettei viesti ollut esimiehen kirjoittama. Keskustelin tapauksesta työntekijän kanssa ja hän totesi, ettei yrityksessä ole ollenkaan arvioitu mahdollisia uhkia ja riskejä ja, ettei yrityksellä ole olemassa lainkaan tieturvakäytänteitä. Vaikka yritys ei työskentele tietoteknisellä alalla, riskit ovat kuitenkin olemassa myös heillä. Tapahtuman jälkeen johto ei kuitenkaan ollut kiinnostunut muutamaan toimintatapoja. Kuten tässä tutkimuksessa todetaan jo alussa, tietoturva on käsitteenä hyvin abstrakti ja sitä voi olla vaikea hahmottaa, se voi myös johtaa siihen, ettei organisaatioilla ole halua tehdä siihen liittyviä toimenpiteitä. Mutta kuten esimerkkitapauksesta voidaan nähdä, se ei tarkoita, että he olisivat suojassa tieturvariskeiltä. Tutkimuksen ja esimerkissä mainitun tapauksen myötä nousi esille aihe jatkotutkimukseen: Kuinka pienyritysten johto saadaan ymmärtämään tieturvariskit ja niiden merkitys yhä muuttuvassa toimintaympäristössä?

LÄHTEET

Amancei, C. (2011) Practical Methods for Information Security Risk Management. Academy of Economic Studies, Bucharest, Romania

Baskerville, R. (1991) Risk analysis: an interpretive feasibility tool in justifying information systems security. School of Management, State university of New York, Binghaton, NY 13902-6000, USA

Badie, N., & Lashkari, A. H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. Journal of Basic and AppliedScientific Research, 2, 9, 9331–9347.

Calder, A., Watkins, Steve, G. (2010) Title:Information Security Risk Management for ISO27001/ISO27002. It Governance Publishing.

Choobineh, J., Dhillon, G., Grimaila M.R., Rees, J. (2007) Management of information security: Challenges and research directions. Communications of the Association for Information systems, 20(2007) 958–971. Haettu osoitteesta https://aisel.aisnet.org/cgi/viewcontent.cgi?article=2640&context=cais

Deloitte. (2020). Global Risk Management Survey: 10th Edition. Haettu osoitteesta: https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/global-risk-management-survey-10th-ed.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 2013, 4, 92-100.

EU:n GDPR info. (27.11.2020). GDPR asetus. Haettu osoitteesta https://gdpr-info.eu/chapter-3/

Euroopan komissio. (2018). MITIGATE: Multidimensional, *IntegraTed, rIskassessmentframework and dynamic, collaborative riskmanaGement tools for critical information infrAstrucTrurEs*. Haettu osoitteesta: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b907c90e&appId=PPGMS

European Social Survey & Ervasti, H. (2015). *European social survey 2014: Suomen aineisto* (versio 1.0) [sähköinen tutkimusaineisto]. Haettu osoitteesta http://urn.fi/urn:nbn:fi:fsd:T-FSD3068

Flowerday, Stephen V. & Tuyikeze, Tite. (2016) Information security policy development and implementation: The what, how and who. *Computers and security,*

61(2016), 169-183. Used from address http://stephenflowerday.me/uploads/Flowerday%20&%20Tuyikeze%202016.pdf

Goodman, S., Straub, W. S., Baskerville R. (2008) Information Security: Policy, Processes and Practices. Taylor and Francis Group.

Haaparanta, L.,Niiniluoto, I. (1986). Johdatus tieteelliseen ajatteluun. Helsinki: Helsingin yliopisto.

Hopkin, P. (2017). Fundamentals of Risk Management - Understanding, evaluating and implementing effective risk management (4. edition). London, New York, Kogan Bage

Ifsecglobal verkkosivu. (22.04.2021) Haettu osoitteesta: https://www.ifsecglobal.com/cyber-security/a-guide-to-the-nist-cyber-security-framework/

International Chamber of Commerce, ICC. (2015) TIETOTURVAOPAS YRITYKSILLE- ICC Cyber security guide for business. ISBN: ICC Cyber security guide for Business ICC Publication No. 450/1081-5 | 978-92-842-033 Haettu osoitteesta https://kauppakamari.fi/wp-content/uploads/2020/06/tietoturvaopas-yrityksille.pdf

Institute of Risk Management (2002). *A Risk Management Standard.* Haettu osoitteesta: https://www.theirm.org/media/4709/arms_2002_irm.pdf

Järvinen, P. (2004). On Research Methods. Tampere, Finland: Opinpajan Kirja

Kansallinen turvallisuusviranomainen.(21.5.2020). Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. Traficomin julkaisusarja 232/2020. Haettu osoitteesta https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Koh, K., Ruighaver, A.B, Maynard, S. & Ahmad, A. (2005). Security governance: its impact on security culture. Proceedings of the Third Australian Information Security Management Conference, Perth, Austraalia

Kyberturvallisuuskeskus. (2.12.2020) Tietoturva nyt. Haettu 22.04.2021 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/top-5-tietoturvauhat-ja-ratkaisut-organisaatioille

Metalidou, E,. Marangi, C., Panagiotis, T., Eberhagen, N., Skourlas, C., Giannakopulos, G. (2015) The human factor of information security: Unintentional Damage perspective. Elsevier. doi: 10.1016/j.sbspro.2014.07.133

Myllynen, T. (2005). Tietoturva ja riskit tietotekniikassa. Teoksessa Kuusela, H., Ollikainen, R. (toim) Riskit ja riskienhallinta (s.242-272) . Tampere university press, Tampere

National Institute of Standards and Technology. (2011A). NIST Special Publication 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

National Institute of Standards and Technology. (2011B). NIST Special Publication 800-39 Managing Information Security Risk. National Institute of Standards and Technology, Gaithersburg. MD 20899-8930 Haettu osoitteesta https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations; A System Life Cycle Approach for Security and Privacy. Revision 2. Haettu osoitteesta: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations Revision 5. Haettu osoitteesta: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

National Institute of Standards and Technology. (2012). NIST Special Publication 800–30 Guide for Conducting Risk Assessments

Ngo, L., (2008), IT Security Culture Transition Process, IGI Global encyclopedia, Encyclopedia of Information Ethics and Security, 319-325

Online Assessment Tool. (26.11.2020) Haettu osoitteesta: https://www.onlineassessmenttool.com/knowledge-center/assessment-knowledge-center/assessment-vs-evaluation/item10642

Oxford Learner's Dictionary. (12.11.2020) Haettu osoitteesta: https://www.oxfordlearnersdictionaries.com/definition/english/risk_1

Paananen, H., Lapke, M., Siponen, M. (2019). State of the art in information security policy development. Elsevier, Computers and Security (2020) 101608

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation, Edinburgh Etelä Austraalia

Raggad, B. G. 2010. "The Information Security Life Cycle" in Information Security Management: Concepts and Practice. Taylor & Francis Group.

Salminen, A. (2011). Mikä kirjallisuuskatsaus? - Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja.

Siponen, M. (2002.) Designing secure information systems and
software: Critical evaluation of the existing approaches and a new paradigm", University of Oulu, Finland.

Siponen, M. & Klaavuniemi, T. 2020. Why Is the Hypothetico-Deductive (H-D) Method in Information Systems Not an H-D Method. Information and Organizations, Volume 30, Issue 1.

Siponen, M., Soliman, W., Holtkamp, P. (2021) Reconsidering the Role of Research Method Guidelines for Qualitative, Mixed Methods, and Design. Reconsidering the Role of Research Method Guidelines for Interpretive, Mixed Methods, and Design Science Research 22(4), 1176–1196.

Siponen, M., Willison R. (2009). Information security management standards: Problems and solutions. Teoksessa *Information and management* (s.267–270). Elsevier. doi:10.1016/j.im.2008.12.007

Suomen Standardoimisliitto SFS ry verkkosivut. (2012a) Haettu 22.04.2021 osoitteesta http://www.cs.tut.fi/kurssit/TLT-3100/doc/iso-27000.pdf

Suomen standardoimisliitto. (2012b). 27005: Tietoturvariskien hallintaprosessi. Haettu 22.5.2021 osoitteesta https://slideplayer.fi/slide/2714066/

Talabis, M., Martin J. (2013) Information security risk assessment toolkit: Practical assessments through data collection and data analysis. Waltham, Syngress

Valtiovarainministeriö. (2010) Liite 4 Riskienhallintaprosessi

Vladimirov, A., Gavrilenko, K., Michajlowski, A. (2014) Assessing Information Security_ Strategies, tactics, logic and framework (2. painos). United Kingdom. IT Governance Publishing

Wheeler, E. (2011) Security Risk Management- Building an Information Security Risk Management Program from the Ground Up. Elsevier. Haettu osoitteesta https://www.researchgate.net/publication/335358551_Implementation_of_ISO_27001_Standards_as_GDPR_Compliance_Facilitator