



Miten toteuttaa riskienhallinnan jatkuvuus ISO 27001 standardissa pienen yrityksen näkökulmasta?

Niina Kuivalainen

Haaga-Helia ammattikorkeakoulu
Ylempi ammattikorkeakoulututkinto
ICT-palvelut ja tietojärjestelmät
Opinnäytetyö
2025

Tiivistelmä

Tekijä Niina Kuivalainen
Tutkinto Tradenomi (YAMK)
Opinnäytetyön nimi Miten toteuttaa riskienhallinnan jatkuvuus ISO 27001 standardissa pienen yrityksen näkökulmasta?
Sivu- ja liitesivumäärä 38 + 8
<p>Tämän opinnäytetyön tarkoituksena on tutkia miten riskienhallinnan jatkuvuutta olisi mahdollista hallita pienen ohjelmistoyrityksen näkökulmasta. Toimeksiantaja on kotimainen yritys, jossa työskentelee reilut 40 henkilöä. Kohdeyrityksessä on käynnissä ISO 27001 sertifikaattiin tähtäävä projekti. Projekti alkoi keväällä 2024 ja aika pian projektiryhmälle kävi selväksi, että sertifikaatin eteen täytyy tehdä paljon töitä.</p> <p>Yritystoimintaan liittyy aina riskejä, osa niistä on negatiivisia ja osa positiivisia. Yrityksen on hyvä tunnistaa omaan liiketoimintaansa liittyvät riskit, jotta niihin on helpompi varautua. Opinnäytetyössä paneudutaan siihen miksi riskienhallinta on tarpeellista ja mitä kaikkea se vaatii onnistuakseen. Kuten lähdekirjallisuudesta kävi ilmi niin kyseessä on laaja kokonaisuus, joka edellyttää sitoutumista yrityksen joka tasolta. Opinnäytetyön näkökulma oli negatiivisissa riskeissä.</p> <p>Teoreettisessa viitekehyksessä esiteltiin ensin ISO 27001 standardin perusteita. Kyseessä on tunnettu standardi, jolla yritys voi osoittaa, että sen tietoturvan hallintajärjestelmä on toteutettu hyvien käytänteiden mukaisesti. Seuraavaksi tutkittiin riskienhallintaa. Sitä tarkasteltiin ensin yleisellä tasolla. Millaisia riskejä on ja miten niihin liittyviä seurauksia voi määritellä. Mitä riskienhallinta tarkoittaa käytännössä, miten yritys voi löytää riskienhallinnan optimitason. Kolmas osio teoreettisessa viitekehyksessä keskittyi jatkuvuussuunnitteluun ja jatkuvuudenhallintaan. Jatkuvuussuunnittelu on osa yrityksen riskienhallintaa ja tietoturvallisuutta. Se on päättymätön prosessi, joka vaatii sitoutumista, säännöllistä seurantaa ja ylläpitoa.</p> <p>Opinnäytetyön varsinainen tutkimus tehtiin aivoriihenä. Siihen osallistui tutkimuksen tekijän lisäksi 6 osallistujaa kohdeyrityksestä. Aivoriihi toteutettiin verkkokokoussovelluksella ja tulokset kirjattiin virtuaaliselle kirjoitustauluille. Aivoriihessä ideoitiin ensin keinoja, miten riskienhallintaa kannattaisi järjestää ja seurata. Seuraavaksi näkökulma vaihdettiin mahdollisiin haasteisiin. Viimeiseksi tarkasteltiin tiettyjä riskipääryhmiä ja pohdittiin pitäisikö eri riskipääryhmiin kohdistaa erilaista jatkuvuudenseurantaa vai voidaanko kaikkia ryhmiä seurata samalla tavalla.</p> <p>Lopputuloksena voi todeta, että yrityksen kannattaa ottaa riskienhallinta osaksi jatkuvaa toimintaansa riippumatta siitä onko tähtäimessä joku tietty sertifiointi vai ei. Joka tapauksessa riskienhallintatyöstä on yritykselle hyötyä, vaikka se vaatii varsinkin aluksi paljon työtä. On olennaista, että riskienhallinnasta tulee säännöllistä, prosessit ovat hyvin dokumentoitu ja mukana on sitoutuneita henkilöitä.</p>
Asiasanat ISO 27001, tietoturvan hallinta, riskienhallinta, jatkuvuus

Sisällys

Sanasto	1
1 Johdanto	2
1.1 Tutkimuskysymykset	3
1.2 Toimeksiantaja	3
2 ISO 27001 standardi	4
2.1 Koko yrityksen ohjenuora	4
2.2 Tulosten mittaaminen ja arviointi	5
3 Riskienhallinta	7
3.1 Riskienhallinnasta yleisesti	7
3.2 Näkökulma organisaatioon	8
3.3 Standardeista apua määrittelyyn	10
3.4 Riskienhallinta käytännössä	11
3.5 Sisäiset ja ulkoiset vaatimukset	13
3.6 Tavoitteet ja haasteet	14
4 Jatkuvuussuunnittelu ja jatkuvuudenhallinta	16
4.1 Jatkuvuus vaatii sitoutumista	17
4.2 ICT-järjestelmien jatkuvuus	18
4.3 Muutosten hallinta	19
5 Tutkimusmenetelmät	20
5.1 Lähestymistapa	20
5.2 Aineiston hankintamenetelmät	21
5.2.1 Havainnointi	21
5.2.2 Aivoriihi	21
5.2.3 Ideoita tekoälyltä	21
5.3 Aineiston analyysimenetelmät	22
5.4 Muut kehittämismenetelmät	22
6 Riskienhallinnan seurannan ja järjestämisen aivoriihi	23
6.1 Ideoita riskienhallinnan seurantaan ja järjestämiseen	23
6.2 Millaisia haasteita voi tulla	24
6.3 Tarkastelu pääteemojen kautta	25
6.4 Pohdintaa toteutuksesta	27
7 Tutkimuksen tulokset ja arviointi	28
7.1 Tulosten suhde tavoitteisiin	28
7.2 Tulosten käytettävyys	29
7.3 Tulosten suhde tutkimuskysymyksiin	29

7.4	Tulosten suhde lähdeteoriaan	30
7.5	Tutkimuksen uskottavuus, eettisyys ja luotettavuus.....	31
7.6	Käytetyt metodit	31
7.7	Oppiminen.....	32
7.7.1	Tulosten vertailua tekoälyn generoimiin	32
8	Johtopäätökset.....	34
8.1	Jatkokehittämissajatukset	34
	Lähteet.....	36
	Liitteet.....	39
	Liite 1. Havainnointipäiväkirja	39
	Liite 2. Copilot-tekoälypurin tuottamat vastaukset 8.4.2025	40
	Liite 3. ChatGPT:n tuottamat vastaukset 5.5.2025.....	42

Sanasto

Auditointi	toimenpide, jolla arvioidaan tietoturvallisuustasoa (Ilmonen, Kallio, Koskinen & Rajamäki 2022, luku Sanasto).
ISMS	Information Security Management System, tietoturvan hallintajärjestelmä.
ISO/IEC 27001:2023	tutkimushetkellä käytössä oleva ISO-standardin versio.
Jatkuvuussuunnittelu	tarkoittaa toimenpiteitä, joilla yritetään ennalta varautua toimintaa häiritseviin ongelmatilanteisiin (Iivari & Laaksonen 2009, 18).
Jäännösriski	tarkoittaa sellaista osaa alkuperäisestä riskistä, joka päätehtään jättää hallintatoimien ulkopuolelle. Tunnistetut jäännösriskit joko hyväksytään tai käsitellään. (Digi- ja väestötietovirasto 2022.)
Operatiivinen riski	syntyy epäonnistuneista prosesseista, inhimillisistä tekijöistä tai järjestelmän hajoamisesta (Hillson 2023, 56). Liittyvät yrityksen päivittäisiin toimintoihin (Ilmonen ym. 2022, luku 3.1).
Riski	tarkoittaa epävarmuuden vaikutusta tavoitteisiin. Riski voi olla myönteinen tai kielteinen (Juvonen, Koskensyrjä, Kuhanen, Kämppi & Talala 2023, 12).
Riskienhallinta	tarkoittaa järjestelmällistä toimintaa, joka sisältää riskianalyyysin lisäksi suunnittelua, toteutusta, seuranta ja mahdollisia korjaavia toimenpiteitä (Kokonaisturvallisuuden sanasto 2017, 50).
Riskinkantokyky	tarkoittaa organisaation kykyä sopeutua niihin seurauksiin, joita toteutuneista riskeistä tulee (Digi- ja väestötietovirasto 2022).
Riskirekisteri	sisältää tunnistetut riskit ja niihin liittyvät arvioinnit (Digi- ja väestötietovirasto 2022).

1 Johdanto

Opinnäytetyön aihe liittyy ISO 27001 standardin riskienhallintaprosessiin. ISO 27001 on kansainvälinen tietoturvaan keskittyvä standardi, joilla organisaatiot voivat hallita tietoturvaansa (Digiturvamalli s.a.). Riskienhallinta on yksi standardin kattamista osa-alueista. ISO 27001 standardin yhteydessä usein käytetään myös termiä ISMS, joka tarkoittaa tietoturvan hallintajärjestelmää.

Riskienhallintaan olisi jokaisen organisaation hyvä kiinnittää huomiota. On tärkeää tunnistaa erilaiset riskit, jotta organisaation toiminta voi nopeammin palautua normaaliksi, jos mahdollinen riski laukeaa. Riskejä on monenlaisia ja niillä on eritasoisia vaikutuksia. Esimerkiksi tilojen ja laitteiden suojaus, henkilöstön fyysinen turvallisuus ja tietojärjestelmien tietojen suojaus ovat osa-alueita, joita riskit voivat koskea.

Tämän opinnäytetyön tarkoituksena on tutkia miten riskienhallinnan jatkuvuutta olisi mahdollista hallita pienen ohjelmistoyrityksen näkökulmasta. ISO-sertifiointilla tavoitellaan organisaatiolle pysyviä malleja ja prosesseja, joilla voidaan tarvittaessa varmistaa asioiden olevan kunnossa.

Tällaiset laajat vaatimuskehikot, kuten ISO 27001, voivat tuntua ylivoimaisilta hankkeilta yrityksille, joilla ei ole omaa monen hengen tietohallinto-osastoa. Pienemmissä yrityksissä harvemmin on työntekijöitä, jotka voisivat päätoimisesti paneutua pelkästään standardin vaatimuksiin. Myös pienissä yrityksissä on kuitenkin tarve osoittaa, että tietoturva on hoidettu asianmukaisesti. Yksi keino tämän todistamiseen on erilaiset standardit.

Ei kuitenkaan riitä, että yritys laittaa auditointia silmällä pitäen kertaalleen tietoturvaansa ja dokumentaationsa kuntoon. Tämä vaatii myös jatkuvuutta ja seuranta, tarvitaan uusia rutiineja ja prosesseja. Kuinka tällainen seuranta olisi paras hoitaa, kun pienessä yrityksessä tehtävään ei ole mahdollista palkata ketään päätoimisesti? Entä kun henkilökunta vaihtuu, miten estetään tietovuoto ja varmistetaan todellinen jatkuvuus?

Tavoitteena on löytää selkeitä ideoita siitä, miten ISO-standardissa määritellyt prosessit ja mallit saadaan jouhevasti osaksi yrityksen toimintaa ja rutiineja, sekä miten pystytään varmistamaan jatkuvuus, jotta valitut toimintamuodot eivät unohdu heti, kun auditointi on tehty ja sertifikaatti on saatu. Sertifiointin voimassa pitämiseksi sisäisiä ja ulkoisia auditointeja täytyy tehdä jatkuvasti, vähintään kerran vuodessa. Tämä opinnäytetyö ei keskity yrityksen liiketoiminnan kaikkien häiriötilanteiden tunnistamiseen eikä tässä ole tarkoitus tehdä yritykselle toipumissuunnitelmaa. Riskien osalta näkökulma on negatiivisissa riskeissä.

1.1 Tutkimuskysymykset

Tutkimuksessa pyritään vastaamaan seuraaviin kysymyksiin:

- K1. Miten määritellään yrityksen riskit?
- K2. Onko ISO 27001 sertifiointista apua yrityksen riskienhallinnalle?
- K3. Miten varmistetaan riskienhallinnan seuranta ja jatkuvuus?

1.2 Toimeksiantaja

Opinnäytetyön toimeksiantaja on työnantajani Kehätieto Oy. Se on pieni kotimainen ohjelmistoalan yritys, jossa työskentelee reilut 40 henkilöä. Yritys on perustettu vuonna 1989. Päätoimipiste on Helsingissä, mutta työntekijöitä on ympäri Suomea. Kehätiedon päätuote on selainkäyttöinen toiminnanohjausjärjestelmä, jolla asiakas voi hallita esim. jäsentensä tietoja. Yrityksen eri järjestelmiä on käytössä lähes sadassa suomalaisessa järjestössä ja liitossa. Asiakaskenttä on laaja edunvalvonta- ja harrastejärjestöistä puolueisiin. Tietosuoja ja tietoturva ovat erittäin tärkeässä asemassa ja tätä halutaan vahvistaa ISO 27001 -sertifiointilla.

Projektissa on alusta lähtien ollut noin 5 hengen ydinporukka, joka vie standardia eteenpäin muiden töiden ohessa. Projektiryhmässä on mm. tietosuojavastaava, muutama projektipäällikkö ja teknologiajohtaja. Lähes kaikki heistä ovat olleet Kehätiedossa töissä jo useita vuosia, ja heillä on kokemusta yrityksen eri toiminnoista ja toimintatavoista. Projektiryhmän kokoonpano on hieman elänyt projektin aikana ja viimeisimmän muutoksen myötä talvella 2025 mukaan tuli myös toimitusjohtaja.

Toimeksiantajan tavoitteena on saada selkeyttä ISO 27001 standardista sekä konkreettisia lopputuloksia siitä, miten riskienhallinnan jatkuvuutta kannattaisi toteuttaa. Pienessä yrityksessä tieto on monesti henkilösidonnaista ja tätä halutaan sertifiointin osalta välttää. Projektista on tulossa jatkuva, joten tietoa pitää pystyä jakamaan ja prosessien pyöriä, vaikka henkilökunnassa olisi vaihtuvuutta. Toimeksiantajalla ei vielä ole valmiita prosesseja sertifiointiin liittyen, joten tässä on hyvä kehittämismahdollisuus.

2 ISO 27001 standardi

ISO/IEC 27000 standardisarja on tietoturvallisuuden johtamisjärjestelmä, jonka avulla yritys suojaa tieto-omaisuuttaan. Standardi antaa neuvoja ja vaatimuksia tietoturvallisuuden eri osa-alueiden hallintaan. Vaatimukset on tehty yleisluonteisiksi, jotta ne sopisivat useimmille organisaatioille. (SFS Suomen Standardit ry. s.a.) ISO 27001 standardia tukee joukko muita parhaita käytäntöjä kuvaavia standardeja. Näistä jokainen sisältää lisäohjeita tietyistä tietoturvan hallinnan osa-alueista. Standardiperhe kasvaa ja kehittyy jatkuvasti. (Calder 2024, luku Introduction.)

ISO-standardit pohjautuvat englantilaiseen BS25999-standardiin. Se oli pitkään laajimman kannatuksen saanut ja eniten lainattu jatkuvuussuunnittelun standardi, joka määritteli jatkuvuussuunnitteluprosessin terminologian ja periaatteet. Tietoturvallisuuden riskienhallintajärjestelmää ja tietoturvalisuusvaatimuksia on kuvattu ISO 27000 -perheen standardeissa. (Ilmonen ym. 2022, luku 1.4.)

ISO/IEC 27001:n alkuperäinen versio julkaistiin vuonna 2005. Kuten nimestä käy ilmi, standardi on kehitetty yhteistyössä Kansainvälisen standardointijärjestön (ISO) ja Kansainvälisen sähköteknisen komission (IEC) kanssa. (Kamil, Lund & Islam 2023, 702.)

ISO 27001 tunnustetaan maailmanlaajuisesti ja sertifiointilla yritys voi osoittaa, että sen tietoturvan hallintajärjestelmä on linjassa parhaiden käytäntöjen kanssa. Usein myös asiakkaat ja kumppanit ymmärtävät sertifiointin tärkeyden. Viitekehys määrittelee pakolliset elementit, jotta se on standardin mukainen. Standardi on vähimmäisvaatimus. (Calder 2024, luku Introduction.) Standardi edellyttää, että organisaatio parantaa jatkuvasti oman tietoturvan hallintajärjestelmänsä tehokkuutta ja soveltuvuutta. Tämä on mahdollista yhdistämällä seuranta, mittaus ja korjaavia toimenpiteitä muodollisen tarkastusprosessin ja sisäisen tarkastuksen kanssa. ISO 27001 edellyttää tehokkuusmittauksia ja tulosten sisällyttämistä johdon arviointikokoukseen. (Calder 2024, luku 8.)

2.1 Koko yrityksen ohjenuora

Turvallisuuskulttuuri tulee nähdä osana organisaatiokulttuuria eikä se ole siitä erillään oleva asia. Se on näkymätöntä toimintaa, joka pohjaa turvallisuuteen liittyviin arvoihin ja perusoletuksiin. Hyvä turvallisuuskulttuuri vaatii koko henkilöstöltä vahvaa sitoutumista. Esimiesten vastuulla on huolehtia valvonnasta, koulutuksesta sekä määrittellä vastuut ja työn turvallinen tekeminen. (Martikainen & Ranta 2020, 17.) Calder (2024, luku Introduction) tarkentaa, että tietoturvallisuuden suunnittelu ja toteutus ei ole pelkästään IT-tiimin vastuulla vaan se kuuluu myös johdon vastuulle. Se vaatii paljon johtamistaitoja ja erilaisia ominaisuuksia projektinhallinnasta ja priorisoinnista viestintään, delegointia, seuranta ja kurinalaisuutta. Hyvän sisäisen käytännön ja tietoturvatietoisuuden saavuttaminen edellyttää yrityksen kulttuurin muutosta.

Standardin käyttöönottoprojektissa on tärkeää kiinnittää huomiota siihen, että standardin syvin ole-
mus tulee ymmärretyksi. Hienoimmatkaan pääprosessit eivät ole hyödyllisiä organisaatiolle, jos ne
ovat irrallaan organisaation perustoiminnoista. Organisaation keskeisillä arvoilla tulee olla selkeä
yhteys riskienhallinnan periaatteisiin. Puiteiden tulee olla osa konkreettista dynaamista johtamista.
(Suomen Standardisoimisliitto SFS ry 2021, 31.)

Kuten Kamil ja muut (2023, 717) huomauttavat, standardissa esitetyt vaatimukset voivat olla moni-
mutkaisia ja haastavia toteuttaa. Niiden läpivienti onnistuneesti voi vaatia yritykseltä paljon työtä ja
asiantuntemusta. Myös sidosryhmien välillä on eroja siinä, miten standardi käsittelee riskienhallin-
nan toimenpiteitä. Standardi opastaa käsittelemään riskejä ja mahdollisuuksia, mutta eri sidosryhmät
saattavat tarvita myös muita menetelmiä tai lähestymistapoja, jotta he pystyvät paremmin tunnista-
maan oman ympäristönsä riskit.

Culot, Fattori, Podrecca ja Sartor (2019, 83) toteavat artikkelissaan, että heidän haastatteluidensa
mukaan erityisesti ISO 27001 standardin koetaan tuovan vain rajoitettua tukea johtajille. Standardeja
pidetään byrokraattisina ja monimutkaisina eikä ne ole suuntautuneita käytännön ratkaisuihin. Tek-
nologia kehittyy vauhdilla, jolloin suositukset ja tarkistuslistat vanhentuvat nopeasti. Standardin im-
plementointi voi tuntua kosmeettiselta muutokselta eikä kovin merkittävältä.

2.2 Tulosten mittaaminen ja arviointi

Organisaation täytyy kyetä mittaamaan miten turvallisuustavoitteissa on edistytty. Jotta mittaus on
hyödyllistä, on tunnistettava mitä mitataan, miten mitataan ja milloin mitataan. Esimerkiksi näiden
toimien tehokkuuden mittaus olisi tärkeää (Calder 2024, luku 8):

- Riskienhallinnassa tunnistetut merkittävimmät riskit.
- Organisaation tietoturvatietoisuus, koulutukset sekä niiden kustannustehokkuus.
- Haavoittuvuuksien hallinta ja korjaus.
- Kulunvalvonta ja ulkoiset sopimukset.
- Tapahtumien käsittelyprosessit.
- Alueellinen turvallisuus ja korjaustoimenpiteiden nopeus.

ISO 27001 standardi edellyttää sisäisiä ja ulkoisia auditointeja suunnitelluin väliajoin. Ei riitä, että
tietoturvan hallintajärjestelmä toimii teoriassa. Sen täytyy toimia myös reaali maailmassa. Kun riskit
on tunnistettu ja sopivat hallintakeinot on valittu, niin on hyvä varmistua, että hallintakeinot toimivat
oikealla tavalla ja mahdollisissa vikatilanteissa myös hätävastatoimet toimivat. (Calder 2024, luku 8.)

Calderin (2024, luku 8) mukaan testit voi jakaa neljään tyyppiin. Ensimmäisenä on sisäinen audi-
tointi, jossa koulutettu auditoija selvittää, että paperilla kuvattu menettely on totta myös käytännössä.
Nämä koulutetut sisäiset tarkastajat on valittu jo standardin käyttöönottoprojektissa ja ne voivat tulla

yrittäjien eri osastoilta. Tärkeää on, etteivät he tarkasta sitä osaa yrityksen toiminnoista, joista he ovat itse vastuussa. Tällöin he täyttävät auditointitiimin vaatimukset. Toisena testityyppinä on rajoitettu paperikoe. Kyseessä on älyllinen harjoitus. Siinä on osallisena useampi henkilö, jotka tuntevat yrityksen haavoittuvuudet sekä mahdolliset uhat. Tarkastajan tulee kyetä loogisesti testaamaan eri kontrollien kuten liiketoiminnan jatkuvuuden tai tapausten hallinnan tehokkuutta.

Kolmantena testityyppinä on rajoitettu reaalielämän arviointi. Tämä voi tarkoittaa esimerkiksi palvelinhuoneen virran katkaisemista työpäivän aikana. Tällöin saadaan selville toimivatko suojausmenetelmät ja palvelimen sammutustoimenpiteet määritellyllä tavalla. Tällaisissa testeissä tulee olla varma siitä, että järjestelmät saadaan palautettua alkuperäiseen tilaan, jos kaikki ei mene suunnitelmien mukaan. Tosielämän arviointiin kuuluu myös sertifioidun ammattilaisen tekemä penetraatiotestaus. Siinä tarkistaja yrittää tunkeutua organisaation järjestelmiin erilaisilla menetelmillä, joita ei ole aikaisemmin tunnistettu. Testin jälkeen voidaan arvioida ovatko käytetyt menetelmät aitoja uhkia, joihin organisaation tulisi valmistautua. (Calder 2024, luku 8.)

Neljäs testityyppi on laajamittainen skenaarioarviointi. Sillä testataan yleensä kyberhäiriöitä ja liiketoiminnan jatkuvuussuunnitelmaa. Tässä testissä yritetään simuloida usean päivän tapahtumat lyhyemmässä ajassa. Osallistujilta vaaditaan oman roolinsa tunnistamista ja tehtävien suorittamista. Nämä testit vaativat huolellista suunnittelua etukäteen ja mahdollisesti myös ulkopuolisia asiantuntijoita. Kaikki tietoturvan hallintajärjestelmän osa-alueiden auditoinnit ja testit tulee olla tehty vuoden aikana. Ulkopuoliset sertifioidut tarvitsevat todisteita tehdyistä tarkastuksista ja testeistä. Näillä on merkitystä implementoinnin viimeisessä vaiheessa eli varsinaisen sertifikaatin hakemisessa. (Calder 2024, luku 8-9.)

3 Riskienhallinta

”On muistettava, että riski on kaksiteräinen miekka. Jos sitä hallitsee oikeaoppisesti, tuloksena on arvon luominen ja säilyttäminen” (Suomen Standardisoimisliitto SFS ry 2021, 12).

Heti kun yritys aloittaa toimintansa, syntyy operatiivisia riskejä. Sellaisia ovat esimerkiksi häiriöt, petokset, inhimilliset virheet, lakirikkomukset, digitaaliset hyökkäykset ja luonnonkatastrofit. Operatiiviset riskit ovat yhtä vanhoja kuin liiketoiminta ja liiketoiminnan kasvun mukana kehittyivät myös operatiiviset riskit. (Hillson 2023, 56.) Riskit kuuluvat liiketoimintaan. Riskienhallinnan ei ole tarkoitus poistaa kaikkia riskejä. Sillä ennemminkin yritetään ymmärtää yrityksen toimintaa ja hallita liiketoimintaympäristön eri mahdollisuuksia ja rajoitteita. Riskienhallinta on toimintamalli, joka tähtää pysyvään prosessimaiseen toiminnan jatkuvaan kehittämiseen. (Ilmonen ym. 2022, luku 2.1.)

Aven ja Thekdi (2022, 207) ovat sitä mieltä, että riskienhallinnassa on pitkälti kyse oikean tasapainon löytämisestä kehityksen ja suojelun välillä. Suojelua tukevat varovaisuus ja ennalta varautumisen periaatteet ja niihin liittyvät strategiat. Kehitystä taas edistetään ottamalla ja hyväksymällä riskejä uusia arvoja tavoiteltaessa. Riskiarviointien kautta yritetään saavuttaa tasapaino näiden välille ja se tarkoittaa, että riskeistä ei voi puhua erikseen vaan ne kuuluvat aina osana käsiteltäviin vaihtoehtoihin. Hopkin ja Thompson (2022, 31) näkevät riskienhallinnan tarjoavan myös mahdollisuuksia ja he uskovat, että tällaisten riskien hallinta tulee olemaan tulevaisuudessa avainasemassa.

3.1 Riskienhallinnasta yleisesti

Riskienhallinta ja jatkuvuus ovat laajoja asiakokonaisuuksia ja toimintamalleja, jotka vastaavat yrityksen jatkuvuuden toteuttamisesta. Näistä muodostuu kokonaisvaltainen toimintamalli, jossa eri osien väliset periaatteet, roolit ja vastuut yhdessä muodostavat dynaamisen prosessimaisen toiminnan. (Suomen Standardisoimisliitto SFS ry 2021, 7.) Kun määritetään yrityksen kokonaisvaltaista riskienhallintaa, on tärkeää pyrkiä tunnistamaan kaikki potentiaaliset riskit. Sen jälkeen tunnistetut riskit voidaan arvottaa, analysoida ja priorisoida. Tämän jälkeen tarkentuu mitkä riskit ovat merkittäviä ja mitkä tarvitsevat vähemmän hallintakeinoja. (Ilmonen ja muut 2022, luku 3.1.)

Tunnistetuille riskeille tulee suunnitella vastuutahot, riskienhallinnalliset toimenpiteet sekä niiden tavoiteaikataulut. Jotkut riskit voivat vaatia päätöksiä ja toimenpiteitä hallituksen taholta, jos toimivan johdon valtuudet eivät riitä. On tärkeää havaita ja hallita myös eri liiketoimintojen väliin jääviä riskejä ja varmistaa sujuva viestintä ja tiedonvaihto organisaation sisällä. (Suomen Standardisoimisliitto SFS ry 2021, 29.)

Riskienhallinnassa arvioidaan riskitaso sekä riskin käsittely. Myös jäännösriskiin on kiinnitettävä huomioita. Riskin käsittelyssä riskiä voidaan jakaa tai lieventää. Se voidaan myös poistaa tai torjua. Joskus voi olla tarpeen ottaa riski. On hyvä huomioida, että riskin käsittely saattaa muuttaa tai

aiheuttaa uusia riskejä. Kaikille riskeille, joita organisaatio ei voi hyväksyä, olisi tärkeää tehdä ennaltaehkäiseviä toimenpiteitä sekä ohjeistus siitä, miten toimitaan, jos riski toteutuu. Riskien arvioinnista on hyvä tehdä kirjallinen dokumentaatio ja kuvata siinä selkeästi tunnistetut riskit ja riskienhallintaprosessi. Riskitason voi määrittää riskilukuna tai sanallisesti. Riskianalyysin pohjalta voidaan arvioida riskin merkitystä ja verrata tuloksia riskikriteereihin. (Martikainen & Ranta 2020, 19-20.)

Toiminnan sietokyvyllä tarkoitetaan yritysten kykyä ehkäistä, mukautua, reagoida, toipua ja oppia toimintahäiriöistä. Yritysten on hyvä varmistaa, että niillä on tarpeeksi resursseja pysyä sietokykyisenä riskien yhteisvaikutusta vastaan. Tähän tarpeeseen on kehitetty operatiivinen riskienhallinta. (Hillson 2023, 56.) Operatiiviset riskit ovat yleensä luonteeltaan ei-taloudellisia. Ne liittyvät valvonnan heikkouksiin, ennakkoluuloihin ja ihmisten epäonnistumisiin sekä toimintaympäristön muutoksiin. Operatiivisilla riskeillä voi olla seurauksia, jotka ovat ensin ei-taloudellisia, mutta joista myöhemmin voi tulla taloudellisia seuraamuksia. (Hillson 2023, 60-61.)

Kuten Martikainen ja Ranta (2020, 20) toteaa, riski voi olla merkityksetön, vähäinen, kohtalainen, merkittävä tai sietämätön (kuva 1). Organisaatio voi tietoisesti hyväksyä tietyt riskit.

TODEN- NÄKÖISYYS	SEURAUSTEN VAKAVUUS		
	LIEVÄSTI HAITALLINEN (1)	HAITALLINEN (2)	ERITTÄIN HAITALLINEN (3)
HYVIN EPÄTODEN- NÄKÖINEN (1)	MERKITYKSETÖN RISKI $1 \times 1^2 = 1$	VÄHÄINEN RISKI $1 \times 2^2 = 4$	KOHTALAINEN RISKI $1 \times 3^2 = 9$
EPÄTODENNÄKÖI- NEN (2)	VÄHÄINEN RISKI $2 \times 1^2 = 2$	KOHTALAINEN RISKI $2 \times 2^2 = 8$	MERKITTÄVÄ RISKI $2 \times 3^2 = 18$
TODENNÄKÖINEN (3)	KOHTALAINEN RISKI $3 \times 1^2 = 3$	MERKITTÄVÄ RISKI $3 \times 2^2 = 12$	SIETÄMÄTÖN RISKI $3 \times 3^2 = 27$

Kuva 1. Esimerkki riskiluvun laskennasta ja riskin arvioinnista (Martikainen & Ranta 2020, 20)

3.2 Näkökulma organisaatioon

Kokonaisvastuu riskienhallinnan järjestämisestä kuuluu yrityksen hallitukselle. Riskienhallinnan tulee sisältää keskeiset osa-alueet ja olla selkeästi jäsennetty. (Suomen Standardisoimisliitto SFS ry 2021, 28.) Tehokas tietoturvan hallintajärjestelmä auttaa organisaatiota saavuttamaan

tietoturvatavoitteensa (Calder 2024, luku 8). Riskienhallinta on olennainen osa hyvää turvallisuuskulttuuria ja organisaatiota ohjataan ja johdetaan sen avulla. Kokonaisvaltainen riskienhallinta kattaa strategiset, taloudelliset, operatiiviset ja vahinkoriskit. Organisaation kaikissa toiminnoissa ja tasoilla tarvitaan riskienhallintaa. (Martikainen & Ranta 2020, 18.)

Riskienhallinnan tarkoitus ei ole hallita kaikkia riskejä samalla tavalla. Riskien analysoinnin idea on löytää ne positiiviset ja negatiiviset asiat, joihin yrityksen kannattaa panostaa, jotta saadaan paras lopputulos. Varsinkin isoissa organisaatioissa voi olla haastavaa tehdä yhteistyötä organisaatorajojen yli. Riskienhallinnan eri työvaiheiden ja raportoinnin kautta toimintoihin tulee enemmän läpinäkyvyyttä, joka voi osaltaan auttaa yritystä löytämään yhteisiä ja kaikkia palvelevia ratkaisuja. Riskienhallinnan kautta saadaan laajemmin tietoa yrityksen tämänhetkisestä tilasta. (Ilmonen ja muut 2022, luku 1.2.)

Riskienhallinnan käyttöönotto vaatii kärsivällisyyttä, ennakointia ja omistautumista. Se ei tapahdu yhdessä yössä vaan on monivuotinen ponnistus. (Lam 2017, luku 5.) Riskienhallinnan prosesseja ei voi kopioida toisista organisaatioista vaan niiden pitää olla räätälöity organisaation omiin tarpeisiin. Dynaamisella riskienhallinnalla on mahdollista ennakoida, havaita ja reagoida oikea-aikaisesti sisäisiin ja ulkoisiin muutoksiin. On tärkeää, että lähtötiedot perustuvat parhaaseen saatavissa olevaan tietoon. Lisäksi on huomioitava inhimilliset ja kulttuuriset tekijät. (Martikainen & Ranta 2020, 19.)

Organisaation riskienhallinnan pitäisi olla yrityksen toimintaan liittyvä prosessi eikä se saisi olla irrallaan yrityksen muusta toiminnasta. On hyvä huomioida, että myös yhteiskunnan arvot saattavat vaikuttaa yrityksen riskienhallintaan ja niihin liittyviin vaatimuksiin. Yrityksen työntekijöillä on oma tapansa suhtautua riskeihin ja se vaikuttaa heidän toimintatapoihinsa. Tämän vuoksi riskienhallintatyö vaikuttaa ihmisten johtamiseen. Tällöin riskienhallinnasta vastaavilta edellytetään riskinsietokykyä suhteessa omiin johtamistaitoihinsa. (Ilmonen ym. 2022, luku 1.5.)

Aven ja Thekdi (2022, 215) ovat sitä mieltä, että oikeassa riskienhallinnassa riskejä ei uhrata muiden etujen ja huolenaiheiden kustannuksella. Tämä pyritään varmistamaan käyttämällä riskien hyväksymiskriteereitä. On kuitenkin hyvä pohtia missä määrin tällaiset kriteerit ovat tehokkaampia tähän tarkoitukseen kuin muut lähestymistavat. Olennaista on, että yrityksen johto on sitoutunut käsittelemään kaikkia asiaankuuluvia riskejä huolellisesti. Joskus on käynyt niinkin, että riskien hyväksymiskriteerien käyttö on johtanut siihen, että silloin on keskitytty vähemmän varsinaisiin riskien parantamisprosesseihin. Sen vuoksi näitä kriteereitä pitäisi käyttää harkiten.

Jokainen yritys määrittelee itse riskienhallintavastuut ja käytännöt. Apuna voi käyttää yleisiä periaatteita. On huolehdittava siitä, että velvollisuudet ja vastuut pysyvät erillään. Yrityksen riskienhallintakulttuuri voi kärsiä, jos työntekijöille syntyy vääriä odotuksia riskienhallinnasta ja sen tukitoimista.

Tärkeää olisi löytää selkeät toimintatavat, ohjeet ja periaatteet, joilla ohjata riskienhallintatyötä. (Ilmonen ym. 2022, luku 2.3.)

Singh (2022, 34-35) on tutkinut näkökulmaa, jossa big datan tarjoamaa analytiikkaa voitaisiin käyttää hyödyksi riskienhallinnassa. Tämä alue on jäänyt vähemmälle tutkimukselle, vaikka organisaatiot ovat yleisesti ottaen panostaneet big data-analytiikan kehittämiseen. Tutkimuksen tuloksista käy ilmi, että riskienhallinnan tehokkuutta on mahdollista parantaa kyseisen analytiikan avulla.

3.3 Standardeista apua määrittelyyn

Markkinoilla on yleisesti hyväksytyjä riskienhallintastandardeja, joiden avulla yritykset voivat järjestää riskienhallinnan. Standardit kattavat laajasti eri osa-alueita ja ne ovat ohjeellisia, jolloin jokainen voi hyödyntää niitä itselleen soveltuvien osien. Ne auttavat yhteisen sanaston ja metodologian luomisessa, joka mahdollistaa ymmärrettävän ja toistettavan riskienhallinnan lähestymistavan. Jokaisella viitekehyksellä on tietty käyttötarkoitus esim. IT, liiketoiminta, turvallisuus, tieto. On huomioitava, että se voi rajata pois sellaisia riskialueita, jotka ovat yrityksen kannalta merkittäviä. Riskienhallinnan standardien tunnettuus helpottaa yrityksen riskienhallinnasta viestimistä esimerkiksi sidosryhmille. (Ilmonen ym. 2022, luku 1.4.)

Riskienhallinnan viitekehys on esitys toimista, tekniikoista ja työkaluista, joita käytetään kokonaisuuden riskien hallitsemiseksi (Hillson 2023, 63). Suuri osa riskienhallintastandardeista ja -metodeista noudattaa perusrunkoa (Ilmonen ym. 2022, luku 1.4):

- Määritellään tavoitteet ja toimintatavat riskienhallinnalle.
- Tunnistetaan riskit.
- Arvioidaan riskien vaikutus ja todennäköisyys.
- Riskienhallintatoimenpiteiden suunnittelu ja toteutus.
- Raportoidaan ja kommunikoidaan tulokset.
- Arvioidaan riskienhallinnan taso säännöllisesti.
- Kehitetään edelleen.

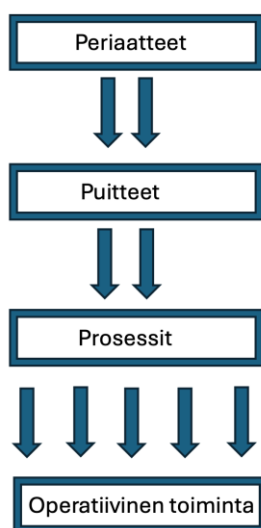
Ilmonen ja muut (2022, luku 1.2) ovat sitä mieltä, että riskienhallinta voi toimia myös yrityksen myyntivalttina. Jos riskienhallinta on hoidettu hallitusti ja tehokkaasti, tämä usein välittyy myös asiakkaille. Tällä voi olla positiivinen vaikutus yrityksen maineeseen. He (2022, luku 2.1) mainitsevat että toiminnan luotettavuutta korostavilla toimialoilla riskienhallinnasta on tullut kilpailutekijä. Erilaisia viitekehys- ja standardeja käytetään soveltaen ja niiden noudattamista vaaditaan myös muilta toimijoilta. On oletettavaa, että kehitys tulee jatkumaan samanlaisena.

3.4 Riskienhallinta käytännössä

Riskien arviointi voidaan jakaa kolmeen osa-alueeseen: riskien tunnistamiseen, analysointiin ja arviointiin. Tunnistamisen tarkoituksena on löytää riskit, joilla on vaikutusta organisaatiolle. On tärkeää tunnistaa myös riskit, joiden lähteiden vaikutusta voi olla vaikeaa tai mahdotonta hallita. Tunnistamisen jälkeen seuraa tarkempi analyysi, jossa selvitetään riskin mahdollisia vaikutuksia, todennäköisyyksiä ja hallintakeinoja. Arviointi tehdään analyysin jälkeen ja siinä tarkastellaan riskin merkitystä osana kokonaisuutta. (Suomen Standardisoimisliitto SFS ry 2021, 21.)

Kaikkea ei kannata yrittää ratkaista kerralla vaan on parempi keskittyä luomaan perusta nopeille vastatoimille, jos riski laukeaa. On hyvä varmistaa, etteivät riskien erityispiirteet pääse monopolisoimaan suunnittelun painopistettä. On olemassa kolme keskeistä kysymystä, joihin kannattaisi ensin keskittyä: miten henkilökunta on valmistautunut, miten toimitaan, jos kriittiset toiminnot ovat vahingoittuneet ja mitä tehdään, jos avainresurssit ovat saavuttamattomissa. (Monahan 2023, 91-92.)

Kokonaisvaltainen riskienhallinta läpäisee koko organisaation ja on läsnä kaikissa eri toiminnoissa (kuva 2). Henkilöstö on organisaation tärkein voimavara, mutta henkilöstöön liittyy myös monta riskiaspektia. Tämä tulisi huomioida operatiivisessa toiminnassa. Henkilöriskit voi jakaa henkilöstöön kohdistuviin tai henkilöstöstä aiheutuviin riskeihin. Pienessä organisaatiossa nämä voivat korostua, jos tietoa ja vastuuta ei ole saatu jaettua useamman henkilön kesken. Organisaation jatkuvuudenhallinnan näkökulmasta jokaisen organisaation tulisi tunnistaa avainhenkilöihin ja osaamiseen liittyvät riskit ja suunnitella varautumiskeinot, jotta mahdollisen riskin lauettua organisaation olemassaolo ei vaarantuisi ja vaikutus olisi siedettävä. (Suomen Standardisoimisliitto SFS ry 2021, 23-24.)



Kuva 2. Riskienhallinnan periaatteiden kulkeutuminen puitteiden kautta prosesseihin (mukaillen Suomen Standardisoimisliitto SFS ry 2021, 23)

Riskienhallinta on käsitteellistä tekemistä. Sillä on oma kielensä, joka voi olla erilaista verrattuna yrityksen normaaliin kielenkäyttöön. Jotta yritys voi tehdä omanlaistaan riskienhallintaa, on tärkeää, että keskeiset käsitteet on määritelty ja niitä käytetään samalla tavalla. Yritys voi ottaa oppia muiden vastaavista ratkaisuista. Myös yhteistyö omien kumppaneiden ja alihankkijoiden kanssa voi olla hyödyllistä, varsinkin jos on tarkoitus käyttää yleisesti tunnettua standardia tai viitekehystä. Olisi tärkeää määritellä mitä tarkoitetaan riskillä, riskin todennäköisyydellä, riskin vaikutuksella, riskinottohalulla ja riskinkantokyvyllä. Jos kaikki eivät ymmärrä keskeisiä käsitteitä samalla tavalla, niiden varaan rakennettu riskienhallintajärjestelmä ei tule toimimaan. On olennaista, että riskin käsite on määritelty kyseisen yrityksen näkökulmasta. (Ilmonen ym. 2022, luku 2.1.)

Tehokas riskienhallinta on tasapainoilua valvontakulujen ja odotettujen tappioiden välillä. Johdonmukainen operatiivisten riskien arviointi voi antaa sellaisia tietoja, joiden pohjalta on mahdollista ohjata lisäinvestointeja sinne, missä mahdolliset tappiot ovat suurimmat. Operatiivinen riskienhallinta ohjaa johdon huomiota juuri näihin potentiaalsiin erittäin vakaviin tapahtumiin eikä vain niihin riskeihin, jotka esiintyvät useammin, mutta joilla on vaatimattomampia mahdollisia tappioita. Operatiivinen riskienhallinta on olemassa jokaisessa prosessissa ja se on jokaisen vastuulla. (Hillson 2023, 59.)

Yrityksen riskienhallinnallisten toimien on tarkoitus tukea johtamista ja päätöksentekoa. Yksinkertaiset ja selkeät menettelytavat pitävät fokuksen pääasiallisessa tekemisessä. On olennaista, että riskit arvotetaan samoja periaatteita noudattaen. Silloin niitä voidaan vertailla keskenään ja priorisoida miten hallintatoimia kohdennetaan. Liian monimutkaiset teoriat saattavat hämärtää toiminnan tarkoitusta ja riskienhallinnasta tulee taakka. Silloin siitä saatava lisäarvo hämärtyy. (Ilmonen ym. 2022, luku 2.1.)

Bissonnette (2016, luku 5) listaa useita käytännöllisiä keinoja, joilla riskejä voidaan tunnistaa:

- Aivoriihi.
- Haastattelut.
- Kyselylomakkeet.
- Asiantuntija-arviot.
- Deplhi-menetelmä.
- SWOT-analyysi.
- Alan parhaiden käytäntöjen katsaus.
- Työnjaon rakenteen tarkastelu.
- Syy-seuraus-kaaviot.
- Vikatyypien ja vaikutusten analyysi.
- Tarkistuslistat.

Riskienhallinnan toteuttaminen vaatii yritykseltä riittävät henkilöresurssit. Jos yrityksessä ei ole päätoimista riskienhallinta- tai turvallisuuspäällikköä, on hyvä pohtia minkä työtehtävän osaksi riskienhallinta sopisi. Vaikka yrityksestä löytyisi edellä mainittu päällikkö, luultavasti hän tarvitsee muita henkilöitä työnsä tueksi. Näiden yhteyshenkilöiden avulla voidaan viedä perusasioita käytäntöön ja he voivat toimia tukena riskienhallintaprosessissa. (Ilmonen ym. 2022, luku 2.1.) Riskienhallintaprosessin eri vaiheet, kuten riskien tunnistaminen, analysointi ja niihin reagoiminen, eivät ole täysin toisistaan erillisiä tapahtuma, jotka voi suorittaa peräkkäin ja saattaa päätökseen. Tyypillisesti nämä ovat toisiinsa integroituja vaiheita, joita suoritetaan iteratiivisesti. (Bissonnette 2016, luku 10.)

Riskienhallinta vaatii herkkyyttä johtamisessa ja on tärkeää korostaa, ettei siinä ole tarkoitus etsiä syyllisiä menneisyydessä toteutuneista epäonnistumisista. Fokus on tulevaisuudessa ja eteenpäin katsomisessa. Toteutuneet riskit on tärkeä tunnistaa, jotta toimintaa voidaan kehittää niiden estämiseksi tulevaisuudessa. Riskienhallinnan on tarkoitus tukea johdon päätöksentekoa eikä kyseenalaistaa heidän liiketoimintapäätöksiänsä. Riskienhallinnan kehittämistyö vaatii kärsivällisyyttä. Aluksi kannattaa laittaa perusasiat kuntoon ja ottaa riskienhallinta osaksi yrityksen vuosisuunnitelua. Riskienhallintaa voi laajentaa myöhemmin. Olennaista on, että kehitys ei pysähdy perusprosessien jalkautuksen jälkeen. Riskienhallinnan pääpaino ei saa olla niiden tunnistamisessa ja analysoinnissa vaan se pitää olla riskien hallinnassa. (Ilmonen ym. 2022, luku 2.1.)

Riskienhallinnan vastuut raportoinnista, valvonnasta ja korjaavista toimenpiteistä on tärkeää määrittellä tarkasti jo alkuvaiheessa. Yrityksen tulee määrittää riskienhallinnan osa-alueet omista lähtökohdistaan. Ensimmäiseksi kannattaa rakentaa kokonaisviitekehys, asettaa mittarit ja tavoitteet. Kun riskienhallinnasta tulee osa yrityksen normaalia toimintaa, siitä tulee tapa tehdä töitä ja olennainen osa yrityksen kulttuuria. Kehittyneessä riskienhallintakulttuurissa se on tärkeä osa jokaisen työntekijän työtehtäviä. Tähän tarvitaan ymmärtämistä ja yhteistä termistöä ja sanastoa. (Ilmonen ym. 2022, luku 2.1.)

3.5 Sisäiset ja ulkoiset vaatimukset

Riskienhallinnan perustan muodostavat yrityksen visio, arvot ja strategia. Niiden avulla luodaan yrityksen riskienhallinnan kulttuuri. Näitä voidaan kutsua sisäisiksi vaatimuksiksi. Yrityksen hallitus ja toimitusjohtaja kantavat lopullisen vastuun riskienhallinnasta. Omistajien riskinottohalukkuus vaikuttaa sisäisiin vaatimuksiin. Sen pohjalta hallitus päättää toiminnoista, joilla sisäiset ja ulkoiset vaatimukset saadaan täytettyä. (Ilmonen ym. 2022, luku 1.3.)

Riskien ja valvonnan itsearviointi on prosessi, jossa yrityksen liiketoimintalinja tai osasto arvioi jokaisen olennaisen operatiivisen riskin todennäköisyyttä ja vaikutusta. Nämä ovat yleensä työpajatyylisiä tilaisuuksia, joissa käsitellään tärkeimpiä jäännösriskejä ja arvioidaan niille altistumista sen jälkeen,

kun on otettu huomioon koulutus, ohjaus ja muut palautusmekanismit. Näistä harjoituksista on tullut yleisiä ja ne kuuluvat nykyään kiinteästi operatiivisten riskien johtajan työkalupakkiin. Nämä itsearviointit johtavat laadulliseen arvioon riskeistä ja kertovat valvontaympäristön tehokkuudesta. Kun itsearviointi tehdään useammalla liiketoimintalinjalla, lopputuloksena on vertaileva yleiskatsaus erilaisista operatiivista riskeistä. Tämä mahdollistaa riskienhallinnan resurssien paremman kohdentamisen sinne, missä riskialtistus ylittää toleranssin. (Hillson 2023, 64-65.)

Lam (2017, luku 6) on tunnistanut kahdeksan teemaa, joilla riskejä voidaan lieventää:

- Palkataan sopivat henkilöt.
- Asetetaan malli ylhäältä käsin.
- Tehdään hyvästä riskikulttuurista helppoa.
- Käytetään asianmukaista mittaria.
- Ymmärretään tiedot.
- Viestitään ongelmasta.
- Toimitaan sen mukaisesti
- Arvioidaan riskikulttuuria säännöllisesti.

Kun puhutaan ulkoisista vaatimuksista, tarkoitetaan mm. lainsäädännöstä, toimialan suosituksista, standardeista tai yritykseen liittyviltä sidosryhmiltä tulevia vaatimuksia. Vaatimusten tunnistamiseksi on tärkeää tuntea lait ja määräykset, jotka liittyvät yrityksen toimialaan sekä mitoittaa painotukset oman toiminnan mukaisesti. Joissakin säädöksissä voidaan vaatia riskianalyysin tekemistä. Tällaiset riskianalyysit kuuluvat riskienhallinnan kokonaisuuteen. (Ilmonen ym. 2022, luku 1.3.) Hillson (2023, 58) huomauttaa, että ulkoisista tapahtumista johtuvat tappiot kuuluvat operatiivisten riskien piiriin. Nämä voivat uhata kokonaisten toimialojen vakautta, joten on tärkeää, että systemaattisesti olennaisia toimialoja säädelään ja valvotaan.

3.6 Tavoitteet ja haasteet

Yksi riskienhallinnan keskeisiä tavoitteita on löytää riskienhallinnan optimitaso. Riskienhallinta on pääoman, kustannusten ja käytettyjen resurssien optimoimista suhteessa tavoiteltaviin hyötyihin. Jos yritys onnistuu tässä, sille voi syntyä kilpailuetua verrattuna toisiin yrityksiin, joiden panostukset riskienhallintaan eivät ole oikeassa suhteessa niiden omiin riskeihin. (Ilmonen ym. 2022, luku 1.2.)

Yksi riskienhallinnan haasteista liittyy siihen, kehitetäänkö sitä kontrollinäkökulmasta vai liiketoiminnan laadullisesta näkökulmasta. Molempien tavoitteiden tulisi näkyä toteutuksessa. Jotta riskienhallinnasta hyötyisi eniten, näiden kahden välille pitäisi saada järkevä tasapaino. Jos kontrollia korostetaan liikaa, riskienhallinta saatetaan nähdä uuden kehittämistä sitovana toimintana. Jos laadullista kehittämistä korostetaan liikaa, kontrolli saattaa jäädä taka-alalle ja keskitytään liiaksi uusiin

liiketoimintamahdollisuuksiin. Molempia siis tarvitaan, jotta kokonaisuudesta saadaan tasapainoinen. Riskienhallinta onkin tasapainon hakemista ja ylläpitämistä näiden välillä. (Ilmonen ym. 2022, luku 2.1.)

Riskienhallinnan käyttöönotto on monimutkainen prosessi, joka voi kestää useita vuosia. Jo pelkäänsä riskien ymmärtäminen ja yhdistäminen vertikaalisesti ja horisontaalisesti on valtava urakka. Tämän lisäksi monet vaiheet voivat olla riippuvaisia toisten vaiheiden valmistumisesta ja ne olisi suoritettava oikeassa järjestyksessä parhaan tehokkuuden saavuttamiseksi. Tässä voi olla apuna etenemissuunnitelma, joka havainnollistaa miten projekti etenee. Hyvä etenemissuunnitelma vastaa seuraaviin kysymyksiin (Lam 2017, luku 5):

- Kuka johtaa projektia?
- Miten mitataan edistymistä?
- Keitä projektissa on mukana?
- Miten yritys hallitsee muutosta?
- Mitä ominaisuuksia ohjelma tarvitsee?

Riskienhallinnan tavoitteet eivät ole yksiselitteisiä. Yrityksessä pitää ymmärtää riskienhallinnan kokonaiskuva, jotta se voi määrittellä pelisäännöt ja tavoitetilan. Mitä riskienhallinta heille merkitsee ja mistä tekijöistä se muodostuu. Riskienhallinta on laaja käsite, joka voi koostua tekemisestä, prosesseista, vastuualueista sekä vakiintuneista tavoista hoitaa asioita. Ei ole olemassa vain yhtä tiettyä määrittystä, joka sisällytetään riskienhallintaan. Näin ollen jokainen yritys muodostaa itse oman tulokintansa siitä millainen riskienhallinta yrityksessä on. On olennaista, että siitä tulee kiinteä osa johtamista ja yrityksen vuosittaista toimintaa. (Ilmonen ym. 2022, luku 2.1.)

4 Jatkuvuussuunnittelu ja jatkuvuudenhallinta

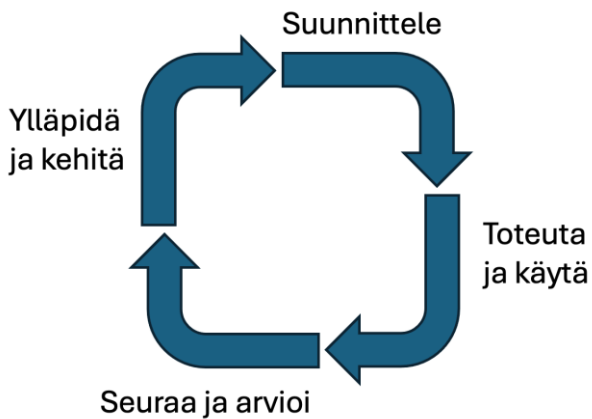
”Jatkuvuussuunnittelu ei ole kertaluontoinen projekti, vaan prosessi” (Iivari & Laaksonen 2009, 18).

Jatkuvuussuunnittelu on osa yrityksen riskienhallintaa, tietoturvallisuutta ja laadunvarmistusta. Suunnittelun tavoitteena on hahmottaa ongelmatilanteet ja varautua niihin ennakolta. Jatkuvuussuunnitelma kattaa normaaliolot ja normaaliolojen häiriötilanteet. Se tulisi nähdä osana organisaation operatiivisten riskien hallintaa. (Iivari & Laaksonen 2009, 18-22.)

Perinteinen riskienhallinta on aiemmin edistänyt käsitystä siitä, että liiketoiminnan jatkuvuus on vain vaikutusten ja vähäisen todennäköisyyden tapahtumien käsittelyä. Tästä on tullut virheellisesti eräänlainen palautus- tai varasuunnitelma katastrofien varalle. Lopputuloksena on ollut suuri joukko tapahtumakohtaisia suunnitelmia, jotka lähinnä keräävät pölyä yritysten hyllyillä. Olisi tärkeämpää keskittyä siihen, miten häiriö vaikuttaa organisaatioon ja tunnistaa ne kohteet, joista organisaation selviytyminen on riippuvainen. (Hillson 2023, 89.)

Iivarin ja Laaksonen (2009, 29) mukaan on tärkeää, että organisaation eri tasot osallistuvat jatkuvuussuunnitteluun. Sillä on vaikutusta mm. hyötyjen realisoitumiseen. Hyvä suunnittelu ja seuranta ovat avainasemassa. Jatkuvuussuunnitteluprosessin aikana tehty järjestelmien ja prosessien dokumentointi on organisaatiolle hyödyllinen ja se voi oppia paljonkin omista toiminnoistaan.

Leflar (2021, 40-41) pitää päättymätöntä prosessia (kuva 3) voimakkaana aspektina, joka jatkuvasti parantaa yrityksen toimintaa. Yhteisen vision kehittäminen ja yhdessä oppiminen mahdollistaa yrityksen kasvun ja juurruttaa pitkän aikavälin muutosaloitteet. Yrityksellä on mahdollisuus muuttaa kulttuuriaan perustavanlaatuisesti, kun kaikki työntekijät kaikilta osastoilta saadaan mukaan. Päättymättömän prosessin malli on sovellettavissa joko koko yrityksen tai sitten vain pienemmän tiimin tai osaston toimintaan. Päättymättömän prosessin malli on syklinen, iteratiivinen ja prosessisuuntautunut. Ongelmatilanteissa prosessissa voi palata taaksepäin ja tehdä muutoksia, koska tämä ei ole lineaarinen prosessi. Mallin vahvuus tulee jatkuvasta oppimisestä eikä muutos koskaan pääty.



Kuva 3. Jatkuvuussuunnittelu on päättymätön prosessi (mukaillen livari & Laaksonen 2009, 23)

Jatkuvuussuunnittelu on organisaation keskeinen tukiprosessi. Se koostuu erilaisista toimenpiteistä ja toimintamalleista. Organisaation on tärkeää ymmärtää miksi jatkuvuussuunnittelua tehdään. Keskeiset tavoitteet ja hyödyt on hyvä kartoittaa jo alussa, jotta jatkuvuussuunnittelua ei nähdä vain pakollisena pahana. Usein jatkuvuuden hallinnan kehittäminen on hyödyksi koko organisaation toiminnalle. (livari & Laaksonen 2009, 230.) Leflar (2021, 40) huomauttaa, että ylimmän johdon tuki on välttämätöntä heti alusta alkaen ja sitä tarvitaan koko prosessin ajan, vaikka kyseessä olisi vain yhtä osastoa tai tiimiä koskeva muutos.

Jatkuvuussuunnittelu tulisi nähdä koko yhteiskunnan asiana. Yrityksillä on tärkeä rooli valtionhallinnon lisäksi yhteiskunnan kriittisten toimintojen turvaamisessa. Varautumisella on tarkoitus turvata kansalaisten hyvinvointi ja yhteiskunnan selviäminen erilaisista kriiseistä. Jatkuvuussuunnitteluun vaikuttavat myös yrityksen ulkopuoliset tahot esimerkiksi lainsäädäntö, asiakkaat ja kumppanit. Oman toimintaympäristön tunnistaminen on tärkeää, jotta ymmärtää omaan toimintaan liittyvät vaatimukset. Vaatimuksissa voi olla vivahde-eroja lähteistä riippuen, mutta useimmiten ne ovat keskenään samankaltaisia. On helpompaa rakentaa kustannustehokkaita ratkaisuja, kun erilaiset vaatimukset on tunnistettu. Vaatimuksissa asetettujen tavoitteiden käytännön toteutuksen yritys saa useimmiten päättää itse. Organisaation ja vaatimusten väliset erot vaikuttavat siihen millainen prosessi jatkuvuudensuunnittelusta lopulta tulee. Joka tapauksessa työn suunnitteluun ja organisointiin on hyvä panostaa, jotta perusta on kunnossa. (livari & Laaksonen 2009, 230-231.)

4.1 Jatkuvuus vaatii sitoutumista

Aidosti toimiva jatkuvuudenhallinta vaatii organisaation johdolta sitoutumista tavoitteisiin, resurssointiin ja tulosten seurantaan. Säännöllisesti tehtävä suorituskyvyn arviointi kuuluu olennaisesti tehokkaaseen jatkuvuudenhallintaan. (Suomen Standardisoimisliitto SFS ry 2021, 9-10.)

Jatkuvuudenhallinnan politiikassa määritellään organisaation ydinryhmän muodostavat henkilöt sekä keskeiset prosessit ja järjestelmät, joiden jatkuvuus on varmistettava. Poliitiikka voi sisältää myös tärkeät sidosryhmät ja toimenpiteet, jotka tulisi huomioida, mikäli jatkuvuus on vaarantunut. Jatkuvuudenhallinnan politiikan dokumentointi on hallituksen hyväksyntä asialle. (Suomen Standardisointiliitto SFS ry 2021, 28.)

Organisaation toiminnan jatkuvuuden turvaaminen kaikissa olosuhteissa on tärkeä tavoite. Hallituksen tulee varmistaa, että riskienhallintaa ja jatkuvuutta kehitetään niin, että (Suomen Standardisointiliitto SFS ry 2021, 29.):

- Tavoitteet ovat yksiselitteiset ja selkeät.
- Strategisia vaihtoehtoja punnittaessa otetaan huomioon mahdolliset riskit, uhat ja hyödyt.
- Huomioidaan organisaation toiminnan jatkuvuus erilaisissa päätöksissä ja valinnoissa.

Jatkuvuussuunnitelman laatiminen ei riitä vaan sitä pitää myös harjoitella ja testata säännöllisesti. Hyvästäkään suunnitelmasta ei ole mitään hyötyä, jos sitä ei ole laatimisen jälkeen päivitetty tai harjoiteltu. Onkin erittäin tärkeää, että jatkuvuussuunnitelmaa testataan ja päivitetään säännöllisesti, jotta se pysyy ajan tasalla. Päivitetty suunnitelma auttaa toimimaan oikein, mikäli toipumistoimia saatetaan tarvitsemaan. (Iivari & Laaksonen 2009, 232.)

Hillson (2023, 92) listaa avainkomponentteja, joista toiminnan jatkuvuudenhallintajärjestelmä koostuu:

- Organisaation politiikka.
- Henkilöillä on määritellyt vastuut.
- Hallintaprosessit politiikoille, suunnittelulle, täytäntöönpanolle, suorituskyvyn arvioinnille, johdon katsaukselle ja parannuksille.
- Kaikki organisaation kannalta merkitykselliset toiminnan jatkuvuudenhallintaprosessit.

4.2 ICT-järjestelmien jatkuvuus

Tietojärjestelmien herkkyys asettaa omat vaatimuksensa järjestelmien vikasietoisuudelle ja toipumiskyvylle. Organisaatioiden ydintoiminnot ovat usein riippuvaisia näistä järjestelmistä. ICT-järjestelmien jatkuvuus ja toimintojen turvaaminen on nykyään kohtuullisen hyvin toteutettu ja huomioitu normaaleissa prosesseissa. Tämä vaatii hyvää tietohallintotapaa ja kunnollista järjestelmien dokumentointia. Jatkuvuudenhallinta koskee myös ostettuja palveluja, ulkoistuksia ja toimittajan käyttämiä alihankkijoita. Suulliset lupaukset eivät tällöin riitä vaan sovitut käytännöt on tärkeää kirjata ylös. Usein jos asiasta ei ole erikseen sovittu, sitä ei myöskään tehdä. Kirjattujen vaatimusten toteutumista pitää myös valvoa säännöllisesti. (Iivari & Laaksonen 2009, 233.)

Hillson (2023, 69) on sitä mieltä, että digitalisaation tuomat hyödyt ja riskit kasvavat jatkuvasti. Riippuvuus IT-infrastruktuureista ja systeemeistä, keskittyminen pilvipalveluiden tarjoajiin ja verkkokaupan laajentuminen ovat osa tätä. Yritykset ovat omaksuneet mallin, jossa ollaan vahvasti riippuvaisia ulkoistamisesta. Operatiiviset riskityypit kuten tietoturva, ohjelmointivirheet, kolmannen osapuolen ja ulkoistuksen riskit ovat moninkertaistuneet viimeisen vuosikymmenen aikana ja niiden odotetaan kasvavan myös tulevana vuosina. Lisääntyneen automaation ja digitalisaation myötä operatiiviset riskit laukeavat harvemmin, mutta niistä tulee vakavampia tapahtumia, kun prosesseissa tapahtuvat muutokset tekevät virheistä toistuvia ja tuhoisempia.

4.3 Muutosten hallinta

Kuten Kang (2014, luku 2.6) huomauttaa, riskiympäristön muutosten käsittely on ollut tutkimuksissa toistuva teema. Muutokseen vastaamisesta on tullut avaintekijä tietoturvariskien hallinnan varmistamisessa. Hän viittaa useisiin vuosituhannen alun tutkimuksiin, joissa peräänkuulutettiin muutoksia ja strategioita tietoturvariskien hallintaan. Tuolloin ei kuitenkaan ole pystytty tarkentamaan kuinka muutoksiin tulisi reagoida, vaikka on tunnustettu, että käytännössä muutos on merkittävä IT-häiriöiden tekijä.

Muutosten hallintaan on olemassa monenlaisia malleja, joista useimmat vaativat paljon tietoa ja kokemusta, jotta niistä saa täyden hyödyn irti. Mallin valintaan vaikuttaa moni asia mm. projektin yksityiskohdat, käytettävät resurssit, mallin selkeys käyttäjälle sekä mallin tarkoituksenmukaisuus. Käyttäjälleen tutut mallit saattavat tulla useimmiten valituksi, vaikka se ei tarkoita, että ne olisivat aina tarkoituksenmukaisia kyseisen yrityksen ympäristöön. Joustava ja mukautuva malli, jonka tuloksista on aikaisempaa kokemusta, voi kuitenkin olla hyvä valinta. (Leflar 2021, 34.)

Riskienhallinnan toteutustiimin on kehitettävä ja jaettava perusteellinen asialista muutosten hallinnan helpottamiseksi. Käyttöänoton kannalta seuraavat viisi vaatimusta ovat kriittisiä (Lam 2017, luku 5):

- Hyvin määritelty konfliktien tunnistamis- ja ratkaisuprosessi.
- Integroitu yhteisymmärrys koko ohjelmassa.
- Toteutuksen aikana läpinäkyvän tiedonkulun mahdollistava viestintäkanava.
- Tehokas hallituksen ja johdon koulutus.
- Kannustimet, jotka on suunniteltu vastaamaan ohjelman tarpeita ja odotuksia.

5 Tutkimusmenetelmät

Tutkimuksessa tehtiin laadullista eli kvalitatiivista tutkimusta. Tällainen tutkimusote soveltui tähän opinnäytetyöhön, koska aineisto kerättiin tutkittavilta vuorovaikutussuhteessa, huomio oli tutkittavien näkemyksissä, tutkija oli aineiston kerääjä ja tavoitteena oli kokonaisvaltainen ymmärrys tutkittavasta ilmiöstä (Kananen 2019, 26). Laadullisessa tutkimuksessa yritetään tehdä löytöjä ilman tilastollisia menetelmiä. Siinä ei pyritä yleistykseen kuten määrällisessä tutkimuksessa. Myös tutkimusprosessi on erilainen kuin kvantitatiivisessa tutkimuksessa eikä se ole suoraviivainen prosessi. Etukäteen ei voida määritellä esimerkiksi kerättävän aineiston määrää vaan sitä tulee kerätä niin paljon, että tutkimusongelmaan löytyy vastaus ja ilmiö tulee ymmärretyksi. (Kananen 2014, 18-19.)

Laadullisessa tutkimuksessa tarkastellaan yksittäistä tapausta ja sen avulla on mahdollista löytää uusia tapoja ilmiön ymmärtämiseksi. Tutkittavasta kohteesta pyritään saamaan irti mahdollisimman paljon. Tutkimustulosta ei voida yleistää vaan se pätee ainoastaan tutkimuskohteen osalta. Laadullinen tutkimus keskittyy yleensä prosesseihin. Näitä on hankala tutkia määrällisessä tutkimuksessa tilastollisen analyysin kautta prosessien ja ilmiöiden monimutkaisuuden vuoksi. Usein laadullinen tutkimus on kuvailevaa, jossa tutkija yrittää ymmärtää ilmiötä sanojen, kuvien ja tekstien kautta. Laadullisella tutkimuksella pyritään ymmärtämään ja määrällisellä tutkimuksella puolestaan yleistämään. (Kananen 2014, 19-20, 26.)

Lähestymistavaksi oli valittu tapaustutkimus, koska siinä tutkitaan syvällisesti kohdetta sen omassa ympäristössä. Tutkimuksen tarkoituksena oli tuottaa yritykselle kehittämissuositus. (Ojasalo, Moilanen & Ritalahti 2015, 36-37.) Tapaustutkimukselle on olennaista saada selville suppeasta kohteesta enemmän tietoa. Tutkimuksen kohteita on usein vähän ja olennaista on, että tutkimuksen kohde on nähtävissä tietynä kokonaisuutena. (Ojasalo ym. 2015, 52-53.)

Tässä tutkimuksessa myös ennakoitiin tuloksia tapaustutkimusta, koska katse oli suunnattu tulevaisuuteen ja riskeihin valmistautumiseen. Ennakointi auttaa kuvaamaan päätöksistä aiheutuvia uhkia ja mahdollisuuksia sekä lisää päätöksenteon valinnanmahdollisuuksia (Ojasalo ym. 2015, 92).

5.1 Lähestymistapa

Olen työssä pienessä ohjelmistoajan yrityksessä, jossa on parhaillaan menossa ISO 27001 sertifikaattiin tähtäävä projekti. Projekti alkoi maaliskuussa 2024 ja olen ollut siinä alusta saakka mukana. Olen pääasiassa keskittynyt seuraamaan muun projektiryhmän työtä (liite 1), mutta minulle on myös annettu sertifikaattiin liittyviä tehtäviä. Ne eivät liity suoraan tähän opinnäytetyöhön, joten en käsittele niitä tässä sen yksityiskohtaisemmin. Kohdeyrityksen alkuperäinen tavoite oli saada sertifikaatti vuoden 2025 loppuun mennessä. ISO 27001 viitekehys ei erottele yrityksiä esimerkiksi yrityksen koon

mukaan vaan viitekehys on kaikille sama. Viitekehys on hyvin laaja ja pelkästään siihen tutustuminen vie paljon aikaa. Jokainen yritys päättää itse onko kuvattu toiminnallisuus sille tarpeellinen vai ei. Tämän työn tarkoituksena ei ole arvioida projektiryhmän työtä.

5.2 Aineiston hankintamenetelmät

Tässä työssä aineistoa on hankittu menetelmillä, jotka sopivat erityisesti laadulliseen tutkimukseen. Tavoitteena on, että kerätyn aineiston kautta tutkimuksen aihetta kyetään ymmärtämään paremmin ja kokonaisvaltaisemmin (Ojasalo ym. 2015, 105).

5.2.1 Havainnointi

Aineiston hankintamenetelmä on aluksi ollut osallinen havainnointi. Kuten Ojasalo ja muut (2015, 42) toteavat, havainnointi on suositeltava menetelmä kaikkeen kehittämistyöhön. Tarkkailemalla aitoja tapahtumia saa usein hyödyllistä tietoa. Havainnoinnin kautta tietoa saa kokonaisvaltaisesti ja prosesseja voi tarkkailla pidemmän ajan kuluessa (Paalumäki & Vähämäki 2010, 131). Tähän asti havainnointitekniikka on ollut strukturoimatonta, koska tarkoituksena on ollut saada mahdollisimman monipuolisesti tietoa asiasta (Ojasalo ym. 2015, 116). Kananen (2014, 65) huomauttaa, että havainnointi on työläs ja aikaa vievä tiedonkeruumenetelmä. Sen käyttö on kuitenkin perusteltua silloin, kun ilmiöstä ei ole tietoa tai sitä on vähän.

5.2.2 Aivoriihi

Toisena aineiston hankintamenetelmänä on käytetty aivoriihityöskentelyä. Se soveltuu tapaustutkimuksen aineiston hankintamenetelmäksi (Ojasalo ym. 2015, 55). Aivoriihityöskentely kävi tähän tutkimukseen hyvin, koska kohdeorganisaatiossa työskentelee useita asiantuntijoita, joilla on kokemusta ja näkemystä tietoturvasta ja riskienhallinnasta. Yhdessä tekeminen ja ideointi sitouttaa henkilökuntaa projektiin. Ojasalon ja kumppaneiden (2015, 40) mukaan osallistujilta vaaditaan tiivistä yhteistyötä ja keskinäistä ymmärrystä, jotta voi syntyä uusia toimivia käytännön ratkaisuja.

Uuden kehittäminen vaatii innovointia ja siinä ryhmätyöskentelyllä on tärkeä merkitys. Yhteisöllisten ideointimenetelmien avulla voidaan tuottaa uusia näkökulmia, ideoita ja ratkaisuja. On olennaista, että ilmapiiri on avoin ja positiivinen, mutta toiminnan tulee samalla olla myös tavoitteellista ja kurinalaista. On hyvä muistaa, että määrä synnyttää laatua ja suuressa joukossa on aina enemmän hyviä ideoita kuin pienessä joukossa. (Ojasalo ym. 2015, 158-160.)

5.2.3 Ideoita tekoälyltä

Ennen varsinaista tutkimusta kysyin myös Microsoftin Copilot-tekoälyapurilta vinkkejä riskienhallinnan seurantaan. Copilot perustuu GPT-4 tekoälymalliin, joka on OpenAI:n kehittämä (Emce 2023).

Copilotin vastaukset löytyvät liitteestä 2. Käytin tekoälyä suomeksi ja se luultavasti osaltaan rajoitti vastausten määrää. Muutenkin vastauksissa tuntui toistuvan samat elementit, vaikka kysyin vähän eri asioita. Yllättävää oli, että automatisointia ehdotettiin käytettäväksi riskienhallinnan seurannassa ja raportoinnissa. Sitä en ollut osannut itse aikaisemmin ajatella, mutta vastaus sinänsä kuulosti ihan järkevältä. Joskus reaaliaikaisesta datasta tai analytiikasta voisi olla hyötyä, jos tarkastellaan tietynlaisia riskejä esim. käyttölokien kautta voisi saada selville epäilyttäviä kirjautumisia yrityksen järjestelmiin.

Tekoälyä pyydettiin myös kertomaan yleisimmät haasteet riskienhallinnan seurannassa. Näistä vastauksista mielestäni puuttuu se olennainen eli henkilökunnan vaihtuvuus. Muut haasteet liittyivät pääosin siihen, että jotain puuttuu, joko resursseja, tietoja tai viestintää. Tällä lyhyellä keskustelulla Copilotin kanssa ei ainakaan löytynyt kovin paljoa uutta tai konkreettista tietoa siitä, miten riskienhallinnan seuranta kannattaisi järjestää.

5.3 Aineiston analyysimenetelmät

Tässä opinnäytetyössä käytettiin analyysimenetelmänä teemoittelua. Riskejä tarkasteltiin pääryhmittäin, jotta olisi helpompaa suunnitella seuranta ja jatkuvuutta. Kaikki riskit eivät ole samanarvoisia. Tässä työssä ei ollut tarkoitus yksityiskohtaisesti eritellä kaikkia mahdollisia riskejä.

5.4 Muut kehittämismenetelmät

Mukautettu skenaariotyöskentely oli tässä tutkimuksessa yksi kehittämismenetelmä. Tutkimuksessa ennakoitiin mahdollisia tulevia riskejä ja pohdittiin niille hallintakeinoja. Skenaarion kautta pystytään paremmin kuvittelemaan millaisia seurauksia eri päätöksillä ja valinnoilla voi olla (Ojasalo ym. 2015, 146-147).

6 Riskienhallinnan seurannan ja järjestämisen aivoriihi

Tutkimus toteutettiin aivoriihenä, jossa tutkimuksen tekijä toimi fasilitaattorina. Tutkimukseen osallistui tekijän lisäksi kuusi muuta henkilöä. Aivoriihi toteutettiin Teams-sovelluksella, koska osallistujat asuvat etäällä toisistaan. Aivoriihen kestoksi oli suunniteltu puolitoista tuntia ja tämä myös toteutui. Tutkimusalustana käytettiin Miro boardsia. Kuten Allah (2023, 86) on todennut, Miro on hyödyllinen työväline aivoriihityöskentelyssä. Tutkimuksen tekijä oli luonut Miroon valmiiksi kolme pohjaa, joita aivoriihessä käytiin läpi (kuva 4). Fasilitaattori toimi kirjurina ja täydensi post-it-lappuja reaaliaikaisesti.

Tutkimusryhmän osallistujat koostuivat yrityksen vakituisesta henkilökunnasta, ja he kaikki ovat olleet jossakin määrin mukana ISO 27001 standardiprojektissa. Anonymiteetin säilyttämisen vuoksi tutkimuksen tuloksissa ei tarkemmin eritellä kunkin osallistujan vastuualuetta tai annettuja vastauksia. Aivoriihen alussa fasilitaattori pyrki luomaan avointa ja rentoa ilmapiiriä, jotta osallistujat tuntisivat olonsa mukavaksi. Puheenvuoroja ei tarvinnut erikseen pyytää, vaan jokainen sai vapaasti kertoa ajatuksensa. Aivoriihen näkökulma koski tulevaisuutta ja hetkeä, jolloin kohdeyrityksellä on jo ISO 27001 standardi auditoituna. Miten riskienhallintatyötä kannattaisi jatkaa sen jälkeen?



Kuva 4. Tutkimuksen lähtötilanne Mirossa.

6.1 Ideoita riskienhallinnan seurantaan ja järjestämiseen

Ensimmäisellä Miro-taululla kerättiin ideoita siitä, miten riskienhallinnan seuranta kannattaisi auditoinnin jälkeen järjestää (kuva 5). Jokainen sai kertoa ideoitaan vapaasti ja fasilitaattori kirjasi niitä sitä mukaa ylös. Tulosten perusteella voi päätellä, että seurantaan kuuluu olennaisesti jonkinlainen valvonta, ajantasainen dokumentaatio, henkilöiden vastuuttaminen ja toimenpiteiden säännöllisyys. Ylipäätään riskien seuranta koettiin tärkeäksi ja sen tulisi olla osa johtoryhmätyöskentelyä. Häiriötilanteiden simuloinnilla ja henkilökunnan koulutuksella on myös merkittävä rooli. Riskiajattelua tulee levittää ja koettiin, että asioista täytyy olla tietoinen. Päävastuu on yrityksen hallituksella ja myös siellä ollaan kiinnostuneita riskienhallinnasta. Hallitukselle ehdotettiin vuosikelloa, jonka mukaan toimenpiteitä voisi säännöllisesti delegoida vastuuhenkilöille. Vastuuttamisen lisäksi pitää seurata sitä, että sovitut tehtävät etenevät. Osallistujat kokivat, että riskit pitäisi huomioida jo

suunnitteluvaiheessa eikä vasta toteutuksessa. Häiriötilanteiden sattuessa olisi selvitettävä tapahtuman juurisyy ja arvioida mahdolliset uudet riskit. Riskien seuranta erilaisilla mittareilla ja automaatioilla koettiin hyödylliseksi varsinkin teknisten riskien havainnoinnissa.



Kuva 5. Tutkimuksen ensimmäinen taulu Mirossa.

6.2 Millaisia haasteita voi tulla

Ideoinnin jälkeen osallistujia pyydettiin keskittymään siihen millaisia haasteita riskien seurannassa voisi tulla (kuva 6). Yleisimpänä pidettiin aikaa ja käytettäviä resursseja. Näiden lisäksi seuranta voi hankaloittaa riskien tunnistamisen vaikeus ja priorisointi. Muuttuva toimintaympäristö, esimerkiksi uudet palvelut ja lainsäädäntömuutokset, tuovat omat haasteensa. Riskien tunnistamiselle pitäisi olla selkeät kriteerit, jotta niiden tunnistaminen olisi systemaattista. Yrityksissä on paljon hiljaista tietoa, joka saattaa jäädä dokumentoimatta. Valitut toimenpiteet saattavat olla tehottomia. Kaikkia ei kiinnosta riskit samalla tavalla, mutta olisi tärkeää löytää keinot, joilla henkilökuntaa saisi motivoitua. Asenteet, sitoutumisen puuttuminen ja toimintatapakulttuuri saattavat myös aiheuttaa ongelmia.



Kuva 6. Tutkimuksen toinen taulu Mirossa.

6.3 Tarkastelu pääteemojen kautta

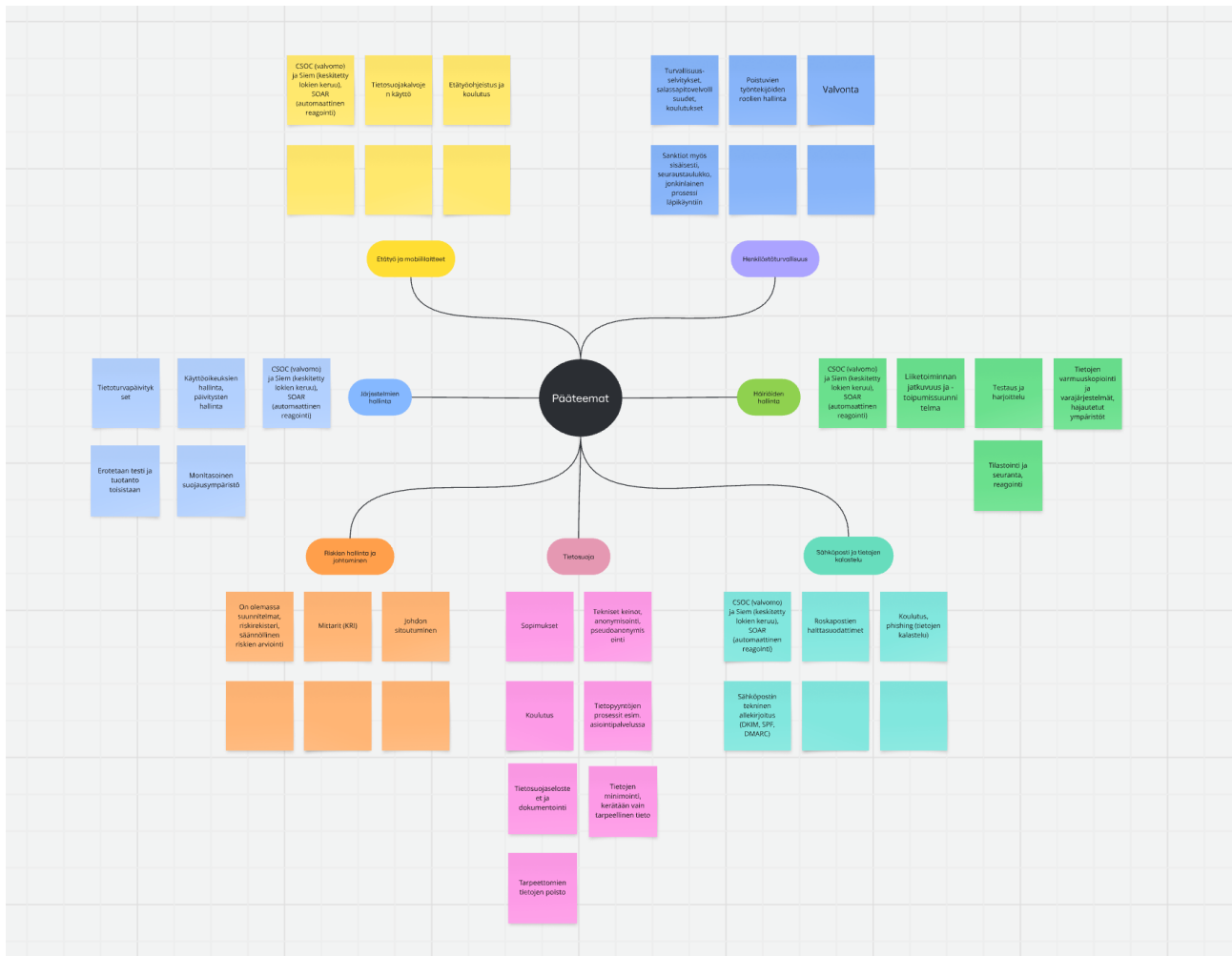
Kolmannella taululla keskityttiin tiettyihin riskipääryhmiin (kuva 7). Tarkoituksena oli pohtia pitäisikö eri riskipääryhmiin kohdistaa erilaista jatkuvuudenseurantaa vai voidaanko kaikkia ryhmiä seurata samalla tavalla. Mukaan oli valittu seuraavat pääryhmät:

- Etätyö ja mobiililaitteet.
- Henkilöstöturvallisuus.
- Häiriöiden hallinta.
- Järjestelmien hallinta.
- Riskien hallinta ja johtaminen.
- Sähköposti ja tietojenkalastelu.
- Tietosuoja.

Tämä taulu vaati enemmän pohdintaa ja välillä fasilitaattori tarkensi millaisia riskejä tietyn ryhmän piiriin kuului. Varsinkin teknisemmät pääryhmät kuten häiriöiden ja järjestelmien hallinta, etätyö ja mobiililaitteet sekä sähköposti ja tietojenkalastelu vaativat erityistä teknistä osaamista, jotta niitä pystyi arvioimaan. Edellä mainittuihin löydettiin yhteisesti sopivia keinoja kuten valvonta, keskitetty lo- kien keruu ja automaattinen reagointi. Sähköpostiin ja tietojenkalasteluun voidaan vaikuttaa myös roskapostisuodattimilla ja teknisillä allekirjoituksilla. Teknisillä allekirjoituksilla voidaan estää sähkö- postien väärentämistä.

Tietosuojaan liittyviä hallintakeinoja ovat sopimukset, anonymisoinnit, pseudonymisoinnit ja erilaiset tietopyyntöjen käsittelyprosessit, joiden tulee olla selkeitä ja hyvin dokumentoituja. Ylipäätään on hyvä muistaa, että kerätään aina vain tarpeellinen tieto eikä mitään ylimääräistä. Tietosuojaseloste mainittiin myös tietosuojan yhteydessä. Häiriöiden hallintaan liittyen liiketoiminnan jatkuvuussuunnitelma, toipumissuunnitelma, varmuuskopiot ja varajärjestelmät ovat olennaisia. Hajautetuilla ympäristöillä voidaan myös hallita mahdollisia häiriöitä.

Henkilöstöturvallisuuteen liittyen keskustelua aiheuttivat mahdolliset sisäiset sanktiot, joilla toivottiin olevan herättävä vaikutus. Riskitilanteista olisi pidettävä jonkinlaista seuraustaulukkoa sekä tilanteen jälkeen pitäisi olla prosessi läpikäyntiin, jotta mahdollinen toistuminen voidaan estää. Koulutus, testaus, ohjeistus ja harjoittelu myös liittyivät useampaan pääryhmään. Riskien hallintaan ja johtamiseen vaikuttaa johdon sitoutuminen sekä olemassa olevat suunnitelmat. Riskirekisteri sekä säännöllinen riskien arviointi ja erilaiset mittarit ovat tähän ryhmään liittyviä keinoja.



Kuva 7. Tutkimuksen kolmannen taulun pääryhmät Mirossa.

6.4 Pohdintaa toteutuksesta

Tutkimuksen osallistujien fyysisen etäisyyden ja tiukkojen aikataulujen vuoksi aivoriihi kannatti toteuttaa Teams-sovelluksella. Sen käyttö oli kaikille ennestään tuttua ja yhteinen aika oli helpompaa sopia, kun tutkimus ei vaatinut osallistujia siirtymään johonkin tiettyyn paikkaan. Teamsin käytön ongelmallisuus tuli esille siinä, että fasilitaattorin oli hankala havainnoida ketkä olivat oikeasti läsnä ja keskittyivät asiaan. Tutkimuksen aikana ei pidetty kameroita päällä. Fasilitaattori jakoi oman koneensa näyttöä ja toimi samalla kirjurina Miro-tauluille.

Tutkimuksen alussa keskustelu oli hyvin vilkasta ja lähes kaikki olivat äänessä. Osallistujien kesken oli rento ilmapiiri. Fasilitaattori pyrki huomioimaan myös hiljaisemmat osallistujat kysymällä suoraan heidän mielipiteitään. Teamsin kautta keskustelu voi jäädä vähän ontoksi. Kaikki eivät pääse heti ääneen, kun ajatus herää ja elekielen tulkinta on olematonta. Lähitilaisuudessa olisi helpompi havaita, jos jollakulla on sanottavaa. Osallistujien keskustelu laimeni selvästi viimeiselle taululle tultaessa. Syynä saattoi olla se, että taulun sisältöä oli vaikeampi hahmottaa eikä siinä käytetyt pääryhmät olleet kaikille selviä. Fasilitaattori pyrki avaamaan pääryhmien sisältöä tarvittaessa, jotta osallistujat tietäisivät mitä niihin kuului. Tässä kohtaa tutkimusta osallistujat, joilla oli laajemmat tekniset tiedot sekä enemmän kokemusta riskienhallintaan liittyvistä elementeistä, olivat selkeässä etulyöntiasemassa. He oikeastaan dominoivat keskustelua viimeisen taulun kohdalla.

Aivoriiehen oli tarkoituksella valittu heterogeeninen osallistujaryhmä yrityksen eri vastuualueilta. Tällä keinolla oli mahdollista saada erilaisia näkökulmia käsiteltävästä aiheesta. Ajatuksena oli myös jakaa nykyistä tietoa osallistujien kesken ja tätä kautta syventää jokaisen osaamista. Riskienhallinta on koko yrityksen projekti ja siksi on tärkeää, että kartutettua tietoa saadaan myös levitettyä. Tutkimusta olisi voinut laajentaa seuraavassa vaiheessa isommallekin joukolle ja katsoa millaisia tuloksia sieltä olisi tullut.

Tutkimus toteutettiin yhtenä 90 minuutin kokouksena. Jälkikäteen ajateltuna tutkimus olisi kannattanut jakaa kahteen 60 minuutin osioon ja ensimmäisessä käydä vain kaksi ensimmäistä taulua läpi. Kolmas taulu olisi vaatinut fasilitaattorilta tarkempaa ohjeistusta ja suunnittelua. Nyt siihen siirryttäessä osallistujien vireystila ei enää ollut parhaalla mahdollisella tasolla ja keskustelu tyrehtyi. Osallistujia olisi voinut myös osallistaa enemmän. Heidät olisi voinut jakaa kahteen kolmen hengen ryhmään ja ohjeistaa ryhmää keksimään ideoita ja haasteita. Ryhmätyön jälkeen tulokset olisi voitu käydä yhdessä läpi ja verrata niitä keskenään.

7 Tutkimuksen tulokset ja arviointi

Riskienhallinta on iso kokonaisuus, jossa on tärkeää aloittaa helpoimmasta ja tehdä pala kerrallaan. Kokonaisuutta voi olla hankala hahmottaa ja riskienhallinnan järjestäminen voi tuntua mahdottomalta tehtävältä. Liiketoiminnasta riippuen myös riskit vaihtelevat ja kuten aivoriihen tuloksista kävi ilmi, niin kaikkia riskiryhmiä ei voi hallita samalla tavalla. Paljon painoarvoa on sillä, että hallintaan liittyvä toiminta on säännöllistä, hyvin dokumentoitua ja mukana on sitoutuneita henkilöitä.

7.1 Tulosten suhde tavoitteisiin

Tutkimuksen tavoitteena oli löytää konkreettisia ideoita siitä, miten ISO-standardissa määritellyt prosessit ja mallit saadaan pysyvästi osaksi yrityksen toimintaa, jotta pystytään varmistamaan niiden jatkuvuus. Työssä keskityttiin riskienhallintaan, joka on yksi osa ISO-standardissa. Riskienhallinta vaatii aina aikaa ja resursseja, mutta näitä ei ole millään yrityksellä rajattomasti. Varsinkin pienillä ja keskisuurilla yrityksillä resurssit voivat olla ongelma. Jos henkilökunta on sitoutunut niin rooleja kannattaa jakaa ja näin levittää tietämystä laajemmin. Tämä helpottaa myös sitä, ettei tieto kasaannu vain harvoille. Säännöllisyys toiminnassa, oli se sitten harjoittelua, ohjeistusta tai seurantaa, on olennaista. Se voi tarkoittaa hallituksen vuosikelloa tai sitten jotain muuta yhteisesti sovittua aikaikkunaa. Myös kaikki dokumentointi kuten suunnitelmat, ohjeet ja koulutusmateriaalit pitää olla ajan tasalla ja jonkun vastuulla. Näitä ei voida tekniikalla automatisoida.

Nykytekniikalla on mahdollista hoitaa joitain osia riskienhallinnan jatkuvuuden seurannasta. Näitä kannattaisi ehdottomasti hyödyntää, jos sillä säästetään muita resursseja. Automaattiset ilmoitukset poikkeavuuksista voivat laukaista toimenpiteen, johon henkilökunta voi reagoida ja kohdistaa tarkempaa selvitystä. Näissä on olennaista se, että tiedetään miten edetään, kun jotain tapahtuu. Automaatiikka ei kuitenkaan korvaa täysin muuta valvontaa ja seurantaa vaan tarjoaa lähinnä lisäkeinoja.

Riskiajattelu kuuluu kaikille. Yleensä yrityksen johto kantaa lopullisen vastuun, mutta he eivät välttämättä ole mukana päivittäisessä operatiivisessa toiminnassa. Riskienhallintavastuu pitäisi jakaa niiden henkilöiden kesken, jotka ovat asiasta kiinnostuneita. On selvää, että kaikkia aihe ei kuitenkaan kiinnosta eikä siihen kannata ketään pakottaa. Syyt voivat olla monitahoiset ja on yrityksen etu, ettei vastuutehtävässä ole vastahakoinen työntekijä. Selkeät roolit ja vastuut nähtiin tärkeinä elementteinä, joilla on vaikutusta henkilöiden sitoutumiseen.

Yrityksen tulisi aina olla varautunut siihen, että henkilökunnassa voi tapahtua muutoksia. Kenestäkään ei saisi tehdä korvaamatonta. Tietoa pitäisi pystyä jakamaan mahdollisimman monelle. Prosessien ja toimintojen pitäisi olla hyvin dokumentoitua. Pienissä yrityksissä helposti käy niin, että

tieto siiloutuu eikä leviä laajemmin. Yrityksen näkökulmasta tämä ei ole hyvä asia ja siiloutumista pitäisi välttää. Myös hiljaista tietoa pitäisi pystyä jakamaan ja tarpeen mukaan luoda uusia prosesseja. Yrityksen täytyy pitää itsensä toimintakykyisenä.

7.2 Tulosten käytettävyys

Tutkimuksen lopputuloksena ei ole mitään yhtä selkeää toimenpidettä, jolla riskienhallinnan ja jatkuvuuden voi saada hallintaan. Aineistosta kuitenkin nousee esiin tiettyjä teemoja, joihin on hyvä kiinnittää huomiota ja ne samat asiat toistuivat myös teoreettisessa viitekehyksessä. Tällaisia ovat säännöllisyys seurannassa ja valvonnassa, hyvät dokumentoinnit ja motivoitunut henkilökunta. Näiden lisäksi jokaisen täytyy ymmärtää miksi riskienhallintaa ylipäätään tehdään. Yrityksen johdon on pidettävä tätä tavoitetta esillä ja mahdollistettava käytettävät resurssit. Tutkimuksen tulokset ovat sen verran yleisluontoisia, että ne eivät ole kohderiippuvaisia vaan yleistettävissä muihinkin yrityksiin, joissa riskienhallintaa halutaan tehdä.

Tutkimuksessa sivuttiin ISO 27001 -sertifikaattia, mutta sen sisältöön tai tarkoitukseen ei syvennytty tarkemmin. Näin ollen tuloksista ei voi vetää suoria johtopäätöksiä kyseisestä sertifikaatista tai sen tarpeellisuudesta. Sertifikaatti on ohjeistus, jolla yritys voi todentaa riskien olevan hyvin hallinnassa ja liiketoiminnan turvattu. On hyvä muistaa, että yrityksen täytyy itse haluta panostaa tähän ja ymmärtää tehtävän työn hyödyllisyys.

7.3 Tulosten suhde tutkimuskysymyksiin

Ensimmäisessä tutkimuskysymyksessä kysyttiin miten määritellään yrityksen riskit (K1). Tähän vaikuttaa olennaisesti yrityksen liiketoimintaympäristö ja jokaisen yrityksen täytyy määritellä itse omat riskinsä. Erilaisten viitekehysten kautta on mahdollista saada apua määrittelyyn, mutta loppupeleissä jokainen yritys tekee päätöksensä itsenäisesti. Yrityksen sietokyvystä riippuu miten se voi sietää erilaisia riskejä.

Toisessa tutkimuskysymyksessä mietittiin onko ISO 27001 -sertifioinnista apua yrityksen riskienhallinnalle (K2). Sertifiointi ja siihen kuuluvat auditoinnit patistavat yrityksiä tekemään tiettyjä asioita oikein ja säännöllisesti. Yrityksestä itsestään täytyy kuitenkin löytyä halua toimia näin eikä pelkkä sertifiointi riitä siihen. Sertifiointi voidaan kokea ylimääräisenä byrokratiana, mutta se on tavallaan kirsikka kakun päällä, kun asiat ovat kunnossa. Prosessit ja mallit täytyy tehdä yrityksen tarpeita varten. Sertifiointi voi tarjota yritykselle kilpailuetua, jos muilla samalla alalla toimivilla ei sitä vielä ole, mutta sen ylläpito vaatii jatkuvaa työtä. Jos yritys on saanut sertifikaatin, sen kannattaa pitää prosessit ja dokumentit kunnossa jatkoauditointeja varten, koska suurin ponnistus on jo tehty. Sertifikaatti voi osoittautua myöhemmin hyödylliseksi ja ainakin sillä on saatu tarpeelliset prosessit jo kertaalleen kuntoon. Paljon riippuu myös yrityksen toimialasta. Varsinkin it-alalla sertifiointit ovat

yleisiä ja niitä osataan vaatia, mutta on monia muita aloja, joissa vastaavaa vaatimusta ei ainakaan vielä ole.

Kolmannessa tutkimuskysymyksessä pohdittiin miten varmistetaan riskienhallinnan seuranta ja jatkuvuus (K3). Tämä oli tutkimuksen hankalin kysymys eikä siihen ole mitään yksiselitteistä vastausta. Seuranta vaatii useita elementtejä onnistuakseen. Mielestäni olennaisia ovat säännöllisesti tehtävät toimenpiteet, ajantasaiset dokumentit ja ohjeistukset sekä roolinsa tunnistava ja motivoitunut henkilökunta. Näiden pohjalta jokaisen yrityksen on mahdollista tehdä omat tarkemmat prosessinsa ja mallinsa, joilla toteuttaa seurantaa ja jatkuvuutta. Pointti onkin oikeastaan siinä, että nämä ovat asioita, joita täytyy tehdä. Ne eivät toteudu itsestään vaan ne vaativat aktiivista toimijuutta. Yhtälö voi tuntua työläältä, mutta se ei ole mahdotonta.

7.4 Tulosten suhde lähdeteoriaan

Riskienhallinnasta on olemassa paljon lähdekirjallisuutta. Aihe ei ole mitenkään uusi, riskien on ymmärretty olevan osa yritysten toimintaa, mutta niihin varautuminen on ehkä uudempi näkökulma. Digitalisaatio on luonut uudenlaisia riskejä ja varsinkin kyberturvallisuudesta on kirjoitettu viime vuosina paljon. Suomenkielinen kirjallisuus näytti liittyvän enemmän yritysten yleiseen riskienhallintaan ja sieltä löytyi hyvin perustaa teoreettiselle viitekehykselle.

Kuten Martikainen & Ranta (2020, 17) ovat todenneet, yrityksen turvallisuuskulttuuri vaatii vahvaa sitoutumista koko henkilöstöltä. Turvallisuuskulttuuri pohjautuu turvallisuuteen liittyviin perusoletuksiin ja arvoihin. Aivoriihen tulokset ovat samoilla linjoilla. Henkilökunnan sitoutumisella ja yrityksen sisällä vallitsevalla riskiajattelulla on suuri merkitys ja molempia tarvitaan, jotta yritys voi onnistua riskienhallinnassa. Yrityksen sisällä tarvitaan ymmärtämistä ja yhteistä termistöä ja sanastoa (Ilmonen ym. 2022, luku 2.1).

Yrityksen hallitukselle kuuluu kokonaisvastuu riskienhallinnan järjestämisestä (Suomen Standardisoimisliitto SFS ry 2021, 28). Hallitus tarvitsee kuitenkin avukseen muita vastuuhenkilöitä ja nimettyjä rooleja, jotta riskienhallinnan järjestäminen on mahdollista. Aivoriihessä todettiin, että vastuuttaminen on erittäin olennaista. Silloin kun roolit ovat selkeitä niin kenenkään ei tarvitse ihmetellä kelle asia kuuluu. Liian usein käy niin, että asiat jäävät hoitamatta, jos ne eivät varsinaisesti kuulu kenenkään työpöydälle. Ilmonen ja muut (2022, luku 2.3) muistuttavat, että jokainen yritys määrittelee itse riskienhallintavastuut ja käytännöt sekä huolehtii siitä, että velvollisuudet ja vastuut pysyvät erillään.

Riskienhallinnan toteuttaminen vaatii yritykseltä riittävät henkilöresurssit (Ilmonen ym. 2022, luku 2.1). Resurssit koettiin aivoriihessä suurena haasteena, niitä ei tunnu koskaan olevan tarpeeksi. Tekemistä on aina enemmän kuin tekijöitä, vaikka tahtoa löytyisikin. Pienissä alle 50 hengen

y yrityksissä harvemmin on henkilöitä, joilla olisi täysipäiväisesti aikaa paneutua riskienhallintaan. Kokonaisuutta ei oikeastaan edes kannattaisi laittaa vain yksille harteille vaan vastuuta pitäisi jakaa mahdollisimman monelle. Myös dokumentointi mainittiin lähdekirjallisuudessa samoin kuin aivoriihessä. Dokumentaatiota täytyy ensinnäkin olla olemassa ja se täytyy pitää ajan tasalla. Auditoinneissa tarkastellaan myös dokumentaatioita ja se on yksi olennainen osa tässä kokonaisuudessa.

Yrityksen täytyy kyetä mittaamaan onko turvallisuustavoitteissa edistytty. Olennaista on silloin tunnistaa mitä mitataan, miten mitataan ja milloin mitataan. Tietoturvan hallintajärjestelmän pitää toimia myös reaali maailmassa. (Calder 2024, luku 8.) Myös aivoriihessä huomautettiin valvonnan ja seurannan tarpeellisuudesta. Se ei vielä riitä, että yrityksestä löytyy olennaiset prosessit ja dokumentaatiot, niitä täytyy myös säännöllisesti valvoa ja harjoitella. Tähän ohjaa myös sertifikaatin vaatimat säännölliset sisäiset ja ulkoiset auditoinnit. Riskienhallinnan tilanteita voi testata esimerkiksi simuloimalla, mutta tämäkin tulee tehdä hallitusti.

7.5 Tutkimuksen uskottavuus, eettisyys ja luotettavuus

Laadullisen tutkimuksen luotettavuuden arviointiin liittyy kolme käsitettä: uskottavuus, eettisyys ja luotettavuus. Uskottavuudella tarkoitetaan sitä voiko tutkimuksen kohteena oleva yritys hyväksyä tutkimuksen tulokset tosiksi ja luottaa siihen, että aineisto on analysoitu huolellisesti. Tutkimuksen lukijoiden tulee olla vakuuttuneita siitä, että tutkimus on tehty asianmukaisesti. Eettisyydellä tarkoitetaan, että tutkija on noudattanut tutkimuksessaan eettisiä periaatteita eikä tutkimuksesta saa aiheutua haittaa tutkimuksen kohteena oleville tahoille. Luotettavuudella tarkoitetaan, että tutkimuksessa on käytetty perusteltuja ja oikeanlaisia lähestymistapoja sekä tutkimuksen eteneminen kuvataan juuri sellaisena kuin se on toteutunut. (Puusa & Juuti 2020, luku 5.)

Tutkimuksen dokumentointiin on kiinnitetty huomioita ja työn eri vaiheita on kuvattu mahdollisimman tarkasti. Aivoriihen osalta lähtötilanne ja lopputulokset on liitetty aineistoon myös kuvina. Tutkimuksen luotettavuutta on varmistettu asianmukaisilla lähteillä. Lähteiden valinnassa on kiinnitetty huomiota niiden ajantasaisuuteen sekä aiheen kannalta merkityksellisyyteen. Lähdemerkinnöissä on noudatettu asianmukaisia lähdeviittauskäytäntöjä. Tutkimuksen tuloksista ei voi todeta olevan haittaa tutkimuksen kohteena oleville tahoille.

7.6 Käytetyt metodit

Tutkimus aloitettiin osallisella havainnoinnilla ja sitä jatkettiin koko tutkimuksen ajan. Ilman havainnointia tutkimuksen tekijän lähtötiedot olisivat olleet paljon hatarammalla pohjalla. Kokonaisuus alkoi kuitenkin paremmin hahmottua vasta opinnäytetyön teoreettisen viitekehyksen myötä. Eri lähteistä kävi ilmi, että riskienhallinta on tarpeellinen, mutta työläs toimenpide, johon eri osapuolten täytyy sitoutua.

Toisena aineiston hankintametodina oli aivoriihi. Tutkimuksen tekijän näkökulmasta se oli hyödyllinen juuri tällaiseen tapaustutkimukseen, jossa kehitetään uusia työmenetelmiä. Yhdessä ideointi ja pohtiminen oli aivoriihessä mutkatonta ja tunnelma pysyi rentona. Aivoriihen osallistujille tilaisuus vaikutti olevan hyödyllinen, ja he saivat uusia näkökulmia asiaan. Aivoriihessä oli mukana monen eri vastuualueen henkilöitä, joten keskustelu oli monipuolista. Aivoriihi olisi voinut onnistua vieläkin paremmin, jos se olisi toteutettu lähitilaisuutena parissa lyhyemmässä erässä. Silloin osallistujat olisivat ehtineet pohtia aihetta enemmän, ja siitä olisi varmasti ollut heille hyötyä. Jos tutkijalla olisi ollut enemmän aikaa, olisi ollut mielenkiintoista haastatella aivoriihen osallistujia jälkikäteen ja kuulla heidän mielipiteensä ja oma arvionsa tilaisuudesta.

7.7 Oppiminen

Tutkimus on tuonut tekijälleen paljon uutta tietoa riskienhallinnasta ja jatkuvuudesta. Sekä myös aiheuttanut hämmennystä siitä, miten isosta kokonaisuudesta todella on kyse. Ei olekaan siis ihme, että varsinkin pienemmissä yrityksissä joudutaan miettimään todella tarkkaan ISO 27001 -sertifioinnin hyötyjä ja kustannuksia. Tästä keskusteltiin myös aivoriihessä. Pieni yritys joutuu punnitsemaan mahdollisia sertifikaatista saatavia etuja omalla markkina-alueellaan ennen kuin se voi sitoutua varsin pitkäkestoiseen projektiin. Jokainen yritys varmasti haluaa näyttää, että heillä asiat on hoidettu asianmukaisesti, mutta vaakakupissa painavat aina myös kustannukset ja käytettävissä olevat resurssit.

Tutkimuksen tekijänä odotin tutkimuksesta nousevan jotain konkreettista ja selkeää lopputulosta, mutta näin ei oikeastaan käynyt. Riskienhallinta vaatii paljon työtä eikä sitä voi kiertää tällä hetkellä mitenkään. Olennaista on, että työtä aletaan tekemään, koska muuten tuloksia ei synny. Yrityksen johdon ja muun henkilökunnan pitää olla sitoutuneita, jotta riskienhallintaa ylipäättään on mahdollista edistää. Jokaisen yrityksen tulee itse päättää miten paljon resursseja sillä on käytettävissään ja missä aikataulussa se haluaa edetä. Kun on kyse isosta kokonaisuudesta niin silloin kannattaa aloittaa helpoimmista tehtävistä ja tehdä pala kerrallaan. On myös tärkeää heti alusta lähtien jakaa vastuuta useammalle henkilölle, jotta kaikki ei ole yhden henkilön harteilla.

7.7.1 Tulosten vertailua tekoälyn generoimiin

Tutkimuksen jälkeen halusin vielä selvittää onko ChatGPT tekoälyn vastauksissa eroja Copilotiin verrattu. ChatGPT:ssä käytettävän tekoälymallin voi itse valita ja valitsin sieltä GPT-4o. ChatGPT:lle esitettiin suomeksi samat kysymykset samassa järjestyksessä kuin aikaisemmin Copilotille. Tämän tekoälyn antamat vastaukset löytyvät liitteestä 3. Vastauksien ulkoasua on stilisoitu, mutta muuten vastauksia ei ole muokattu.

Ensimmäisenä kysyttiin miten riskienhallinnan seuranta kannattaisi toteuttaa. Molempien vastauksissa oli samoja elementtejä kuten tavoitteiden tunnistaminen ja arviointi, seuranta ja mittarit, raportointi ja jatkuva parantaminen sekä sidosryhmien vastuuttaminen ja koulutus. ChatGPT ehdotti lisäksi erilaisia digitaalisia työkaluja, joista voisi olla hyötyä. Copilotilta ei tullut vastaavaa ehdotusta.

Toisena kysyttiin millainen olisi hyvä seurantajärjestelmä. ChatGPT ehdotti ensimmäisenä keskitettyä riskirekisteriä ja neuvoi mitä siihen kannattaa kirjata. Lisäksi se tarjosi muutaman esimerkin seurantajärjestelmän toteutustavoista ja mainitsi jälleen eri työkaluja. Osa ehdotetuista työkaluista eivät ole ennestään tuttuja, joten en pysty arvioimaan niiden soveltuvuutta. Copilotin vastaus oli yleisempi eikä siinä menty yksityiskohtiin. ChatGPT:n vastauksesta oli mahdollista löytää enemmän käytännön neuvoja.

Kolmantena haluttiin tietää mitkä ovat yleisimmät haasteet seurannassa. Tässä molempien vastaukset olivat samansuuntaisia, vaikka ne oli muotoiltu vähän eri sanoin. Pääosin syynä pidettiin sitä, että jotain puuttuu. Tällaisia ovat esim. resurssien, sitoutumisen, reagoinnin tai mittareiden puute. ChatGPT tarjosi lopuksi vielä keinoja, joilla haasteita voi ehkäistä. Näistä ainakin jatkuva parantaminen ja vastuuhenkilöiden nimeäminen ovat olennaisia.

Neljäs kysymys oli miten voisi kehittää seurantajärjestelmää. ChatGPT:n vastaukset näyttävät tehtävälialta, jossa oli mainittu ihan hyviä yksityiskohtia kuten rakenteen prosessivaiheet, joista voisi olla hyötyä. Jälleen vastauksessa suositeltiin eri työkaluja ja ne olivat osittain samoja kuin aikaisemminkin. Copilotin vastaukset olivat samalla linjalla kuin aikaisemmin eli paljon yleisluontoisempia kuin ChatGPT:llä.

Vaikuttaa siltä, että ChatGPT tarjoaa yksityiskohtaisempia vastauksia kuin Copilot ja jostain syystä suosittelee tiettyjä ohjelmistoja hyvinkin usein. Vaikea sanoa miksi juuri nämä tietyt ohjelmistot on valittu. Erikoista on, että näistä osa on Microsoftin ohjelmia, mutta silti Copilot ei maininnut niitä omassa vastauksissaan. Molempien vastauksista löytyi paljon samoja teemoja, jotka olivat aikaisemmin tulleet esille myös lähdekirjallisuudessa. Sen puolesta molempien tekoälyjen antamat vastaukset vaikuttavat ihan relevanteilta.

8 Johtopäätökset

Riskit eivät ole katoamassa minnekään vaan niiden kanssa täytyy opetella elämään. Riskit eivät ole samanlaisia kaikille yrityksille. Siksi olisikin tärkeää, että yrityksen johto ymmärtää mitä riskienhallinta tarkoittaa ja miten yritys voi hyötyä siitä. Yrityksen kannattaa ottaa riskienhallinta osaksi jatkuvaa toimintaansa riippumatta siitä onko tähtäimessä joku tietty sertifiointi vai ei. Joka tapauksessa riskienhallintatyöstä on yritykselle hyötyä. On tärkeää tunnistaa omaan toimintaan liittyvät riskit ja varautua niihin mahdollisuuksien mukaan. Myös jatkuvuudesta täytyy huolehtia, koska yrityksen toimintaympäristö ei pysy stabiilina. Riskit muuttuvat ja niitä pitää säännöllisesti arvioida uusiksi. Kuten huomattiin Covid-pandemian aikana, maailma voi muuttua hyvinkin yllättäen ja vaikutukset voivat olla dramaattisia. Jos yrityksen tekemä työ halutaan tehdä näkyväksi myös omille sidosryhmille, voi olla järkevää panostaa sertifiointiin.

Kuten Lam (2017, luku 6) totesi, on tärkeää löytää juuri oikeat henkilöt. Olen tästä samaa mieltä. Tähän voidaan kiinnittää huomiota esimerkiksi jo työntekijöiden rekrytoinnissa ja painottaa erityisesti olennaisia tietoja tai koulutusta. Haastattelun myötä saa tarkempaa kuvaa henkilön asenteista ja aikaisemmasta kokemuksesta. Kun henkilökunta on sitoutunutta ja motivoitunutta, riskiajattelua voi olla helpompi tehdä kaikille tunnetuksi. Muuten siitä voi tulla kivireki, jota vain harvat ja valitut vetävät. Riskeistä täytyy olla tietoinen ja ne vaativat tietynlaista ajattelutapaa. Ei kuitenkaan tarvitse olla teknisesti taitava, jotta riskejä voi ymmärtää.

8.1 Jatkokehittämisajatukset

Kohdeorganisaatiossa riskienhallintaan liittyvää työtä on tehty tietyn projektiryhmän kesken ja heillä alkaa olla jo paljon tietoa aiheesta. Tutkimuksen jatkokehityksenä olisikin mielenkiintoista viedä tätä tietoa myös muulle henkilökunnalle ja katsoa millaisia ajatuksia ja ideoita heiltä nousisi. Onhan mahdollista, että henkilökunnassa on jo paljon tietämystä, mutta se ei vain ole tullut esille. Tietämystä pitäisi ehdottomasti laajentaa ja näkisin, että siinäkin aivoriihi voisi olla ensimmäinen työskentelytapa. Osallistujat kannattaisi jakaa pienempiin ryhmiin ja antaa heille tarkasti rajattuja ongelmia ratkaistavaksi ja näin tuoda riskienhallintaa tutuksi kaikille.

Työntekijät hyötyisivät myös riskienhallinnan peruskoulutuksesta, jossa käytäisiin ensin perusteita läpi ja ylipäättään pohjustettaisiin riskiajattelua - miksi se on tärkeää. Kaikkien pitäisi olla tietoisia mitä sillä tarkoitetaan. Kun ajatukset on viritetty oikealle taajuudelle niin samalla saadaan muokattua asenteita ja yrityksen kulttuuria. Usein saatetaan kuvitella, ettei tietyt riskit koske juuri meitä. Ihmisten oletetaan toimivan loogisesti ja tietyllä tavalla. Tämä ei kuitenkaan pidä paikkaansa. Asenteita ja tapoja ei ole helppo muuttaa, siihen tarvitaan paljon tietoa, esimerkkejä ja harjoittelua.

Kohdeorganisaation henkilökunnan ikäjakauma on 20-60 ikävuoden välillä. Henkilökunnassa on nuoria aloittelijoita sekä vanhempia konkareita. On oletettavaa, että nämä ryhmät ajattelevat asioista eri tavalla ja tämä koskee myös riskienhallintaa. Nuorilla saattaa olla tuoreita ideoita ja vanhemmilla taas käytännön tuomaa kokemusta. Myös teknisissä taidoissa on varmasti eroja. Olisi hyödyllistä saada nämä ryhmät kohtaamaan toisensa ja tekemään yhteistyötä yrityksen riskienhallinnan eteen.

Lähteet

Allah, R. K. 2023. The Use of Miro in Teaching Practice. *Exchanges: The Interdisciplinary Research Journal*, 10(3), 77–91. <https://doi.org/10.31273/EIRJ.V10I3.1277>. Luettu: 26.4.2025.

Aven, T. & Thekdi, S. 2022. *Risk science: an introduction*. Routledge. London.

Bissonette, M. 2016. *Project Risk Management: A Practical Implementation Approach*. Project Management Institute. E-kirja. Luettu: 19.4.2025.

Calder, A. 2024. *Nine Steps to Success – An ISO 27001:2022 Implementation Overview*. IT Governance Publishing Ltd. E-kirja. Luettu: 8.3.2025.

Culot, G., Fattori, F., Podrecca, M. & Sartor, M. 2019. Addressing Industry 4.0 Cybersecurity Challenges. *IEEE engineering management review*, 47(3), 79-86. Luettu: 9.3.2025.

Digi- ja väestötietovirasto 2022. Sanastot. Luettavissa: <https://sanastot.suomi.fi/terminology/digiriski>. Luettu: 12.5.2025.

Digiturvamalli. s.a. ISO 27001:2013. Luettavissa: <https://www.digiturvamalli.fi/vaatimuskehikot/iso-27001>. Luettu 22.9.2024.

Emce 2023. Mikä on Microsoft 365 Copilot ja miten se muuttaa tekemistämme? Luettavissa: <https://ajankohtaista.emce.fi/mik%C3%A4-on-microsoft-365-copilot-ja-miten-se-muuttaa-tekemist%C3%A4mme>. Luettu: 1.5.2025.

Hillson, D. 2023. *The risk management handbook: a practical guide to managing the multiple dimensions of risk (Second edition)*. Kogan Page. London.

Hopkin, P. & Thompson, C. 2022. *Fundamentals of risk management: understanding, evaluating and implementing effective enterprise risk management*. Sixth edition. Kogan Page. London.

Iivari, M. & Laaksonen, M. 2009. *Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen*. Tietosanomaa Oy. Helsinki.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2022. *Johda riskejä: käytännön opas yrityksen riskienhallintaan*. 4. päivitetty painos. Finva Finanssi- ja vakuutuskustannus. E-kirja. Luettu: 11.1.2025.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Kämppe, P. & Talala, T. 2023. *Yrityksen riskienhallinta*. 3. päivitetty laitos. Aalto University Executive Education Oy.

- Kamil, Y., Lund, S., & Islam, M. S. 2023. Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and E-Business Management*, 21(3), 699–722. Luettavissa: <https://doi.org/10.1007/s10257-023-00646-y>. Luettu: 1.2.2025.
- Kananen, J. 2014. Laadullinen tutkimus opinnäytetyönä. Jyväskylän ammattikorkeakoulu. Jyväskylä.
- Kananen, J. 2019. Opinnäytetyön ja pro gradun pikaopas. Jyväskylän ammattikorkeakoulu. Jyväskylä.
- Kang, M-C. 2014. Responsive security: be ready to be secure. CRC Press/Taylor & Francis. Boca Raton. E-kirja. Luettu: 9.3.2025.
- Kokonaisturvallisuuden sanasto. 2017. Sanastokeskus TSK ry. Helsinki. Luettavissa: https://turvalisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf. Luettu: 1.2.2025.
- Lam, J. 2017. Implementing Enterprise Risk Management. John Wiley & Sons, Incorporated. E-kirja. Luettu: 21.4.2025.
- Leflar, J. J. 2021. Change management for risk professionals. CRC Press. Boca Raton.
- Martikainen, S. & Ranta, T. 2020. Varautuva, ennakoiva oppilaitos ja korkeakoulu: jatkuvuuden turvaaminen arjen normaalioloista poikkeusoloihin. Laurea-ammattikorkeakoulu. E-kirja. Luettavissa: <https://urn.fi/URN:ISBN:978-951-799-577-1>. Luettu: 2.2.2025.
- Monahan, B. 2023. Strategic corporate crisis management: building the unconquerable organization. Routledge. New York.
- Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. Sanoma Pro Oy. E-kirja. Luettu: 8.4.2025.
- Paalumäki, A. & Vähämäki, M. 2010. Havainnointi organisaatiotutkimuksessa. Teoksesta: Puusa, A. & Juuti, P. Laadullisen tutkimuksen näkökulmat ja menetelmät. Gaudeamus. Helsinki.
- Puusa, A. & Juuti, P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Gaudeamus. Helsinki. E-kirja. Luettu: 27.4.2025.

SFS Suomen Standardit ry. s.a. ISO/IEC 27000 Tietoturvallisuuden standardisarja. Luettavissa: <https://sfs.fi/standardeista/tutustu-standardeihin/suosittu-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/>. Luettu: 6.1.2025.

Singh, N. 2022. Developing Business Risk Resilience through Risk Management Infrastructure: The Moderating Role of Big Data Analytics. *Information Systems Management*, 39(1), 34–52. Luettavissa: <https://doi.org/10.1080/10580530.2020.1833386>. Luettu: 18.4.2025.

Suomen Standardisoimisliitto SFS ry. 2021. SFS-käsikirja 18:2021. Riskienhallinta ja liiketoiminnan jatkuvuus.

Liitteet

Liite 1. Havainnointipäiväkirja

Kevät 2024

Aloitettiin Digiturvamallin avulla käymään läpi ISO 27001 vaatimuskehikkoa. Lisättiin ulkoisia tietosuojavarantoja ja asiakkaita Digiturvamallin tietosuojadokumentaatioon. Terminologian ja mallin hahmottamisessa vaikeuksia. Vaatimuskehikko on laaja. Projekti etenee hitaasti muiden töiden vuoksi. Kokeiltiin myös toista työkalua vaatimuskehikon hallintaan (Kiwa Comply) ja tultiin siihen tulokseen, että valmiit työkalut eivät olleet meille sopivia.

Syksy 2024

Tutustumista hallituksen politiikkadokumentteihin. Tutkittiin muiden yritysten julkisia poliitikkoja. Jaettiin projektiryhmän kesken aihealueet, joita kukin valmisteli itsenäisesti. Tietoturvan riskianalyysiä varten luotiin excel, jossa riskit oli jaoteltu kategorioittain. Riskikohtaisesti määritellään syy, lopputulos, hallintakeino, vaikutus, todennäköisyys, vakavuus ja riskiluokitus. Riskianalyysin täyttö aloitettiin fyysisestä tietoturvallisuudesta.

Talvi 2025

Projektiryhmän palaverit siirtyvät jatkuvasti muiden töiden vuoksi. ISO 27001 projekti ei juuri etene marraskuun 2024 ja helmikuun 2025 välisenä aikana. Maaliskuussa 2025 pidetään pitkää aikaa palaveri ja päätetään edistää asiaa. Tehtäviä jaetaan uusiksi ja tilannepalaverit varataan valmiiksi kalenteriin.

Kevät 2025

Standardin aikataulu tulee venymään eikä kaikkia osioita saada valmiiksi vuoden 2025 loppuun mennessä. Projektiryhmä jatkaa säännöllisiä tilannepalavereita ja vie projektia eteenpäin.

Liite 2. Copilot-tekoälypurin tuottamat vastaukset 8.4.2025

Copilotin käyttämä tekoälymalli on GPT-4.

Miten riskienhallinnan seurantaan kannattaisi toteuttaa?

Copilot

Riskienhallinnan seuranta on tärkeä osa organisaation riskienhallintaprosessia. Tässä muutamia keskeisiä vaiheita ja käytäntöjä, joita voit hyödyntää:

1. **Riskien tunnistaminen ja arviointi:** Aloita tunnistamalla ja arvioimalla organisaatiosi riskit. Tämä vaihe sisältää riskien analysoinnin ja niiden vaikutusten sekä todennäköisyyksien arvioinnin ¹.
2. **Seurantamittareiden määrittäminen:** Määrittele selkeät mittarit, joiden avulla voit seurata riskien kehitystä. Näitä voivat olla esimerkiksi riskin toteutumisen todennäköisyys, vaikutuksen vakavuus ja riskienhallintatoimenpiteiden tehokkuus ¹.
3. **Säännöllinen raportointi:** Laadi säännölliset raportit, joissa käsitellään riskienhallinnan tilaa. Raportit voivat sisältää tietoa uusista riskeistä, toteutuneista riskeistä ja riskienhallintatoimenpiteiden vaikutuksista ¹.
4. **Jatkuva parantaminen:** Hyödynnä P-D-C-A (Plan-Do-Check-Act) -menetelmää, joka on osa ISO 31000 -standardia. Tämä menetelmä auttaa jatkuvassa parantamisessa ja varmistaa, että riskienhallintaprosessi pysyy ajan tasalla ².
5. **Koulutus ja viestintä:** Varmista, että kaikki organisaation jäsenet ovat tietoisia riskienhallintakäytännöistä ja -prosesseista. Säännöllinen koulutus ja viestintä auttavat ylläpitämään riskitietoisuutta ja varmistamaan, että kaikki toimivat yhteisten tavoitteiden mukaisesti ¹.

Näiden vaiheiden avulla voit luoda tehokkaan ja kattavan riskienhallinnan seurantarjestelmän. Onko sinulla jotain erityistä riskiä tai tilannetta mielessä, johon kaipaisit tarkempia neuvoja?

Millainen olisi hyvä seurantarjestelmä?

Copilot

Hyvä riskienhallinnan seurantarjestelmä sisältää useita keskeisiä elementtejä, jotka varmistavat tehokkaan ja kattavan riskienhallinnan. Tässä muutamia tärkeitä ominaisuuksia:

1. **Selkeät tavoitteet ja mittarit:** Määrittele selkeät tavoitteet ja mittarit, joiden avulla voit seurata riskienhallinnan edistymistä. Tämä auttaa arvioimaan, kuinka hyvin riskienhallintatoimenpiteet toimivat ¹.
2. **Jatkuva seuranta ja raportointi:** Toteuta jatkuva seuranta ja säännöllinen raportointi. Tämä tarkoittaa riskienhallinnan tilan ja toimenpiteiden vaikutusten säännöllistä tarkastelua ja dokumentointia ².
3. **Kattava dokumentaatio:** Pidä kattavaa dokumentaatiota kaikista riskeistä, niiden arvioinneista ja hallintatoimenpiteistä. Tämä auttaa varmistamaan, että kaikki riskit ja niiden hallinta ovat hyvin dokumentoituja ja helposti saatavilla ³.
4. **Automatisointi:** Hyödynnä automatisoituja järjestelmiä ja työkaluja, jotka helpottavat riskienhallinnan seurantaan ja raportointia. Tämä voi sisältää esimerkiksi riskienhallintaohjelmistoja, jotka tarjoavat reaaliaikaista dataa ja analytiikkaa ².
5. **Koulutus ja viestintä:** Varmista, että kaikki organisaation jäsenet ovat tietoisia riskienhallintakäytännöistä ja -prosesseista. Säännöllinen koulutus ja viestintä auttavat ylläpitämään riskitietoisuutta ja varmistamaan, että kaikki toimivat yhteisten tavoitteiden mukaisesti ¹.
6. **Jatkuva parantaminen:** Hyödynnä jatkuvan parantamisen menetelmiä, kuten P-D-C-A (Plan-Do-Check-Act) -sykliä, joka auttaa pitämään riskienhallintaprosessin ajan tasalla ja tehokkaana ¹.

Näiden ominaisuuksien avulla voit luoda tehokkaan ja kattavan riskienhallinnan seurantarjestelmän. Onko sinulla jotain erityistä riskiä tai tilannetta mielessä, johon kaipaisit tarkempia neuvoja?

Mitkä ovat yleisimmät haasteet seurannassa?



Riskienhallinnan seurannassa voi kohdata useita haasteita. Tässä muutamia yleisimpiä:

1. **Tietojen kerääminen ja analysointi:** Riskienhallinnan seuranta vaatii jatkuvaa tietojen keräämistä ja analysointia. Tämä voi olla haastavaa, jos tietoja ei ole saatavilla tai ne ovat hajallaan eri järjestelmissä ¹.
2. **Resurssien puute:** Tehokas riskienhallinta vaatii riittävästi resursseja, kuten aikaa, rahaa ja osaamista. Resurssien puute voi johtaa siihen, että riskienhallintatoimenpiteitä ei toteuteta tai seurata riittävän hyvin ².
3. **Muuttuvat olosuhteet:** Organisaation toimintaympäristö voi muuttua nopeasti, mikä voi vaikeuttaa riskienhallinnan seuranta. Uudet riskit voivat nousta esiin, ja aiemmin tunnistetut riskit voivat muuttua ³.
4. **Viestinnän puutteet:** Tehokas riskienhallinta edellyttää hyvää viestintää organisaation sisällä. Jos viestintä ei toimi, riskienhallintatiedot eivät välttämättä saavuta kaikkia tarvittavia tahoja, mikä voi heikentää riskienhallinnan tehokkuutta ¹.
5. **Seurantajärjestelmien puutteet:** Ilman asianmukaisia seurantajärjestelmiä riskienhallinnan seuranta voi olla tehotonta. Hyvät seurantajärjestelmät auttavat keräämään ja analysoimaan tietoja sekä raportoimaan riskienhallinnan tilasta ².

Näiden haasteiden tunnistaminen ja niihin varautuminen voi auttaa parantamaan riskienhallinnan seuranta. Onko sinulla jokin erityinen haaste, johon kaipaisit tarkempia neuvoja?

Miten kehittää seurantajärjestelmää?



Seurantajärjestelmän kehittäminen on tärkeä osa tehokasta riskienhallintaa. Tässä muutamia keskeisiä vaiheita ja käytäntöjä, joita voit hyödyntää:

1. **Nykytilan arviointi:** Aloita arvioimalla nykyinen seurantajärjestelmäsi. Tunnista sen vahvuudet ja heikkoudet sekä alueet, jotka vaativat parannusta ¹.
2. **Selkeät tavoitteet ja mittarit:** Määrittele selkeät tavoitteet ja mittarit, joiden avulla voit seurata riskienhallinnan edistymistä. Tämä auttaa arvioimaan, kuinka hyvin riskienhallintatoimenpiteet toimivat ².
3. **Automatisointi:** Hyödynnä automatisoituja järjestelmiä ja työkaluja, jotka helpottavat riskienhallinnan seuranta ja raportointia. Tämä voi sisältää esimerkiksi riskienhallintaohjelmistoja, jotka tarjoavat reaaliaikaista dataa ja analytiikkaa ².
4. **Säännöllinen raportointi:** Laadi säännölliset raportit, joissa käsitellään riskienhallinnan tilaa. Raportit voivat sisältää tietoa uusista riskeistä, toteutuneista riskeistä ja riskienhallintatoimenpiteiden vaikutuksista ³.
5. **Koulutus ja viestintä:** Varmista, että kaikki organisaation jäsenet ovat tietoisia riskienhallintakäytännöistä ja -prosesseista. Säännöllinen koulutus ja viestintä auttavat ylläpitämään riskitietoisuutta ja varmistamaan, että kaikki toimivat yhteisten tavoitteiden mukaisesti ².
6. **Jatkuva parantaminen:** Hyödynnä jatkuvan parantamisen menetelmiä, kuten P-D-C-A (Plan-Do-Check-Act) -sykliä, joka auttaa pitämään riskienhallintaprosessin ajan tasalla ja tehokkaana ¹.

Näiden vaiheiden avulla voit kehittää seurantajärjestelmääsi ja varmistaa, että se tukee tehokasta riskienhallintaa. Onko sinulla jokin erityinen haaste tai tilanne, johon kaipaisit tarkempia neuvoja?

Liite 3. ChatGPT:n tuottamat vastaukset 5.5.2025

ChatGPT:n käyttämä tekoälymalli on GPT-4o.

Miten riskienhallinnan seuranta kannattaisi toteuttaa?

ChatGPT said:

Riskienhallinnan seurannan toteuttaminen on keskeinen osa organisaation kokonaisturvallisuutta ja projektien onnistumista.

Alla on kattava katsaus siihen, miten riskienhallinnan seuranta kannattaa toteuttaa käytännössä:

1. Määrittele seurannan tavoitteet

Ennen seurantaprosessin aloittamista tulee määrittää:

- Miksi riskejä seurataan (esim. projektien jatkuvuuden turvaamiseksi, turvallisuussyistä, budjetin hallitsemiseksi).
- Mitä seurannalla halutaan saavuttaa (esim. riskien varhainen tunnistaminen, vaikutusten minimoiminen).

2. Luo selkeä seuranta- ja raportointiprosessi

Toimintatavat:

- **Riskiloki tai riskirekisteri**, jota päivitetään jatkuvasti (esim. Excel, Confluence, Jira, Power BI tai erilliset GRC-työkalut kuten RiskCloud, Resolver).
- Määritä vastuuhenkilöt kullekin riskille.
- Käytä **riskin tilan** (aktiivinen, toteutunut, suljettu) seurantaan.

Aikataulu:

- Määritä tarkastus- ja päivityssykli (esim. kuukausittain, kvartaalittain).
- Projektikohtaisesti voi tehdä viikoittaisia katselmuksia.

3. Hyödynnä mittareita ja avainindikaattoreita

Esimerkkejä seurattavista asioista:

- **Riskin todennäköisyys ja vaikutus**: Onko tapahtunut muutoksia?
- **Riskien lukumäärä** tietyllä vakavuusasteella.
- **Kontrollitoimenpiteiden tehokkuus**.
- **Riskien toteutuminen** ("läheltä piti" -tilanteet tai tositapahtumat).
- **Budjetti- ja aikataulupoikkeamat**, jotka viittaavat riskien toteutumiseen.

4. Osallista sidosryhmät

- Pidä **riskityöpajoja** ja **riskikatselmuksia** projektien tai liiketoimintayksiköiden yhteydessä.
- Hyödynnä **asiantuntija-arvioita** ja **henkilöstön havaintoja** (esim. palautekanavat).
- Luo matalan kynnyksen ilmoituskanava uusien riskien tunnistamiseksi.

5. Päivitä riskikarttaa ja prioriteetteja

- Visualisoi riskit riskikartalla (matriisilla, jossa todennäköisyys vs. vaikutus).
- Päivitä karttaa aina merkittävien muutosten jälkeen (esim. uuden projektivaiheen alkaessa).
- Priorisoi toimenpiteet kartan perusteella.

6. Hyödynnä digitaalisia työkaluja

Työkalut voivat sisältää:

- **Excel tai Google Sheets** (pienille tiimeille).
- **Trello/Jira** (ketterään projektityöhön).
- **GRC-alustat** kuten:
 - Resolver
 - RiskCloud
 - LogicManager
 - Archer

7. Toteuta jatkuva parantaminen

- Arvioi säännöllisesti seurantaprosessin tehokkuus.
- Tee kehitystoimenpiteitä palautteen ja analytiikan perusteella.
- Kouluta henkilöstöä riskitietoisuuden lisäämiseksi.

Haluatko esimerkkejä riskirekisterin rakenteesta tai valmiita pohjia seurannan toteuttamiseksi?

Millainen olisi hyvä seurantajärjestelmä?

ChatGPT said:

Hyvä riskienhallinnan seurantajärjestelmä yhdistää **läpinäkyvyyden, systemaattisuuden ja helpon käytettävyyden**.

Alla on kuvattu järjestelmän keskeiset piirteet, tekniset ratkaisut ja vinkit käyttöönottoon:

Hyvän seurantajärjestelmän keskeiset ominaisuudet

1. Keskitetty riskirekisteri

- Jokaiselle riskille kirjataan:
 - Kuvaus
 - Todennäköisyys (esim. 1–5)
 - Vaikutus (1–5)
 - Riskin vakavuus (todennäköisyys × vaikutus)
 - Kontrollitoimenpiteet
 - Vastuuhenkilö
 - Tilannepäivitykset ja historiatieto

2. Automaattiset muistutukset ja päivityssykli

- Mahdollisuus asettaa muistutuksia, esim. kuukausikatselmuksista tai kontrollien arvioinnista.

3. Raportointi ja visualisointi

- Riskikartta (heatmap)
- Aikajanalogi (riskien toteutumishistoria)
- Hallituksen/johtoryhmän raporttinäkymät
- KPI-/KRI-seuranta

4. Käyttöoikeuksien hallinta

- Mahdollisuus jakaa eri näkyvyys- ja muokkaus oikeudet eri rooleille.

5. Helppokäyttöisyys ja integrointi

- Käyttöliittymä, joka ei vaadi koulutusta.
- Integraatiot muihin työkaluihin (esim. projektinhallinta, Jira, Slack, Google Workspace, M365).

Esimerkkejä seurantajärjestelmän toteutustavoista

◆ 1. Kevyt ratkaisu: Google Sheets / Excel + Power BI

Plussat: nopea, halpa, muokattava

Miinukset: ei skaalaudu hyvin suuriin organisaatioihin, manuaalinen ylläpito

◆ 2. Projektipohjainen ratkaisu: Jira + Confluence

Plussat: hyvä tiimeille, integraatiot projektinhallintaan

Miinukset: vaatii konfigurointia ja käyttäjäopastusta

◆ 3. Erillinen GRC-työkalu

Esimerkkejä:

- RiskCloud
- LogicManager
- Archer
- OneTrust

Plussat: skaalautuu, prosessit sisäänrakennettu

Miinukset: kallis, käyttöönotto vie aikaa

Rakenteellinen esimerkki: Google Sheets -pohja

Riski	Todennäköisyys (1–5)	Vaikutus (1–5)	Vakavuus	Kontrolli	Vastuuhenkilö	Status	Päivityspäivä
Palvelun kaatuminen julkaisussa	4	5	20	Käyttöönottesti	Tiina T.	Avoin	5.5.2025

Lisäksi Power BI -dashboardilla voi visualisoida riskimatriisin automaattisesti.

Käyttönoton vinkit

- Aloita pienesti:** yksi tiimi tai yksikkö, kevyellä työkalulla.
- Dokumentoi toimintamalli:** milloin ja miten riskejä päivitetään.
- Kouluta käyttäjät** ja kerää palautetta.
- Laajenna asteittain** ja harkitse skaalautuvaa ratkaisua myöhemmin.

Mitkä ovat yleisimmät haasteet seurannassa?

ChatGPT said:

Riskienhallinnan seurannassa esiintyy usein monia käytännön haasteita, jotka voivat heikentää koko riskienhallintaprosessin vaikuttavuutta.

Alla on koottu yleisimmät haasteet ja niiden taustalla olevia syitä:

🔧 Yleisimmät haasteet riskienhallinnan seurannassa

1. Päivitysten unohtuminen tai viivästyminen

- **Syy:** Ei ole selkeää vastuuhenkilöä tai päivitysaikataulua.
- **Seuraus:** Riskitiedot vanhenevat nopeasti → riskirekisteri menettää luotettavuutensa.

2. Seurannan muodollisuus ilman todellista vaikuttavuutta

- Riskien seuranta tehdään vain "ruksiksi taulukkoon", ei osana päätöksentekoa.
- Puuttuu yhteys projektien, tavoitteiden tai liiketoimintariskien välillä.

3. Heikko sitoutuminen

- Johdon tai tiimien kiinnostus riskiseurantaan voi olla vähäistä.
- Riskienhallinta nähdään usein ylimääräisenä vaivana tai hallinnollisena pakkona.

4. Ei reagoitua riskien muutoksiin

- Vaikka uusia riskejä tunnistetaan tai vanhat muuttuvat, toimenpiteitä ei päivitetä.
- Esimerkiksi projektissa jokin riski realisoituu, mutta kontrollitoimenpiteitä ei säädetä vastaavasti.

5. Tieto on hajautunut eri järjestelmiin

- Riskitietoa voi olla:
 - Excelissä
 - Slack-keskusteluissa
 - Projektityökaluissa (Jira, Asana)
 - Confluencessa
 → Seuranta vaikeutuu, kun tiedot eivät ole keskitetysti saatavilla.

6. Puuttuvat mittarit ja indikaattorit

- Ilman selkeitä mittareita (esim. KRI:t, seuraindeksit) on vaikea arvioida riskien kehittymistä tai hallintatoimien tehoa.

7. Liiallinen monimutkaisuus

- Liian raskas seurantarakenne voi johtaa siihen, että käyttäjät eivät jaksakaan tai osaa käyttää järjestelmää.
- Etenkin pienissä tiimeissä tämä voi johtaa järjestelmän sivuuttamiseen.

8. Uusien riskien tunnistamatta jättäminen

- Seurantafokus jää usein olemassa oleviin riskeihin → uusia riskejä ei havaita ajoissa.
 - Seuranta ei mahdollista jatkuvaa havaintoa muuttuvasta toimintaympäristöstä.
-

🔧 Miten haasteita voi ehkäistä?

- 📅 **Automatisoidut muistutukset ja aikataulut**
 - 👤 **Vastuuhenkilöiden nimeäminen**
 - 📊 **Yksinkertainen, visuaalinen järjestelmä**
 - 📧 **Säännölliset katselmuksot ja jatkuva parantaminen**
 - 🔗 **Linkitys tavoitteisiin, projekteihin ja päätöksentekoon**
-

Miten kehittää seurantajärjestelmää?

ChatGPT said:

Seurantajärjestelmän kehittäminen on keskeinen osa kypsää riskienhallintaa. Järjestelmän ei tarvitse olla monimutkainen — tärkeintä on, että se tukee jatkuvaa oppimista, päätöksentekoa ja reagointia muuttuvaan toimintaympäristöön. Alla on vaiheittainen opas järjestelmän kehittämiseen:

1. Arvioi nykytila ja määrittele tavoitteet

Kysymyksiä nykytilasta:

- Käytetäänkö tällä hetkellä riskirekisteriä? Missä muodossa?
- Onko vastuut ja päivityssykli määritelty?
- Miten riskejä hyödynnetään päätöksenteossa?
- Onko järjestelmä käyttäjäystävällinen?

Tavoitteet:

- Esim. "Parantaa riskien läpinäkyvyyttä ja vähentää päivityksiin kuluva aikaa 50 %."

2. Rakenna selkeä rakenne ja prosessi

Ydinosa:

- **Riskirekisteri:** kuvaukset, luokitus, vastuhenkilöt, kontrollit, päivityspäivämäärä.
- **Riskikartta / -matriisi:** visualisointi vakavuuden mukaan.
- **Päivitysprosessi:** kuinka usein ja kuka päivittää mitään.

Prosessivaiheet:

1. Tunnistaminen
2. Arviointi
3. Toimenpiteet
4. Seuranta ja arviointi
5. Raportointi

3. Valitse ja kehitä työkalut käytettävyyden ehdoilla

Valitse teknologia organisaation kypsyden ja koon mukaan:

Ratkaisu	Sopii kun...	Plussat	Esimerkki
Excel / Sheets	Aloituvaiheessa	Nopea, tuttu	Google Sheets + pivot-raportit
Notion / Trello	Tiimitasolla	Visuaalinen, kevyt	Kanban-jakelu + aikaleimat
Jira + Confluence	Projektit	Hyvät integraatiot	Jiran riskityyppi + sivukoosteet
Power BI / Looker	Organisaatiotaso	Automaatio ja raportointi	Riskidata + KRI:t yhdistetty

 Integraatiot Slackiin, sähköpostiin tai projektityökaluihin voivat vähentää manuaalista työtä merkittävästi.

4. Ota käyttöön jatkuva kehityssykli (PDCA)

Plan – Suunnittele:

- Määrittele kehitystavoitteet (esim. parempi raportointi, riskikatselmusten ajastus)

Do – Toteuta:

- Päivitä työkaluja ja toimintamalleja
- Testaa pienellä tiimillä tai pilottiprojektilla

Check – Arvioi:

- Seuraa käyttöastetta, päivitystiheyttä, palautetta
- Tarkastele riskien realisoitumista suhteessa arvioihin

Act – Paranna:

- Mukauta prosessia, lisää ohjeistusta, tehosta automaatiota
-

5. Kouluta ja osallista käyttäjiä

- **Ohjeistus:** Tee selkeä "Miten päivitän riskin?" -dokumentti
 - **Säännölliset työpajat:** Uusien riskien tunnistamiseen ja vanhojen arviointiin
 - **Palaute:** Pyydä käyttäjiltä palautetta käytettävyydestä ja kehitysehdotuksia
-

6. Lisää älykkyyttä ja ennakoivuutta

Kun perusjärjestelmä toimii:

- Lisää **KRI:t** (Key Risk Indicators) ja visuaaliset mittarit
 - Hyödynnä **historian perusteella oppivia** ennusteita (esim. Power BI:n trendeillä)
 - Tuo mukaan "**läheltä piti**" -tapaukset ja hiljaiset signaalit
-

Esimerkki kehityspolusta:

1. 📄 Sheets + säännöllinen muistutus sähköpostilla
 2. 📊 Riskikartta + automaattinen status-muutos >90 pv
 3. 📈 Visualisointi + KRI-dashboard Power BI:ssä
 4. 🗨️ Integraatio projektityökaluun + johdon kuukausiraportti
-