LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Turvallisuusjohtamisjärjestelmän luominen ammattikorkeakouluun

Aholainen, Miika

2017 Laurea

Laurea-ammattikorkeakoulu

Turvallisuusjohtamisjärjestelmän luominen ammattikorkeakouluun

Miika Aholainen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Huhtikuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma
Tradenomi (AMK)

Miika Aholainen

Turvallisuusjohtamisjärjestelmän luominen ammattikorkeakouluun

Vuosi 2017 Sivumäärä 84

Tämän toiminnallisen opinnäytetyön tavoitteena oli selvittää, miten suomalaiseen ammattikorkeakouluun voidaan luoda turvallisuusjohtamisjärjestelmä. Työn toimeksiantajana oli Ammattikorkeakoulu Arcada, jonka kampus sijaitsee Helsingin Arabianrannassa. Tavoitteena oli myös luoda malli, jolla mikä tahansa suomalainen ammattikorkeakoulu pystyy aloittaa turvallisuusjohtamisjärjestelmän luomisen. Tätä mallia hyödynnettiin myös Arcadaan, jotta se voisi saavuttaa turvallisuusjohtamisjärjestelmän edellyttämän tason seuraavan 5-10 vuoden aikana.

Kehittämistehtävä on jatkumona turvallisuusjohtamisen kehittämistyölle, joka on alkanut Arcadassa vuonna 2016. Osana kehittämistehtävää Arcadan johto saa toimenpide-ehdotukset, jotka tulisi liittää osaksi seuraavaa turvallisuuden toimintaohjelmaa. Arcadan turvallisuuden kehittämistyö jatkuu opinnäytetyön jälkeen.

Opinnäytetyön viitekehys on riskienhallinnan ja turvallisuusjohtamisen useista eri lähteistä johdettua kirjallisuus- ja tutkimustietoa. Teoriassa korostuvat ne prosessit ja toiminnot, jotka sisältyvät turvallisuusjohtamisjärjestelmään. Tutkimuksia ja selvityksiä hyödyntämällä on lähestytty aihetta oppilaitoksien ja erityisesti korkeakoulujen näkökulmasta.

Tiedonkeruumenetelminä käytettiin kvalitatiivisia menetelmiä, haastattelua ja benchmarkingia. Haastatteluilla on pyritty kartoittamaan, mitä on ammattikorkeakoulujen toiminta ja miten turvallisuusjohtaminen on osa koulun normaalia toimintaa. Benchmarkingin avulla on pyritty oppimaan useita vuosia systemaattisesti kehittäneen korkeakoulun toiminnasta. Arcada pyrkii hyödyntämään benchmarkingin tuloksia turvallisuusjohtamisjärjestelmän luomisessa, soveltamalla Laurea-ammattikorkeakoulun turvallisuusjohtamisen periaatteita ja puitteita.

Opinnäytetyön tuloksena voidaan todeta, että ammattikorkeakoulujen turvallisuusjohtaminen ei poikkea muiden organisaatioiden turvallisuusjohtamisesta periaatteiltaan. Systemaattisen turvallisuusjohtamisen tulisi perustua riskienhallintaan. Työn keskeinen tuotos on turvallisuusjohtamisjärjestelmän luomisen malli. Kun turvallisuustyön päämääränä on turvallisuusjohtamisjärjestelmä, malli esittää, miten organisaatio pääsee alkuun systemaattisessa kehittämistyössään.

Saadut tulokset ovat riskienhallinnan ja turvallisuusjohtamisen teorian kanssa yhdenmukaisia. Ammattikorkeakoulujen turvallisuusjohtaminen poikkeaa toisistaan toteutukseltaan, mutta haastateltujen ammattikorkeakoulujen turvallisuustoiminnan periaatteet johdetaan riskienhallinnasta ja erityisesti riskien arvioinnin tuloksista. Tuloksena saatiin myös hyviä toimintatapoja, joilla turvallisuutta johdetaan ja joilla turvallisuusjohtaminen on integroitu osaksi organisaation kaikkea toimintaa. Johtopäätöksenä voidaan todeta, että turvallisuusjohtamiseen löytyy hyviä käytänteitä ja malleja, mutta tärkeintä olisi saada resurssit toimintaan ja korkeakouluyhteisön kaikki jäsenet mukaan turvallisuuskulttuurin kehittämiseen. Turvallisuusjohtamisjärjestelmää tulisi alkaa luoda systemaattisesti riskienhallinnan avulla.

Asiasanat: riskienhallinta, turvallisuusjohtaminen, turvallisuusjohtamisjärjestelmä

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

Miika Aholainen

Creating a Security and Safety Management System in a University of Applied Sciences

Year 2017 Pages 84

The purpose of the thesis was to research how a University of Applied Sciences (UAS) can create a security and safety management (SSM) system. The commissioner of the thesis was Arcada UAS, which has a campus located in Arabianranta, Helsinki. Another objective was to create a model which any Finnish UAS may apply when beginning the creation of an SSM system.

The project was a continuation for the development work that began in Arcada in 2016. The objective was to create a plan, which can be applied to developing and implementing Arcada's SSM system in the next 5-10 years. As a part of the project Arcada's management received a suggestive action plan that should be integrated into the security and safety program in the future.

The framework of the thesis is based on literature and research on security, safety and risk management. Those processes and functions that are included in an SSM system were highlighted while creating the framework of the thesis. The subject was approached by exploiting research papers and studies from the educational institutions', and especially from UASs', point of view.

Interviewing and benchmarking were the exploited qualitative research methods. The objective of the interviews was to examine what the business function of a Finnish UAS is and how the SSM is integrated as a part of the general management. The focus of the benchmarking was to research how Laurea UAS has developed its SSM and what the procedures and best practices are and how they can be applied in Arcada.

The results indicate that the UASs' SSM principles do not differ from other fields. A holistic SSM should be based on risk management. A fundamental product of the thesis is a model that can be applied in creating an SSM system. The model highlights how an organisation may begin creating an SSM system by planning and implementing its SSM systematically to achieve a holistic SSM system in 5-10 years.

The results comply with the theories on risk management and SSM. UASs' SSM differs from each other by implementation but the results of the interviews indicate that the security and safety principles are based on risk management and especially on the results of the risk assessment. In addition, the results presented best practices, and how SSM is integrated into general management of a UAS. It can be stated that SSM may be applied by several different best practices and models but the most important aspect is receiving resources to develop the SSM and to get the whole organisation, stakeholders included, to develop a safety culture. It may be concluded that the creation of an SSM system must be begun by systematically managing risks.

Keywords: Risk Management, Security and Safety Management, Security and Safety Management System

Sisällys

1 Johdanto 7
1.1 Tavoite, rajaus ja tutkimuskysymys 7
1.2 Keskeiset käsitteet 8
1.3 Tausta 9
2 Riskienhallinta 9
2.1 Riskienhallinnan periaatteet ja puitteet 9
2.2 Riskienhallintaprosessi 11
2.3 Riskien arviointimenetelmät 16
3 Turvallisuusjohtaminen 20
3.1 Turvallisuusjohtamisen periaatteet 21
3.2 Jatkuvuudenhallinta 23
3.3 Turvallisuusvaatimusten täyttäminen 24
3.4 Henkilöstöturvallisuus 25
3.5 Työturvallisuus 27
3.6 Tietoturvallisuus 28
3.7 Kiinteistö- ja toimitilaturvallisuus 31
3.8 Pelastusturvallisuus 32
3.9 Tuotannon, toiminnan ja ympäristön turvallisuus 33
3.10 Väärinkäytösten, poikkeamien ja kriisinhallinta sekä varautuminen 34
4 Turvallisuusjohtamisjärjestelmä 34
5 Oppilaitosten turvallisuus 39
6 Turvallisuusjohtaminen Arcada-ammattikorkeakoulussa 41
7 Opinnäytetyön prosessi 46
8 Opinnäytetyössä käytetyt menetelmät 47
8.1 Toiminnallinen opinnäytetyö 48
8.2 Laadullisen tutkimuksen periaatteet 49
8.3 Tiedonkeruumenetelmät 49
8.4 Aineistolähtöinen sisällönanalyysi 51
9 Tulokset 52
9.1 Riskienhallinta ja turvallisuusjohtaminen 52
9.2 Turvallisuusjohtamisjärjestelmän luominen 54
10 Johtopäätökset 58
10.1 Yhteenveto kehittämishankkeesta 65
10.2 Toimenpide-ehdotukset 66
10.3 Jatkotutkimukset 66
10.4 Oman oppimisen arviointi 67
Lähteet 68

Kuviot 73
Taulukot 74
Liitteet 75

1 Johdanto

Turvallisuus on moniulotteinen osa organisaatioiden riskien- ja laadunhallintaa. Turvallisuuden ulottuvuuksia ovat muun muassa taloudellinen kannattavuus, turvallisuuden tunne, riskienhallinta, hyvä hallintotapa ja laadunhallinta. Organisaation strategia ja riskienhallinta asettavat periaatteet ja puitteet, joiden mukaisesti turvallisuutta johdetaan. Turvallisuuspolitiikka on organisaation turvallisuusjohtamisen perusta ja se johdetaan organisaation strategiasta, arvoista, visiosta ja tavoitteista. Turvallisuuden voi nähdä organisaation liiketoiminnan mahdollistavana ja toiminnan jatkuvuuden varmistavana toimintakokonaisuutena, joka on kuitenkin läsnä arkipäiväisenä toimintona osana normaalia organisaation johtamista. Turvallisuuden tärkeimmät mahdollistajat ovat organisaation työntekijät, jotka omilla toimillaan luovat onnistuneen turvallisuuskulttuurin ja tilan, jossa turvallisuus on ennaltaehkäisevää ja havaittuihin poikkeamiin reagoidaan asianmukaisesti. Kun turvallisuutta vielä seurataan ja mitataan, päästään jatkuvan parantamisen tilaan, jossa uusista tuloksista johdetaan aina uudet, ajantasaiset ja perustellut toimenpiteet. Uusien toimenpiteiden aktiivinen seuranta ja vaikutuksien arviointi ovat osa ennaltaehkäisevää turvallisuustyötä.

Tämä on toiminnallinen opinnäytetyö, joka käsittelee turvallisuusjohtamista ammattikorkeakouluissa, joissa turvallisuustyö on hyvin arkipäiväistä. Tavoitteena on varmistaa turvallinen opiskelu- ja työympäristö kaikille opiskelijoille ja työntekijöille sekä muille käyttäjille. Turvallisuusjohtamisen ja riskienhallinnan periaatteet luovat perustan jatkuvan kehittämisen turvallisuustyölle korkeakouluissa, joiden liiketoimintaympäristö koostuu pääosin opetus- ja tutkimustyöstä. Turvallisuudesta vastaa korkeakoulussa ylin johto, jonka vahva tuki ja myöntämät resurssit luovat edellytykset turvallisuuden kehittämistyölle ammattikorkeakoulussa.

1.1 Tavoite, rajaus ja tutkimuskysymys

Opinnäytetyön tavoitteena oli selvittää, miten suomalaiseen ammattikorkeakouluun voidaan luoda turvallisuusjohtamisjärjestelmä. Toisena tavoitteena oli tuottaa vaihe vaiheelta kuvattu turvallisuusjohtamisen ja riskienhallinnan toimintamalli, prosessi, jota voivat soveltaa kaikki Suomen ammattikorkeakoulut. Malli tarjoaa ammattikorkeakouluille periaatteet ja puitteet aloittaa luoda kokonaisvaltaista turvallisuusjohtamisjärjestelmää, joka kattaa turvallisuusjohtamisjärjestelmään kohdistuvat lainsäädännön vaatimukset ja toiminnalliset elementit. Mallia soveltamalla luotiin työn tilaajalle, Arcada-ammattikorkeakoululle, suunnitelma, jolla se pystyy luomaan turvallisuusjohtamisjärjestelmän seuraavan 5-10 vuoden aikana.

Opinnäytetyö pyrkii kuvaamaan turvallisuusjohtamisjärjestelmän kehittämisen alkuvaiheet organisaatiolle, jolla ei ole turvallisuuteen mitään järjestelmää. Työ rajoitetaan huomioimaan,

mitä elementtejä sisältyy turvallisuusjohtamisjärjestelmään ja miten pääsee alkuun järjestelmän kehittämisessä. Kokonaisvaltaista, valmista, mallia työ ei yritä kuvailla, vaan tarkoituksena on tarjota periaatteet, puitteet ja suuntaa-antava malli, joilla organisaatio pystyy itse luomaan järjestelmänsä valmiiksi kokonaisuudeksi. Kattavan järjestelmän kuvaaminen on hyvin subjektiivista joka tapauksessa, ja käytännössä jokainen organisaatio luo oman mallinsa omien tarpeidensa ja strategiansa mukaisesti. Tämän takia ei ole järkevää kuvata kattavaa, yksityiskohtaista mallia, joka on räätälöity opinnäytetyön tilaajaorganisaation strategian ja tavoitteiden mukaisesti.

Opinnäytetyön tutkimuskysymykseksi määräytyi:
Miten turvallisuusjohtamisjärjestelmä luodaan ammattikorkeakouluun?

1.2 Keskeiset käsitteet

Riskienhallinta on koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Riskienhallinta on myös prosessi ja johdon toimenpiteitä, joilla pyritään parhaaseen mahdolliseen lopputulokseen ja pienentämään lopputuloksen epävakaisuutta ja vaihtelevuutta. Riskienhallintaprosessi alkaa toimintaympäristön määrittelyllä, keskeinen vaihe on riskin arviointi -prosessi ja riskin käsittelyn jälkeen prosessi alkaa alusta. Prosessin jokaiseen vaiheeseen kohdistuu myös tiedonvaihtoa, viestintää, seurantaa ja katselmointia. (Hopkin 2014, 407; SFS-ISO 31000.)

Turvallisuusjohtaminen on osa organisaation johtamista, jossa turvallisuus integroidaan organisaation strategiaan ja päätöksentekoon. Se on ihmisten, ympäristön ja omaisuuden suojelemista sekä tavoitteellista kehittämistä. Turvallisuusjohtaminen on myös kokonaisvaltaista toimintaa organisaation turvallisuuden hallitsemiseksi ja sillä tarkoitetaan kaikkia johdon toimenpiteitä, joilla pyritään organisaation turvallisuustason kehittämiseen. (Kerko 2001, 31; Booth&Lee 1995, 393-400; Reiman & Oedewald 2008, 43; Paasonen 2012, 16.)

Turvallisuusjohtamisjärjestelmä on kaikista organisaatioturvallisuuden osa-alueista ja toiminnoista yhteen koottu järjestelmä, jonka lähestymistapa organisaation turvallisuuden hallintaan on systemaattista ja dokumentoitua. Turvallisuusjohtamisjärjestelmä sisältää johtamis-, järjestelmä- ja laatupiirteet ja sen pohjana toimii turvallisuusjohtamisen käsite. Turvallisuusjohtamisjärjestelmä on eri elementeistä muodostuva kokonaisuus. (Leppänen 2006, 57; Kerko 2001, 22; Levä 2003, 37.)

1.3 Tausta

Toiminnallinen opinnäytetyö perustuu toukokuussa 2016 tekijän aloittamaan turvallisuuden kehittämistyöhön Arcada-ammattikorkeakoulussa. Tavoitteeksi kehittämistyölle asetettiin kokonaisvaltainen turvallisuuden kehittäminen Arcadassa ja siihen liittyvät muut tehtävät. Aiemmin tammikuussa Arcadaan tehtiin turvallisuuden auditointi Tutor Max –auditointimallilla, joka selvitti kokonaisvaltaisesti Arcadan turvallisuuden nykytilaa verraten lainsäätäjän tarkoittamaan vähimmäistasoon (Martikainen & Ranta 2015). Auditoinnin tulokset selvittivät työn priorisoinnin ja antoivat myös korjaavia toimenpide-ehdotuksia, joilla kehittämistyössä päästään alkuun.

Työ Arcadassa kehittyi syksyllä 2016 siihen vaiheeseen, että kokonaisvaltaista turvallisuuden johtamisjärjestelmän tarvetta ja hyötyä alettiin suunnitella suhteessa turvallisuuden kehittämistyöhön Arcadassa. Lopputuloksena päätettiin luoda suunnitelma, jolla Arcada saavuttaa turvallisuusjohtamisjärjestelmän tason seuraavan 5-10 vuoden aikana. Tavoitteeksi määriteltiin luoda malli, jota muutkin korkeakoulut voisivat hyödyntää. Perimmäinen tarkoitus on kuitenkin selvittää, mistä tulisi aloittaa turvallisuusjohtamisjärjestelmän luominen. Opinnäytetyö on toiminnallinen, koska se tehdään tiiviissä yhteistyössä Arcadan kanssa organisaation sisältä kuvattuna, osana muuta työskentelyä.

2 Riskienhallinta

Turvallisuusjohtaminen vaatii systemaattisen lähestymistavan, jolla turvallisuusjohtamista kehitetään, mikäli tavoitteena on turvallisuusjohtamisjärjestelmä. Riskienhallinta antaa välineen ammattikorkeakoulun turvallisuuden systemaattiselle kehittämiselle ja turvallisuusjohtamisen pitäisikin aina perustua riskienhallintaan. Organisaation strategian tulisi ohjata riskienhallintaa, toimintaa, joka koostuu periaatteista, puitteista ja toteuttamisesta, jota voidaan kuvata riskien arviointiprosessina. Opinnäytetyössä keskeinen osa on myös riskien arviointimenetelmillä, joita hyödyntämällä saadaan toimenpiteet, joilla turvallisuusjohtamista kehitetään. Työssä nousee esille ammattikorkeakouluille soveltuvat tärkeimmät riskien arviointimenetelmät, joiden käyttäminen on oikeassa ohjauksessa helppoa. Riskienhallinnassa korostuu siihen myönnetyt resurssit, johdon tahto ja sitoutuminen, riskienhallintapolitiikka ja riskienhallintasuunnitelma, jolla politiikkaa toteutetaan.

2.1 Riskienhallinnan periaatteet ja puitteet

Standardin SFS-EN 31010 mukaan kaiken tyyppiset ja -kokoiset organisaatiot kohtaavat riskejä, jotka voivat vaikuttaa siihen saavuttaako organisaatio tavoitteitaan, jotka voivat koskea organisaation toimintaympäristöä, strategiaa, prosesseja- ja projekteja tai esimerkiksi talous-

ja kaupallisia asioita. Organisaation tulisi hallita riskejään, joita on kaikissa sen toiminnoissa. Riskienhallintaprosessi auttaa päätöksenteossa, jossa otetaan huomioon epävarmuus ja mahdolliset tulevat tapahtumat tai olosuhteet ja niiden vaikutukset tavoitteisiin. Riskienhallinta tulisi myös liittää osaksi organisaation kaikkiin prosesseihin ja käytäntöihin ja sen tulisi olla järjestelmällistä ja ajantasaista. Riskienhallinnan periaatteisiin kuuluu myös, että se tukee jatkuvaa parantamista, perustuu epävarmuuden ja inhimillisten sekä kulttuuristen tekijöiden huomioonottamiseen sekä avoimuuteen. (SFS-EN 31010.)

Jatkuva parantaminen on olennainen osa riskienhallintaa ja sillä tarkoitetaan kaikkia toimenpiteitä, joilla parannetaan jatkuvasti tuotteita, palveluita ja prosesseja. Jatkuva kehittäminen on synonyymi jatkuvalle parantamiselle, sillä se tulee englanninkielen termistä ”Continuous improvement”, joka on tulkittu SFS-ISO 31000 mukaan myös jatkuvaksi kehittämiseksi. Yksi yleisimmistä jatkuvan parantamisen välineistä on niin sanottu PDCA-malli, jonka vaiheet ovat suunnittele, toteuta, arvioi ja paranna. Prosessi aloitetaan tunnistamalla muutosmahdollisuus, joka suunnitellaan. Toteutusvaiheessa tulee taas tehdä muutos pienellä skaalalla, minkä jälkeen hyödynnetään dataa, jolla selvitetään edellisen vaiheen muutoksia ja päätellään, tapahtuiko muutosta. Arviointivaihe on käytännössä seurantaa ja tuloksien raportointia. Mikäli muutos oli onnistunut, se toteutetaan suuremmalla skaalalla. Mikäli muutos oli negatiivinen, palataan suunnitteluvaiheeseen ja aloitetaan parantaminen uudelleen. Näin parantamisesta tulee johdettu, jatkuva, prosessi. (ASQ 2016; ISO 22301.)

Riskienhallinta koostuu periaatteista, puitteista ja riskienhallintaprosessista, jolla riskienhallintaa toteutetaan. Riskienhallinnan onnistuminen riippuu SFS-ISO 31000 -standardin mukaan puitteista, riskienhallinnan perustalla olevista johtamisrakenteista, joilla riskienhallinta sisällytetään koko organisaation toimintaan. Puitteet varmistavat, että riskienhallintaprosessista saatua tietoa käytetään päätöksentekoon ja raportoidaan oikealla tavalla.

Riskienhallinnan puitteita voidaan kuvailla prosessina, jossa johdon tulee sitoutua riskienhallintaan ja perusteelliseen suunnitteluun, jotta voidaan varmistaa, että kaikki organisaation tasot saadaan sitoutumaan riskienhallintaan. Riskienhallinnan puitteiden suunnittelu johdetaan riskienhallinnan periaatteista ja suunnittelun jälkeen toteutetaan puitteita ja riskienhallintaprosessia. Toteuttamisen jälkeen seurataan ja katselmoidaan puitteita, jotta voidaan varmistaa ja mitata riskienhallintasuunnitelman toteutumista. Puitteiden seurannan ja katselmoinnin tulosten perusteella tulisi päättää, miten puitteita, riskienhallintapolitiikkaa ja riskienhallintasuunnitelmaa kehitetään. (SFS-ISO 31000.)

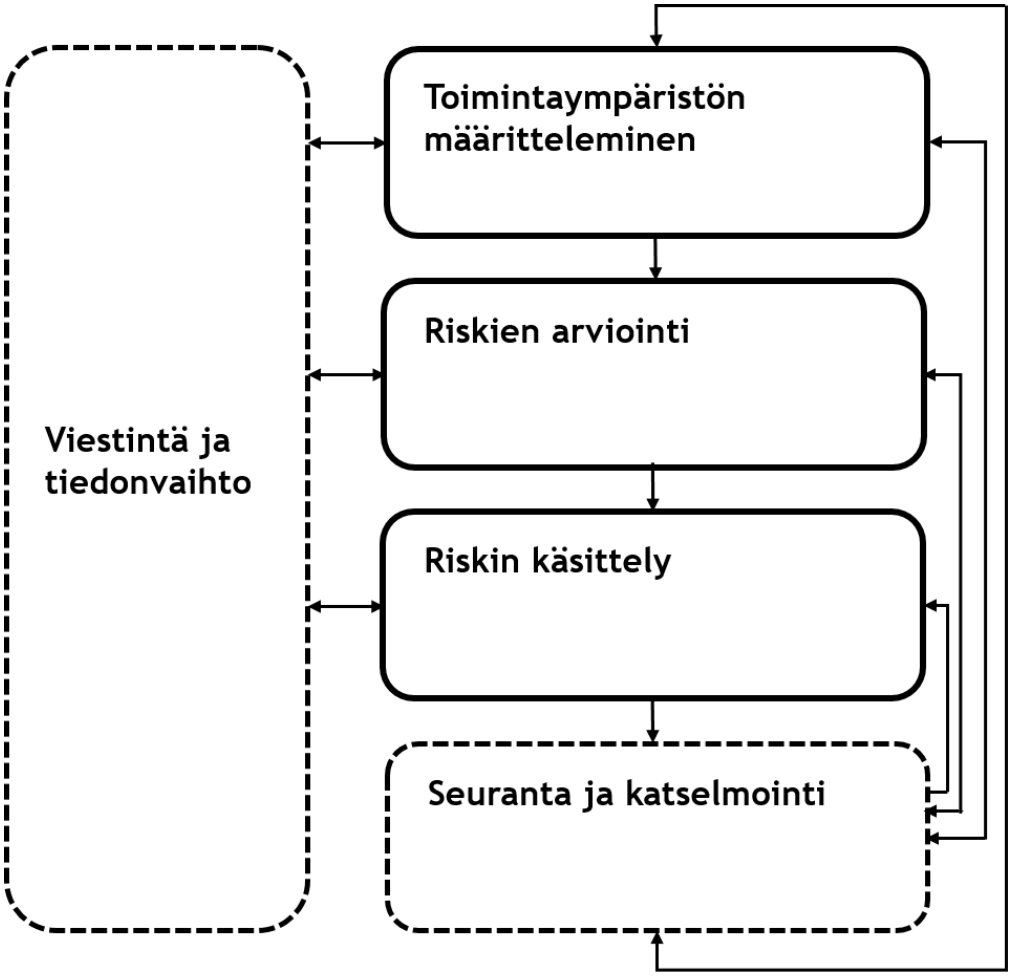
Johdon tulisi sitoutumisen varmistamiseksi määritellä ja vahvistaa riskienhallintapolitiikka, joka ohjaa ja linjaa organisaation riskienhallinnan tavoitteita, menettelytapoja ja organisointia. Politiikan tulee olla osa organisaation johtamista ja ohjausta ja sen tarkoitus on tukea

strategian toteutumista, joten sen tulee olla linjassa vision, arvojen ja toiminta-ajatuksen kanssa. Riskienhallintapolitiikka sisältää, mitä riskillä tarkoitetaan, keskeiset päämäärät ja tavoitteet, vastuut ja organisointi sekä raportointikäytännöt eri organisaation tasoilla. Politiikassa tulisi myös määritellä riskikuva tai merkittävimmät riskialueet sekä miten riskienhallinnassa onnistutaan. Riskienhallintapolitiikkaa toteutetaan riskienhallintasuunnitelmalla, jolla varmistetaan, että politiikka sisällytetään organisaation kaikkiin prosesseihin ja toimintoihin. Suunnitelma on osa riskienhallinnan puitteita ja sen tulisi sisältää resurssit, riskien hallintaan sovellettava toimintamalli ja osatekijät. (SFS-ISO 31000; Suomen riskienhallintayhdistys 2017b.)

2.2 Riskienhallintaprosessi

Vellanin (2007, 109-110) mukaan riskienhallintaprosessi sisältää uhkien, haavoittuvuuksien ja riskien arvioinnin sekä turvallisuustoimenpiteiden arvioinnin ja valitsemisen, joilla pienennetään tunnistettuja riskejä. Se sisältää myös valittujen toimenpiteiden toteutuksen ja seurannan, jotta toimenpiteiden toimivuus voidaan varmistaa. Vellani (2007, 110) selvittää, että riskienhallinta on myös vakuutus- ja laillisuustekijöitä, turvallisuuden lisäksi.

SFS-ISO 31000 -standardi määrittelee riskienhallinnan toteuttamisen olevan prosessi (kuvio 1), jossa organisaation periaatteita, menettelyjä ja käytänteitä sovelletaan järjestelmällisesti toimintaympäristön määrittelemiseen, riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan ja katselmointiin. Edellä mainittuja toimintoja sovelletaan myös viestintään ja tietojenvaihtoon sidosryhmien kanssa. SFS-ISO 31000 -riskienhallintastandardi suositteleekin, että organisaatiot kehittävät ja toteuttavat jatkuvasti puitteita, joiden tarkoitus on yhdistää riskienhallintaprosessi organisaation yleiseen hallintotapaan, strategiaan, suunnitteluun, johtamiseen, raportointiin, toimintatapoihin, arvoihin ja kulttuuriin. (SFS-ISO 31000.)



Kuvio 1: Riskienhallintaprosessi (SFS-ISO 31000)

Riskienhallintaprosessi alkaa toimintaympäristön määrittelemisestä. Seuraavaksi tehdään riskien arviointi ja lopulta riskin käsittely, jonka jälkeen tehdään vielä seurantaa ja katselmointia ennen kuin prosessi alkaa alusta. Prosessi aloitetaan alusta, jos olosuhteet muuttuvat riittävästi tai tulee seuraava sovittu ajankohta riskien arvioinnille. Koko prosessin ajan käydään tiedonvaihtoa ja viestintää sidosryhmien kanssa riskien hallinnasta. Prosessin jokaisessa vaiheessa tapahtuu myös seurantaa ja katselmointia, joilla pyritään tunnistamaan poikkeamat vaaditusta tasosta ja arvioidaan asetettujen tavoitteiden saavuttamiseen tarvittavien toimenpiteiden riittävyys ja vaikuttavuus. (SFS-ISO 31000; SFS-opas 73.)

Jokaisella toimialalla tai riskienhallinnan soveltamiskohteella on aina omat näkemyksensä, tarpeensa ja kohdeyleisönsä, minkä takia toimintaympäristön määrittely sisällytetään riskienhallintaprosessiin. SFS-ISO 31000 -standardin mukaan toimintaympäristön määritteleminen on sisäisten ja ulkoisten muuttujien määrittely, riskienhallintapolitiikan kattavuuden ja riskikriteerien määritteleminen. Toimintaympäristö kattaa sisäisen ja ulkoisen toimintaympäristön ja

se asettaa soveltamisalueen rajat ja kriteerit. Toimintaympäristön määrittelyssä tulee määrittää ja hyväksyä riskien arvioinnin tavoitteet, riskikriteerit ja riskien arviointiohjelma. (SFS-ISO 31000.)

Vellanin (2007, 110-111) mukaan riskien arviointi luo organisaatiolle perustan tehokkaille kehittämistoimenpiteille. Riskien arviointi -prosessi alkaa suojeltavien arvojen tunnistamisella ja nykyisten turvallisuustoimenpiteiden, jotka suojaavat arvoja, määrittelyllä. Kolmannessa vaiheessa uhat tunnistetaan, luokitellaan ja arvioidaan määrällisellä tai laadullisella asteikolla. Seuraavaksi tehdään haavoittuvuusanalyysi, jossa haavoittuvuudet tunnistetaan kyselyllä. Viimeiseksi tehdään kustannus-hyöty -analyysi, riskien arviointi ja toimenpide-ehdotukset sisältävä raportti. (Vellani 2007, 110-112.)

Riskien arviointi on osa riskienhallintaa, joka tarjoaa järjestelmällisen menetelmän, jolla tunnistetaan potentiaaliset vaikutukset tavoitteisiin (SFS-EN 31010). Riskien arviointi prosessi käsittää SFS-ISO 31000 -standardin mukaan riskin tunnistamisen, riskin analysoinnin ja riskin merkityksen arvioinnin. Riskien tunnistaminen on riskien havaitsemisen ja kuvaamisen prosessi. Riskianalyysi koostuu riskin luonteen ymmärtämisestä ja riskitason määrittämisestä eli todennäköisyyksien ja seurauksien yhdistelmästä. Riskin merkityksen arvioinnissa riskianalyysin tuloksia verrataan riskikriteereihin vertailemalla, jolloin saadaan tietoa, onko riski hyväksyttävä tai siedettävä. Arkikielessä puhutaan usein riskeistä ja vaaroista synonyymeinä, vaikka todellisuudessa vaara on vahingon lähde tai sen mahdollistava olosuhde. (SFS-opas 73; SFS-IEC 60300-3-9.)

Riski koostuu lähteestä, tapahtumasta, syistä ja seurauksista (SFS-opas 73). Riskiin vaaditaan aina jokin tapahtuma, tekijä, joka kykenee aiheuttamaan riskin sekä tietyt olosuhteet tai olosuhteiden muutokset. Haavoittuvuus taas altistaa riskin lähteelle, joka voi aiheuttaa tapahtuman, jolla on seurauksia. Mikäli tapahtumalla ei taas ole seurauksia, puhutaan vaaratilanteesta tai läheltä-piti -tilanteesta. Tapahtumalle altistuminen johtaa seurauksiin, jotka voivat olla positiivisia tai negatiivisia, määrällisiä tai laadullisia sekä erilaisia. Näin vaara voidaan mieltää riskin lähteeksi. (SFS-opas 73; SFS-IEC 60300-3-9.)

Esimerkkivaarana voisi pitää tulipaloa, joka on selkeästi vahingon lähde, mutta ei kerro enempää tapahtumasta, syistä eikä seurauksista. Vastaava riski voisi esimerkiksi olla kuvaus, jossa ilman valvontaa jätetty nuotio leviää kuivan sään ja tuulen seurauksena taloon, joka palaa kokonaan. Kuvauksessa tuli on riskin lähde, tulen tekeminen luo haavoittuvuuden ja nuotion jättäminen ilman valvontaa luo olosuhteiden muutoksen, tapahtuman. Kuiva ja tuulinen sää mahdollistaa taas altistumisen tulipalon leviämiselle, jonka seurauksena talo palaa.

Riskien tunnistaminen on riskien löytämisen, tuntemisen ja tallentamisen prosessi. Riskin tunnistamisen tarkoitus on selvittää, mitä tapahtuisi tai millaisia tilanteita syntyisi, jotka voisivat vaikuttaa organisaation tavoitteiden saavuttamiseen. Riskien tunnistamismenetelmät voivat sisältää ryhmätyöskentelyä, näyttöön perustuvia menetelmiä, induktiivisen päättelyn keinoja tai erilaisia tukitekniikoita, kuten aivoriihi-menetelmä. (SFS-EN 31010.)

Riskianalyysissa muodostetaan käsitys riskistä sekä luodaan lähtökohta sille, tarvitseeko riskejä käsitellä, riskien merkityksen arvioinnille. Riskianalyysissa määritetään tunnistettujen riskien todennäköisyydet ja seuraukset, jotka yhdistetään riskitason määrittämiseksi. Analyysissa tulee myös ottaa huomioon kaikki nykyiset hallintakeinot sekä niiden tehokkuus. Tavallisesti riskianalyysi sisältää arvion erilaisista seurauksista, jotka voivat syntyä olosuhteista tai tapahtumasta, ja niihin liittyvistä olosuhteista. Toisaalta on myös mahdollista, että seuraus esiintyy erilaisten tapahtumien tai olosuhteiden yhteisenä seurauksena, tai erityistä tapahtumaa ei ole tunnistettu. Tällöin riskien arvioinnin tarkoituksena on analysoida järjestelmän komponenttien merkitystä ja haavoittuvuutta tarkoituksena määrittää ne toimenpiteet, jotka koskevat suojaustasoa. (SFS-EN 31010.)

Riskianalyysimenetelmä voi kvalitatiivinen, kvantitatiivinen tai semi-kvantitatiivinen. Laadullinen analyysi määrittää seurauksen, todennäköisyyden ja riskin tason merkittävyysasteikolla ”suuri, ”keskisuuri” ja ”pieni”. Laadullisen menetelmän kaikille termeille on oltava selvitykset. Semi-kvantitatiivinen analyysimenetelmä käyttää todennäköisyyksille ja seurauksille numeerisia arviointiasteikkoja, jotka voivat olla lineaarisia tai logaritmisia tai niillä voi olla jokin muu suhde. Määrällinen analyysimenetelmä arvioi seurauksille ja todennäköisyyksille taas käytännön arvot, ja tuottaa riskitason arvot määritettyinä yksikköinä, jotka on määritelty toimintaympäristöä rajattaessa. (SFS-EN 31010.)

Seurausanalyysi on osa riskianalyysia ja se määrittää seurausten vaikutuksen luonteen ja tyypin, joka voi tapahtua, mikäli tietty tilanne tai olosuhde on esiintynyt. Tapahtumalla voi olla erilaisia ja eri suuruisia vaikutuksia, jotka voivat koskettaa sidosryhmiä, jotka on määritelty toimintaympäristöä määriteltäessä. Vaikutuksilla voi olla pieni todennäköisyys ja suuret seuraukset tai pienet seuraukset ja suuri todennäköisyys tai jotakin näiden väliltä. Organisaatiojohdon näkökulmasta tulisi painottaa riskejä, joiden seuraukset ovat erittäin mittavat. (SFS-EN 31010.)

Riskin todennäköisyyden arvioinnissa käytetään kolmea erilaista lähestymistapaa. Aikaisemmin esiintyneiden tapahtumien tunnistamiseen hyödynnetään historiatietoja, mutta tällöin tulee varmistua siitä, että esiintymistaajuus on riittävä, jotta todennäköisyys voidaan arvioida luotettavasti. Kun historiatietoja ei ole käytettävissä, tulee hyödyntää ennakoivia tekniikoita, kuten vikapuuanalyysia, jolloin saadaan todennäköisyysennusteita. Tällöin todennäköisyys

saadaan analysoimalla järjestelmä, ihmiset, organisaatio tai laitteisto ja siihen liittyvät epäonnistumiset. Kolmas lähestymistapa hyödyntää asiantuntijoiden näkemyksiä, joiden on perustuttava kaikkeen saatavilla olevaan luotettavaan tietoon, kuten historiatietoihin. Erilaiset kaavamaiset menetelmät hyödyntävät asiantuntijoiden näkemysten selville saamiseksi. (SFS-EN 31010.)

Riskin merkittävyyden arviointi perustuu riskin arvioidun tason vertaamiseen riskikriteereihin, jotka määritellään osana toimintaympäristön määrittelyä. Riskin merkityksen arviointiin käytetään riskin ymmärtämistä, joka on saatu riskianalyysin aikana tulevia toimenpiteitä koskevia päätöksiä varten. Suomen riskienhallintayhdistyksen (2017c) mukaan riskin merkittävyyden arvioinnin tarkoitus on auttaa tekemään päätöksiä siitä, mitkä riskit ovat merkityksellisiä organisaation näkökulmasta ja mikä on riskien tärkeysjärjestys hallintatoimenpiteiden käsittelemiseksi. (SFS-EN 31010.)

Riskin käsittely on SFS-oppaan 73 mukaan riskin muokkaamisprosessi, johon voi sisältyä riskin torjuminen lopettamalla riskin aiheuttava toiminta, riskin ottaminen, riskin lähteen poistaminen, riskin todennäköisyyden tai seurausten muuttaminen, riskin jakaminen toisen osapuolen, kuten sopimuksen tai vakuuttamisen kautta, kanssa ja riskin säilyttäminen tietoon perustuvalla päätöksellä. Haitallisten seurausten käsittelyä kutsutaan riskin poistamiseksi tai pienentämiseksi. Hallintakeino kuuluu riskien käsittelyyn siten, että se on riskiä muuttava varsinainen toimenpide. (SFS-opas 73.)

Suomen Riskienhallintayhdistyksen (2017c) mukaan riskien käsittely tarkoittaa sitä, miten riskitaso pidetään tietyn riskin osalta päätetyllä tasolla hyödyntämällä erilaisia hallintakeinoja. Hallintakeinojen vaikuttavuuden arviointi on tarpeen, jotta voidaan päättää, onko jäännösriski, hallintakeinojen jälkeinen riskitaso, hyväksyttävissä vai tarvitaanko lisää hallintakeinoja. Sopivimman hallintakeinon löytämiseksi tulisi tehdä kustannus- ja hyötyanalyysit sekä huomioida vaatimustenmukaisuus. Riskin käsittelyssä tulee huomioida koko organisaation lisäksi sidosryhmät, jotka otetaan mukaan päätöksentekoon, mikäli riskin käsittelyn toimenpiteillä voi olla niihin vaikutusta. Riskin käsittely voi epäonnistua ja sitä seuraava seurausriski tulee huomioida riskienhallintaprosessissa. Riskienhallinnan toimenpiteet tulee sisällyttää riskien arvioinnin dokumenttiin tai laatia omana riskienkäsittelysuunnitelmanaan, johon tulisi sisällyttää päätetyt toimenpiteet resursseineen, mittarit, missä järjestyksessä toimenpiteet suoritetaan ja perustella valinnat kustannuksia ja hyötyjä vertailemalla. (Suomen Riskienhallintayhdistys 2017c.)

Viestintä ja tiedonvaihto ovat riskienhallintaprosessissa jatkuvat ja toistuvat prosessit, joilla organisaatio antaa, jakaa tai hankkii tietoa, joka liittyy riskin luonteeseen, todennäköisyy-

teen, seuraukseen tai käsittelyyn. Organisaatio käy vuoropuhelua sidosryhmiensä kanssa riskien hallinnasta. Tiedonvaihto sidosryhmien kanssa vaikuttaa päätöksiin, mutta ei yhteiseen päätöksentekoon, ja tiedonvaihdossa tulisikin olla hyvissä ajoin yhteydessä sidosryhmiin ennen kuin organisaatio tekee päätöksen jostakin asiasta tai siihen liittyvästä menettelystä. Sidosryhmä on henkilö tai organisaatio, joka voi vaikuttaa päätökseen tai toimintoon, johon jokin päätös tai toiminto voi vaikuttaa. (SFS-opas 73.)

Katselmus on toiminto, jolla arvioidaan asetettujen tavoitteiden saavuttamiseen tarvittavien toimenpiteiden soveltuvuus, riittävyys ja vaikuttavuus. Seuranta on vastaavasti valvontaa, arviointia tai tarkistamista, jolla pyritään tunnistamaan poikkeamat vaaditusta tasosta. Suomen riskienhallintayhdistyksen (2017c) mukaan seuranta kuuluu oleellisesti riskienhallintaprosessiin ja sen on huomioitava organisaation toimintaympäristön muutokset riittävän tehokkaasti. Säännöllinen valvonta kuuluu seurantaan, jonka vastuut tulee määritellä koko organisaation kattavasti ja voidaan vaikuttua hallintakeinojen tehokkuudesta ja toimivuudesta (Suomen Riskienhallintayhdistys 2017c). Katselmus ja seuranta voivat kohdistua riskienhallintaprosessiin ja riskienhallinnan puitteisiin sekä hallintakeinoihin. (SFS-opas 73.)

2.3 Riskien arviointimenetelmät

Riskien arvioinnin tekemiseen tulee valita toimintaympäristöön ja riskien arviointiin parhaiten soveltuva työkalu. Suomen standardisoimisliiton standardi SFS-EN 31010 tarjoaa lukuisia eri riskien arviointimenetelmiä erilaisiin toimintaympäristöihin. Tähän katsaukseen sisältyy liiketoiminta-analyysi, joka on jatkuvuudenhallinnan menetelmä ja potentiaalisten ongelmien analyysi, joka on riskien arviointimenetelmä. Näiden menetelmien lisäksi on tarjolla muita helppokäyttöisiä ja merkittäviä menetelmiä, jotka soveltuvat yleisesti ammattikorkeakoulujen toimintaympäristöön ja toimialaan. Näitä ovat muun muassa kustannus-hyötyanalyysi, juurisyyanalyysi ja vikapuuanalyysi. Kaikki edellä mainitut riskien arviointimenetelmät ovat kuvattu liitteessä 4. Jokaisen ammattikorkeakoulun tulee valita aina omien tarpeidensa ja tavoitteidensa mukaan riskien arviointimenetelmät ja –työkalut (Suomen riskienhallintayhdistys 2017c).

Liiketoiminta-analyysi, joka on englanniksi business impact analysis, on riskien arviointimenetelmä, joka tunnistaa ja määrittää valmiuksien määrän, joka tarvitaan hallitsemaan avainhäiriöriskejä. Liiketoiminta-analyysi antaa myös tietoa organisaation keskeisten prosessien, toimintojen ja niihin liittyvien resurssien sekä riippuvuussuhteiden tunnistamisessa. Analyysi myös selvittää, miten häiriöt vaikuttavat kriittisten liiketoimintatavoitteiden saavuttamiseen sekä resurssit, jotka tarvitaan palauttamaan toiminta sovitulle tasolle, häiriön tapahduttua. Keskeisimmät tuotokset (taulukko 1) luovat pohjan jatkuvuuden hallinnan suunnittelutyölle. (SFS-EN 31010.)

Panokset	Tuotokset
Ryhmän tekemä analyysi.	Luettelo kriittisistä prosesseista ja niiden välisistä riippuvuussuhteista.
Laadittu kyselylomake.	Tunnistettujen kriittisten prosessien tarvitsemat resurssit.
Luettelo haastateltavista, joihin otetaan yhteyttä liittyen keskeisiin prosesseihin.	Keskeytysajan kesto kriittiselle prosessille ja sen tietotekniikan palautumisajat.
Tiedot tavoitteista, toiminnoista ja riippuvuussuhteista.	Prosessien keskeytymisestä johtuvien taloudellisten ja toiminnallisten vaikutusten dokumentit.
Prosessien menettämisestä johtuvat taloudelliset ja toiminnalliset seuraukset.	
Yksityiskohdat toiminnoista, prosesseista ja tukiresurssit.	
	

Taulukko 1: Liiketoiminta-analyysin panokset ja tuotokset (SFS-EN 31010)

Analyysiä käytetään määrittämään prosessien ja niihin liittyvien resurssien kriittisyys sekä palautumisajanjaksot sen varmistamiseksi, että tavoitteissa pysytään. Liiketoiminta-analyysi voidaan toteuttaa kyselylomakkeilla, haastatteluina ja työryhmissä. Menetelmän keskeiset vaiheet ovat:

1. Määritetään keskeiset prosessit sekä niiden kriittisyys riskin perusteella.
2. Määritetään häiriön taloudelliset ja toiminnalliset seuraukset tietyssä prosessissa, tiettynä ajanjaksona.
3. Tunnistetaan riippuvuussuhteet sisäisten ja ulkoisten sidosryhmien kanssa.
4. Määritetään nykyiset ja tarvittavat resurssit toiminnan jatkamiseksi hyväksyttävällä tasolla, häiriön tapahduttua.
5. Tunnistetaan vaihtoehtoisia prosesseja tai kiertoteitä, mikäli nykyiset prosessit ovat riittämättömiä häiriöstä palautumiseksi.
6. Suurimman hyväksyttävän keskeytysajan, jonka organisaatio kestää, määrittäminen prosesseille.

7. Toipumisaikatavoitteiden määrittäminen erikoislaitteille ja tietotekniikalle. Toipumisaika tarkoittaa aikaa, jonka sisällä organisaatio pyrkii palauttamaan erityislaitteet ja tietotekniikan toimimaan.
8. Prosessien nykyinen valmiustaso mahdollisissa häiriötilanteissa. Esimerkkeinä varalaitteet tai varahenkilöjärjestelyt.
   (SFS-EN 31010.)

Potentiaalisten ongelmien analyysi on vaarojen tunnistamismenetelmä, joka hyödyntää eri ammattiryhmien kokemusta ja osaamista. Analyysi perustuu ryhmässä tehtyyn aivoriiheen, jossa tunnistetaan vaaroja, arvioidaan riskejä ja tehdään toimenpide-ehdotuksia riskien käsittelemiseksi (Valtiovarainministeriö 2003, 70-71). Menetelmä soveltuu hyvin laajan kohteen, kuten työpaikan tai osaston keskeisten ongelma-alueiden selvittämiseen. Analyysi soveltuu hyvin myös teknisten järjestelmien ja ihmisten työtoiminnan arviointiin, koska siinä tunnistetaan ja luokitellaan vaaroja yleisellä tasolla. (Suomen riskienhallintayhdistys 2017; Laitinen ym. 2013, 296-297.)

Potentiaalisten ongelmien analyysin valmistelussa tulee huomioida, että analyysiin osallistuu eri asioista tietäviä henkilöitä, joilla on tietoa laadusta tai riskeistä. Mukana tulisi olla laitteiden tai tilojen päivittäisiä käyttäjiä, joilla on todennäköisesti paras tieto tarkasteltavista kohteista ja niihin liittyvistä riskeistä. Osallistujia tulisi olla vähintään kolme tai neljä. Lisäksi työpajalle tarvitaan osaava vetäjä, joka tuntee analyysin menetelmänä hyvin. Vetäjä ei saisi olla johtaja, ettei arvioitsijoiden kesken tule tunnetta siitä, että he eivät voi sanoa jotain, josta voi tulla seurauksia. Riittävät resurssit ja johdon hyväksyntä ovat vaatimuksena työpajalle, kuten riskien arvioinnille yleensäkin. Työpajaan tulisi olla vähintään kaksi tuntia käytettävissä ja häiriöttömät tilat. (Suomen riskienhallintayhdistys 2017; Valtiovarainministeriö 2003, 69-71.)

Työpajan vetäjä kertaa ennen ideointia vielä säännöt, joihin tulisi lukeutua ainakin kertaus rajauksesta ja työpajan tavoitteesta sekä kertoa, että tarkoitus ei ole syytellä tai selitellä vaan keskittyä asioihin ja ongelmiin eikä ihmisiin. Näin työpajassa säilyy avoin ilmapiiri. Työpaja alkaa hiljaisella aivoriihellä, jolloin jokainen osallistuja kirjoittaa lapuille ideoimiaan vaaroja. Laput kiertävät osallistujilta toisille, jolloin jokainen pääsee näkemään muiden ideoimia vaaroja. Vetäjän roolina on tällöin antaa avainsanoja osallistujille, kun vaarojen ideointi alkaa hidastua. (Suomen riskienhallintayhdistys 2017.)

Kun kirjoittaminen hidastuu, siirrytään keskustelumuotoiseen aivoriiheen, jossa osallistujat kertovat oman näkemyksensä ideoimistaan vaaroista. Tavoitteena on selvittää, ovatko vaarat

todellisia, mitkä ovat niiden syyt ja seuraukset. Nämä kirjataan myös analyysin yhteenvetolomakkeille. Samalla yritetään löytää uusia vaaroja, lopuksi kaikki vaarat jaetaan ryhmiin esimerkiksi vaarojen syiden perusteella. (Suomen riskienhallintayhdistys 2017.)

Vaarat muunnetaan tämän jälkeen riskeiksi arvioimalla niiden seurauksien vakavuus ja todennäköisyys (taulukko 2) riskimatriisilla. Muita matriiseja voidaan käyttää myös. Esimerkkinä seuraus-hallinta-riskimatriisi, joka perustuu siihen, miten hyvin vaara hallitaan, todennäköisyyden arvioimisen sijasta. Riskiluku saadaan matriisista molemman nimittäjän perusteella, riippumatta kumpaa matriiseista käytetään. Yleisempi riskimatriisi on kuitenkin seurausten vakavuus-todennäköisyys-riskimatriisi, joka perustuu siihen, että todennäköisyys on yhdellä ja seurauksen vakavuus on toisella akselilla. (Suomen riskienhallintayhdistys 2017; Laitinen ym. 2013, 297-298; Valtiovarainministeriö 2003.)

Todennäköisyys	**Seurauksen vakavuus**		
	vähäiset	**haitalliset**	**vakavat**
epätodennäköinen	merkityksetön riski	vähäinen riski	kohtalainen riski
mahdollinen	vähäinen riski	kohtalainen riski	merkittävä riski
todennäköinen	kohtalainen riski	merkittävä riski	sietämätön riski

Taulukko 2: Seuraus-todennäköisyys riskimatriisi (SFS-EN 31010)

Seuraus-todennäköisyysmatriisi on keino yhdistää seuraus ja todennäköisyys riskitason tuottamiseksi. Potentiaalisten ongelmien analyysissä tunnistetaan todennäköisesti useita riskejä, joiden seulontaan matriisi soveltuu sen selvittämiseksi, mitkä riskit tarvitsevat tarkempaa analysointia. Matriisi soveltuu myös määrittämään, onko tietty riski yleisesti hyväksyttävä sen mukaan, missä se matriisissa sijaitsee. Menetelmän käyttämisessä on tärkeää, että matriisi on räätälöity olosuhteisiin ja toimintaympäristöön, jossa sitä käytetään. Menetelmä perustuu siihen, että molemmille, todennäköisyydelle ja seurauksen vakavuudelle räätälöidään asteikot, jotka kattavat erityyppiset seurausluokat ja jotka ovat niin yksiselitteisiä kuin olla ja voi. (SFS-EN 31010.)

Potentiaalisten ongelmien analyysi, kuten seuraus-todennäköisyysmatriisi ovat molemmat helppoja menetelmiä organisaatiolle, jolla ei välttämättä ole resursseja määrällisemmälle analyysille tai jolla ei ole riittävästi yksityiskohtaista tietoa analyysia varten. Toisaalta voi olla vaikeaa saada yhteen järjestelmä, joka soveltuu organisaation kaikkien olosuhteiden alueelle. Ongelmana on myös se, että riskejä ei pystytä yhdistämään, jolloin on tärkeätä hyvä vaaraluettelointi potentiaalisten ongelmien analyysissa. (SFS-EN 31010.)

Johdon määrittelemän riskitason perusteella tehdään toimenpide-ehdotukset riskien käsittelemiseksi. Ensisijaisesti tulee keskittyä riskin poistamiseen tai pienentämiseen, mikäli vain mahdollista. Osa riskeistä tulee ja on kannattavaa myös pitää omalla vastuulla, riippuen määritellystä riskitasosta. Taulukko 3 esittää järjestyksessään tehtävät analyysin vaiheet. (Suomen riskienhallintayhdistys 2017; Laitinen ym. 2013, 301; Valtiovarainministeriö 2003.)

Vaihe	**Keskeiset tehtävät**
1. Valmistelu	Resurssit, johdon hyväksyntä, osallistujat ja vetäjä.
2. Vaarojen tunnistaminen	Hiljainen aivoriihi, rajaus, tavoitteet, vaarojen kirjaaminen ja avainsanat.
3. Järjestelmällinen arviointi	Keskustelumuotoinen aivoriihi, uusien vaarojen kirjaaminen, luettelointi ryhmittäin, kirjaaminen analyysin yhteenvetolomakkeille.
4. Vaaroista riskeiksi	Riskien todennäköisyyksien ja seurauksien vakavuuksien arviointi asteikolla 1-3.
5. Riskien käsittely	Toimenpide-ehdotuksien määrittäminen riskitason ylittäville riskeille. Ensisijaisesti ennaltaehkäiseviä toimenpiteitä.
6. Raportointi	Kaikki tuotetut dokumentit, kohteen kuvaus ja rajaus, johtopäätökset, yhteenveto ja jatkotoimenpiteet.

Taulukko 3: POA-analyysin vaiheet (Suomen riskienhallintayhdistys 2017a; AHRQ 2017)

Viimeisenä vaiheena analyysi raportoidaan, johon sisältyy työpajassa arvioidut riskit, vaaraluettelo, toimenpide-ehdotukset ja yhteenvetolomake. Kaikki aineisto tulisi myös säilyttää tulevia riskien arviointeja varten. Tällöin helpointa on sähköinen raportointi työpajasta. Hyvällä raportoinnilla myös edesautetaan analyysin katselmusta ja esittelyä. (Suomen riskienhallintayhdistys 2017; Valtiovarainministeriö 2003, 69, 73.)

3 Turvallisuusjohtaminen

Opinnäytetyössä turvallisuusjohtamisella tarkoitetaan kaikkea turvallisuuden kokonaisvaltaista toimintaa, joilla suojataan organisaation arvoja. Kokonaisvaltainen turvallisuusjohtaminen perustuu organisaation strategiaan ja riskienhallintaan. Kokonaisvaltaisella turvallisuusjohtamisella tarkoitetaan tässä opinnäytetyössä myös toimintaa, joka kattaa kaikki turvallisuuden eri ulottuvuudet, jotka myös esitellään. Eri turvallisuusjohtamisen osa-alueet painottuvat korkeakoulun turvallisuustoiminnassa riippuen organisaatiosta, vaikka samat periaatteet pätevät käytännössä kaikkiin suomalaisiin ammattikorkeakouluihin. Turvallisuusjohtamisella

ohjataan eri osa-alueiden toimintaa ja suojellaan arvoja, mutta toiminta itsessään tulisi tähdätä organisaation toiminnan jatkuvuuden varmistamiseen kaikissa tilanteissa ja olosuhteissa sekä vaatimusten mukaiseen toimintaan.

3.1 Turvallisuusjohtamisen periaatteet

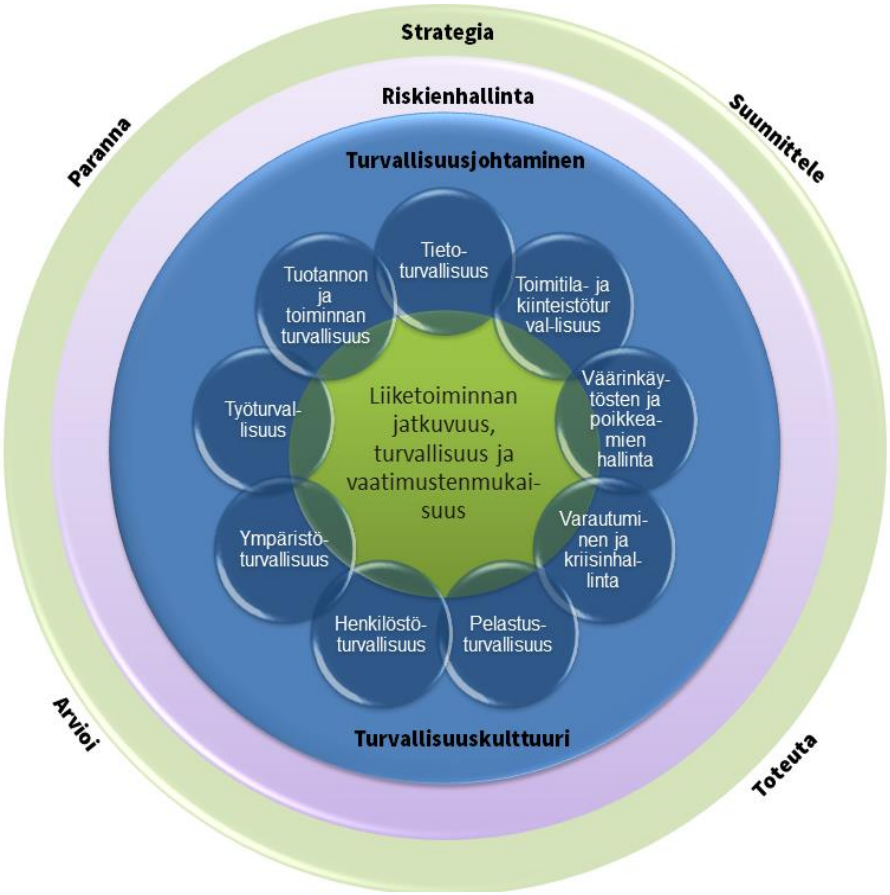
EK:n (2017) mukaan ”Turvallisuusjohtaminen on osa normaalia yrityksen johtamista”. Paasosen (2012, 80) mukaan turvallisuusjohtaminen on kokonaisvaltaista toimintaa organisaation turvallisuuden hallintaan, ja turvallisuusjohtaminen on prosessi, jossa yhdistyvät ennaltaehkäisevä ja ongelmiin reagoiva työympäristö jatkuvaksi parantamiseksi. Kerkon (2001, 38) mukaan turvallisuusjohtaminen on selkeää ja johdonmukaista yhteistyötä, jossa liiketoimintaprosessien eri vaiheet erottuvat selkeästi toisistaan, kaikki tietävät velvollisuutensa ja toimintaa ohjataan johdonmukaisella päätöksenteolla ja tavoitteellisuudella. Turvallisuusjohtaminen onkin pohjimmiltaan kiinteä osa organisaation strategiaa ja päätöksentekoa, eikä erillinen toiminto (Kerko 2001, 31).

Turvallisuusjohtaminen on Reimanin ja Oedewaldin (2008, 66) mukaan ottanut esimerkkiä laatujärjestelmistä, joita alettiin kehittää Suomessa 1980-luvun lopussa. Reiman ja Oedewald (2008, 66) toteavat Reasonin ja Hobbsin (2003, 162) mukaan, että laadulle ja turvallisuudelle yhteisiä piirteitä ovat, että molempia on johdettava ja suunniteltava ja ne nojaavat mittaamiseen ja seurantaan sekä dokumentointiin, käsittävät koko organisaation henkilöstön ja kaikki toiminnot sekä molemmat pyrkivät jatkuvaan parantamiseen.

Yritysturvallisuus tai organisaatioturvallisuus on EK:n termi turvallisuusjohtamiselle, jolla tarkoitetaan kaikkia turvallisuuden toimintoja, joilla suojataan organisaatiolle tärkeitä arvoja, kuten omaisuutta, henkilöstöä, mainetta, tietoa ja ympäristöä. Kerkon (2001, 32) mukaan turvallisuusjohtaminen on erityisen tärkeää liiketoiminnan vaatimusten kannalta, koska ilman turvallisuusjohtamisjärjestelmää organisaation on vaikea toimia lainsäädännön vaatimuksien mukaan. EK (2017) selvittääkin, että turvallisuusjohtamisen tavoite on organisaation vaatimuksenmukaisuuden lisäksi organisaation jatkuvuuden varmistaminen kaikissa tilanteissa. (EK 2017; Kerko 2001, 21.)

Organisaation kokonaisvaltainen turvallisuusjohtaminen koostuu Kerkon (2001, 31) mukaan useista osa-alueista, joista jokaisesta on huolehdittava. EK (2017) on kehittänyt turvallisuusjohtamisen mallin, joka soveltuu kaikille yrityksille ja organisaatioille. Malli (kuvio 2) esittää, että organisaation liiketoiminta ja toimiala ohjaavat aina riskienhallinta- ja turvallisuusjohtamisprosessia sekä turvallisuusjohtamisen osa-alueita. Riskienhallinta antaa vastaavasti edellytykset turvallisuuskulttuurin ja turvallisuusjohtamisen kehittämiselle. Suunnittele-toteuta-ar-

vioi-paranna viittaa vastaavasti jatkuvan parantamisen prosessiin, joka soveltuu liiketoiminnan ja riskienhallinnan lisäksi turvallisuusjohtamiseen, joka luo Kerkon mukaan (2001, 22) pohjan turvallisuusjohtamisjärjestelmälle. (EK 2017.)



Kuvio 2: Turvallisuusjohtamisen malli (EK 2017)

EK:n (2017) turvallisuusjohtamismalli sisältää osa-alueet, jotka ovat henkilöstöturvallisuus, kiinteistö- ja toimitilaturvallisuus, pelastusturvallisuus, tuotannon ja toiminnan turvallisuus, ympäristöturvallisuus, tietoturvallisuus, väärinkäytösten ja poikkeamien hallinta, varautuminen ja kriisinhallinta sekä työturvallisuus. Näiden osa-alueiden tarkempi tarkastelu on tarpeen, jotta pystytään kehittämään turvallisuusjohtamista kokonaisvaltaisesti. Kokonaisvaltainen turvallisuusjohtaminen on tarpeen, jotta turvallisuuden kehittämisestä ei tule sirpalemaista toimintaa ilman selkeää suuntaa ja tavoitteita. Martikaisen (2016, 6) mukaan suomalaisten ammattikorkeakoulujen turvallisuusjohtaminen on yleisesti sirpaleista.

3.2 Jatkuvuudenhallinta

Martikainen (2016b, 15) on todennut, että oppilaitos hallitsee toimintakykyänsä kaikissa häiriötilanteissa varautumisella, joka on jatkuvuudenhallintaa; toimintaa, jolla varmistetaan häiriötön toiminta varautumalla erilaisiin häiriötilanteisiin. Liiketoiminnan jatkuvuudenhallinta on SFS-EN 22301 -standardin mukaan prosessi, jossa tunnistetaan organisaatioon kohdistuvat uhat ja niiden vaikutukset liiketoimintaan ja joka mahdollistaa organisaation mukautumiskyvyn ja tehokkaan reagoinnin häiriöihin sekä tärkeimpien sidosryhmien toimintojen suojaamisen. Huoltovarmuuskeskuksen (2017) mukaan jatkuvuudenhallinta on toimintamalli, jolla organisaatio tunnistaa toimintansa riskit, häiriötilanteet ja riippuvuudet, organisoi ja toteuttaa menettelytavat häiriötilanteiden varalle, varmistaa kriittisten sidosryhmiensä kyvyn toimia häiriötilanteissa ja suojaa toimintansa intressit sekä arvontuotannon kykynsä. Jatkuvuudenhallinnan systemaattisen kehittämisen avulla vähennetään toimintakatkoista johtuvia kustannuksia, tehostetaan toimintaa häiriötilanteissa ja nopeutetaan tilanteesta toipumista (Huoltovarmuuskeskus 2017).

Jatkuvuussuunnittelun tavoitteena on varmistaa organisaation ydintoimintojen mahdollisimman häiriötön toiminta ja se on osa organisaation kokonaisturvallisuutta (Valtiovarainministeriö 2016). Jatkuvuussuunnittelu pyrkii erityisesti pienentämään toimintaa haittaavien tapahtumien vaikutusta ja kestoa. Jatkuvuussuunnitelma ohjaa organisaatiota reagoimaan, palautumaan, jatkamaan ja palauttamaan ennalta määritellyn toimintatason häiriötilanteen jälkeen. Suunnitelma sisältää resurssit, palvelut ja toiminnot, joita kriittisten liiketoimintojen jatkaminen vaatii. (SFS-EN 22301; Valtiovarainministeriö 2016, 7, 24.)

Organisaation liiketoiminnan jatkuvuussuunnittelu aloitetaan johdon määrittäessä resurssit, laatimalla jatkuvuuden hallinnan periaatteet, edistämällä jatkuvaa parantamista ja osoittaen sitoutumisensa jatkuvuussuunnitelman suunnittelulle, laatimiselle, ylläpidolle ja seurannalle. Seuraavaksi tehdään liiketoiminnan vaikutusanalyysi, joka on keskeinen osa organisaation jatkuvuuden hallintaa. Vaikutusanalyysissä organisaatio määrittelee jatkuvuuden ja palautumisen tärkeysjärjestyksen, tavoitteet ja kohteet. Riskien arvioinnilla vastaavasti tunnistetaan, analysoidaan ja arvioidaan järjestelmällisesti organisaatioon kohdistuvat häiriöriskit, jatkuvuuden hallinnan näkökulmasta. Vaikutusanalyysin ja riskienarvioinnin voi suorittaa eri menetelmillä SFS-ISO 31000 -standardin mukaisesti. Tässä opinnäytetyössä vaikutusanalyysin ja riskienarvioinnin menetelmänä esitellään liiketoiminta-analyysi. (SFS-EN 22301.)

Organisaation on Koskenrannan (2012) mukaan luotava, toteutettava, käytettävä, valvottava, katselmoitava, ylläpidettävä ja jatkuvasti kehitettävä hallintajärjestelmää, jotta organisaatio voi suojautua, varautua ennalta ja toimia häiriöiden aikana sekä toipua normaalille palvelutasolle niiden jälkeen. Koskenranta (2012, 8, 24) nostaa esille ISO 22301 -standardin jatkuvuu-

denhallinnan järjestelmän vaatimuksista, koska se soveltuu arvioimaan kaikkien organisaatioiden kyvykkyyttä kohdata jatkuvuudelle esitetyt tarpeet ja vaatimukset, myös korkeakoulujen. (SFS-EN 22301.)

SFS-EN 22301 -standardi hyödyntää Koskenrannan (2012, 25) mukaan PDCA-mallia jatkuvuudenhallinnan jatkuvaan parantamiseen ja se on yhdenmukainen muidenkin standardien SFS-EN ISO 14001, SFS-EN 9001 ja SFS-ISO/IEC 27001 kanssa. Suunnitteluvaiheessa tulisi luoda jatkuvuuspolitiikka, tavoitteet ja päämäärät, prosessit ja menettelyt tavoitteena parantaa liiketoiminnan jatkuvuutta. Seuraavaksi sovelletaan ja toteutetaan organisaation jatkuvuuspolitiikka, tavoitteita ja päämääriä sekä prosesseja ja menettelyjä. Seuranta ja katselmointi kohdistuvat politiikkaan ja tavoitteisiin, joiden tuloksista raportoidaan johdolle, joka voi päättää korjaavista ja parantavista toimenpiteistä. Johdon päättämät toimenpiteet toteutetaan, millä ylläpidetään ja parannetaan jatkuvuudenhallintajärjestelmää sekä arvioidaan jatkuvuuspolitiikkaa ja tavoitteita. (Koskenranta 2012, 25; SFS-EN 22301.)

ISO 22320 -standardin ”Emergency management” viittaa Koskenrannan (2012, 8, 26) mukaan esimerkiksi kriisijohtamiseen tai poikkeamien hallintaan ja se nostetaan esille yhdeksi korkeakouluille soveltuvista turvallisuusjohtamisen standardeista. Standardi ohjeistaa luomaan kriisijohtamisen mallin, joka perustuu tilannekuvaan, sidosryhmäyhteistyöhön, johtamisvastuisiin ja päätöksentekoon. Kriisijohtamiseen sisältyy myös suunnittelu ja harjoittelu, ja Koskenranta (2012, 26) painottaa myös sisäisen- ja ulkoisen viestinnän keskeistä merkitystä onnistuneessa kriisijohtamisessa. (ISO 22320.)

3.3 Turvallisuusvaatimusten täyttäminen

Ammattikorkeakoululaki (932/2014) toimii perustana ammattikorkeakoulujen turvallisuudelle. Ammattikorkeakoulun opiskelijalla on oikeus turvalliseen opiskeluympäristöön ja koulu voi asettaa järjestyssäännöt, joilla voidaan antaa turvallisuuden ja viihtyisyyden kannalta tarpeellisia määräyksiä. Omaisuuden käsittelemisestä ja liikkumisesta ammattikorkeakoulun tiloissa ja alueella voidaan antaa myös tarpeellisia määräyksiä. (Ammattikorkeakoululaki 932/2014.)

Valmiussuunnitelmat ovat ammattikorkeakouluille pakollisia, jotta se pystyy hoitamaan tehtäviänsä mahdollisimman hyvin ja häiriöttömästi myös poikkeusoloissa. Opetus- ja kulttuuriministeriö valvoo varautumista ja se voi määrätä puutteiden korjaamisesta. Opetus- ja kulttuuriministeriö voi vaatia varautumissuunnitelmien lisäksi häiriö- ja erityistilanteista laaditut tilannekuvaraportit. (Ammattikorkeakoululaki 932/2014.) Jokaisen ammattikorkeakoulun tulisi lisäksi sisäistää pelastusturvallisuuteen ja kiinteistöturvallisuuteen liittyvät lain vaatimukset,

koska usean henkilön samanaikainen siirtyminen suurissa rakennuksissa ei ole itsestäänselvyys. Pelastuslain (379/2011) mukaista pelastussuunnitelmaa ja rakentamismääräyksien (Edilex 2016) mukaisia kunnossapito- ja huoltovelvoitteita tulisi noudattaa, jotta ammattikorkeakoulujen tilat ja käyttäjien osaaminen mahdollistavat turvallisen poistumisen tai sisälle siirtymisen hätätilanteessa.

Työturvallisuuslaki (738/2002) on yleisesti työntekijän turvallisuutta säätelevää lainsäädäntöä, joka velvoittaa työnantajaa useisiin toimiin työntekijöiden turvallisuuden varmistamiseksi ja monen muun lain, asetuksen tai päätöksen huomioimiseen. Työntekijöiden ja opiskelujen turvallisuutta käsittelevää lainsäädäntöä on hyvin paljon ja kaikki vaatimukset tulisi kartoittaa erikseen, tila ja käyttäjäkunta kerrallaan, jotta voidaan varmistua vaatimusten noudattamisesta. Työturvallisuuslaissa säädellään muun muassa työsuojelutoiminnasta, vaarojen ja riskien arvioimisesta sekä niiden hallintatoimenpiteistä (738/2002).

Ammattikorkeakouluja koskettavaa lainsäädäntöä on paljon. Tärkeintä on se, että jokainen koulu tunnistaa itseään koskevat vaatimukset. Tässä opinnäytetyössä on tehty nostoja turvallisuusjohtamisen tärkeimmistä lainsäädännön, päätöksien, ohjeiden ja EU-direktiivien vaatimuksista, jotka koskettavat suomalaisia ammattikorkeakouluja. Turvallisuusjohtamisen oikeudellista vastuuta koskevaa sääntelyä on paljon, vaikka se ei välttämättä kohdistu suoraan turvallisuusjohtamiseen vaan eri tilanteisiin ja henkilöihin yleisellä tasolla (Paasonen, 104).

3.4 Henkilöstöturvallisuus

Henkilöstöturvallisuus on EK:n (2017) ja Leppäsen (2006, 204) mukaan keskeinen osa organisaation turvallisuutta ja sillä pyritään takaamaan ihmisten turvallisuus ja toiminta suojaten heitä rikoksilta ja häiriöiltä. Kerkon (2001, 265-271), EK:n (2017) ja Leppäsen (2006, 204-217) mukaan henkilöstöturvallisuus koostuu asiakkaiden ja vierailijoiden turvallisuudesta, avainhenkilöiden turvallisuudesta, kodin ja perheen turvallisuudesta, matkustusturvallisuudesta, varahenkilöjärjestelyistä ja rekrytoinnin luotettavuusmenettelyistä tai luotettavuuden varmistamisesta, johon voidaan lukea mukaan turvallisuusselvitykset, huumausainetestaukset ja salassapitosopimukset.

Kerkon (2001, 271) ja Leppäsen (2006, 205) mukaan asiakkaiden ja vierailijoiden turvallisuus vaikuttaa siihen, millaisen mielikuvan asiakkaat saavat organisaatiosta ja miten organisaatio ylipäätänsä suhtautuu vierailijoihin ja asiakkaisiin. Ammattikorkeakoulun asiakkaat ovat esimerkiksi tutkinto-opiskelijoita ja muita maksulliseen kurssiopetukseen osallistuvia kurssilaisia (Arcada 2017). Leppäsen (2006, 206) mukaan asiakkaiden ja vierailijoiden turvallisuusjärjeste-

lyt tulee liittää osaksi toimitila- ja tietoturvallisuuskäytäntöjä. Vierailevat henkilöt ovat organisaation vastuulla, joten erityisen perehdytyksen tai koulutuksen vaatimien tilojen esittelyä tulisi ainakin harkita, mikäli tilat sisältävät esimerkiksi koneita ja laitteita.

Avainhenkilö on Höökin (2016) mukaan henkilö, jonka tiedot, taidot, pätevyys ja persoona ovat kriittisiä organisaation olemassaololle ja jonka menettäminen saattaisi vaikuttaa merkittävästi organisaatioon. Kerkon (2001, 266) mukaan avainhenkilöiden tunnistamisella ja heidän osaamisen jakamisella varmistetaan liiketoiminnan jatkuvuus, mikäli avainhenkilö poistuu tai on muuten estynyt osallistumasta organisaation toimintaan. Leppäsen (2006, 207) mukaan avainhenkilöiden tunnistamisen tulee perustua liiketoimintaprosessien analysointiin. Jokaiselle henkilöresurssille tulisi määritellä osaamisvaatimukset, minkä jälkeen voidaan arvioida jokaisen henkilön osaaminen ja korvaamattomuus. Avainhenkilöriskien hallintatoimenpiteet perustuvat sijaisjärjestelyihin ja muun henkilöstön osaamisen lisäämiseen. Ihanteellisessa tilanteessa vähintään kaksi henkilöä pystyy hoitamaan jokaista toimintoa ja kriittistä toimintoa vähintään kolme henkilöä. (Leppänen 2006, 206-207.)

Leppäsen (2006, 208) mukaan matkustusturvallisuus tarkoittaa työntekijän turvallisuutta matkustettaessa työtehtävien takia koti- ja ulkomailla. Työnantajan on annettava työntekijälle matkustusturvallisuusohjeet, ja erilainen toimintaympäristö tulee huomioida ohjeistuksessa kohdemaan tai -alueen mukaan. Perusperiaatteita ulkomaan matkustusturvallisuuden riskien hallinnassa ovat alkoholin käytön rajoittaminen, maan kulttuuria ja tapoja kunnioittava käytös sekä liikkuminen vain alueilla, joissa on muitakin ulkomaalaisia. (Leppänen 2006, 210-211.)

Rekrytoitaessa uutta työntekijää tulisi Kerkon (2001, 269) ja Leppäsen (2006, 214) mukaan hyödyntää erilaisia luotettavuusmenettelyjä, jotta työnantaja saa oikeanlaista henkilöstöä sekä pystyy ennaltaehkäisemään erilaisia väärinkäytöksiä. Menettelyihin tarvitaan aina hakijan suostumus. Eräs menettely on Suojelupoliisin (2017) tekemä henkilöturvallisuusselvitys, jossa poliisin selvittää selvityksen pyytäjälle, työnantajalle, hakijan tietoja hyödyntämällä erilaisia viranomaisten henkilörekistereitä. Suojelupoliisi tekee Suomessa kaikki siviilipuolen turvallisuusselvitykset, jotka voidaan tehdä henkilön lisäksi myös yritykselle (Suojelupoliisi 2017). Henkilöturvallisuusselvitys laaditaan suppeana, perusmuotoisena tai laajana, riippuen haettavan tehtävän vaatimuksista ja esimerkiksi sen perusteella, pääseekö tehtävässä käsiksi suojausluokituksen alaisiin asiakirjoihin (L726/2014).

Huumausainetestin tarkoituksena on Leppäsen (2006, 214) mukaan selvittää kohdehenkilön laittomien huumaus- ja lääkeaineiden käyttö. Koska testitulos kertoo työntekijästä aina arkaluontoista tietoa, tulee testejä teettää vain tarpeellisten työtehtävien kannalta. Työnantaja

voi velvoittaa työnhakijan huumausainetestiin, mikäli huumeiden alaisena voi esimerkiksi vaarantaa itsensä tai toisen hengen, terveyttä tai työturvallisuutta, vaarantaa liikenneturvallisuutta tai ammattisalaisuutta. Työnantaja voi velvoittaa myös työntekijän huumausainetestiin, mikäli on perusteltua syytä epäillä, että työntekijä on huumausaineiden vaikutuksen alaisena töissä sekä hänen työskentely huumausaineiden alaisena vakavasti vaarantaa itsensä tai toisen henkeä, terveyttä tai työturvallisuutta. (Laki yksityisyyden suojasta työelämässä 759/2004.)

3.5 Työturvallisuus

Työsuojelutoiminta ja työterveyshuolto muodostavat työturvallisuustoiminnan, joka on vahvasti säädeltyä Työturvallisuuslaissa (738/2002). Työturvallisuustoiminnan tavoitteena on turvallinen työ ja työntekijöiden hyvinvointi. Työturvallisuuden toimintaohjelman avulla kehitetään EK:n (2017) mukaan työturvallisuutta ja ohjelma sisältääkin konkreettiset toimenpiteet työn terveydellisten haittojen ehkäisemiseksi. Työsuojeluorganisaatio koostuu organisaation työsuojelun toimikunnasta, johon kuuluvat työturvallisuuspäällikkö ja työsuojeluvaltuutetut. (EK 2017.)

Työnantaja ja työntekijä ovat Työsopimuslakiin (55/2001) vedoten velvollisia huolehtimaan työturvallisuudesta työntekijän suojelemiseksi työtapaturmilta ja terveyteen kohdistuvilta vaaroilta, kuten säädetään Työturvallisuuslaissa (738/2002). Työnantajan tulee huolehtia työntekijöiden turvallisuudesta ja terveydestä tarpeellisilla toimenpiteillä, jotka on suunniteltava ja toteutettava työolosuhteiden parantamiseksi. Työnantajan tulee noudattaa periaatteita, että vaara- ja haittatekijöiden syntyminen estetään tai poistetaan. Mikäli poistaminen ei ole mahdollista, tulee ainakin vähentää haittaa ja vaaraa. Työnantaja myös velvoitetaan tarkkailemaan työympäristöä, työyhteisön tilaa ja työtapojen turvallisuutta sekä seurattava toteutettujen toimenpiteiden vaikutusta työn turvallisuuteen ja terveyteen. Laitisen ym. (2013, 178) mukaan periaatteena on myös jatkuva parantaminen, koska työnantajan tulee seurata myös tekniikan ja muiden torjuntakeinojen kehittymistä ja otettava ne huomioon toimenpiteissään. (Työturvallisuuslaki 738/2002.)

Työturvallisuuslain (738/2002) 9 § määrittää työsuojelun toimintaohjelmasta, joka sisältää työympäristöön liittyvien tekijöiden vaikutukset ja työolojen kehittämistarpeet. Ohjelman perusteella asetetaan turvallisuuden ja terveyden edistämiseksi tavoitteet, jotka tulee huomioida kaikessa työpaikan kehittämistoiminnassa. Laitisen ym. (2013, 179) mukaan työsuojelun toimintaohjelmalla tarkoitetaan erilaisten johtamisstandardien turvallisuuspolitiikkaa vastaavaa ohjelmaa, jolla johto ilmaisee organisaation yleiset tavoitteet ja periaatteet. Turvallisuuden johtaminen edellyttää johdon tahtoa, toimintasuunnitelmia ja niiden toteutusta (Laitinen ym. 2003, 179; Työturvallisuuslaki 738/2002.)

Työturvallisuuslaki perustuu organisaation omaan vastuuseen työturvallisuudestaan, mikä tarkoittaa Laitisen ym. (2013, 179) mukaan sitä, että työnantajan tulee itse selvittää haitta- ja vaaratekijät. Työtapaturmien ja terveyshaittojen esiintyessä työnantaja ei voi vedota tietämättömyyteen. Työturvallisuuslain (738/2002) 10 § säätää järjestelmällisestä vaarojen ja haittojen selvittämisestä, joka tarkoittaa, että haittojen ja vaarojen merkitys työntekijöille tulee arvioida. Selvitys ja arviointi tulee olla ajantasainen ja työnantajan hallussa. (Työturvallisuuslaki 738/2002.)

Työnantajan tulee Työturvallisuuslain (738/2002) mukaan perehdyttää työntekijä työhön, työpaikan olosuhteisiin, työvälineisiin sekä turvallisiin työtapoihin. Työntekijälle tulee myös antaa tiedot työn haitoista ja vaaroista, miten haittoja ja vaaroja estetään ja torjutaan sekä opastusta häiriö- ja poikkeustilanteiden varalta (Työturvallisuuslaki 738/2002). Laitinen ym. (2013, 180) korostavat, että myös esimiehille on annettava opetus ja ohjaus, ja ulkomaalaisille annettava ohjaus on annettava heidän ymmärtämällään kielellä.

Työntekijän velvollisuuksiin kuuluu ilmoittaa työssä havaituista vioista ja puutteista työnantajalle ja työsuojeluvaltuutetulle, jos vika tai puute voi aiheuttaa haittaa tai vaaraa työntekijälle. Työnantajan tulee puolestaan kertoa työntekijälle ja työsuojeluvaltuutetulle, mitä toimenpiteitä tullaan tekemään haitan tai vaaran poistamiseksi. Työntekijällä on myös velvollisuus noudattaa työnantajan ohjeita ja määräyksiä sekä yleisesti noudatettava turvallisuuden ja terveyden ylläpitämiseksi vaadittavaa huolellisuutta ja varovaisuutta. Mikäli työstä aiheutuu vakavaa vaaraa työntekijälle, saa hän vastaavasti pidättäytyä työnteosta ennen kuin työnantaja on poistanut vaaratekijät siten, että työn voi suorittaa turvallisesti. (Työturvallisuuslaki 738/2002.)

3.6 Tietoturvallisuus

Tietoturvallisuus perustuu Whitmanin & Mattordin (2016, 2), EK:n (2017) ja Leppäsen (2006, 260) mukaan organisaation tietojen luottamuksellisuuden, käytettävyyden ja eheyden suojelemiseen. Whitman & Mattord (2016, 2) määrittelevät lisäksi, että suojeleminen suunnitellaan ja toteutetaan politiikan, ohjeistuksen, koulutuksen, harjoittelun, turvallisuustietoisuuden lisäämisen ja teknologian avulla. Whitman & Mattord (2016, 6) toteavat, että tietoturvallisuusalan kolme perusarvoa muodostavat kolmion (kuvio 3), jonka keskellä on suojeltavat arvot, tieto ja palvelut.

Kuvio 3: Tietoturvallisuuden perusarvot -kolmio (Whitman & Mattord 2016, 7)

Tiedon käytettävyydellä Leppänen (2006, 260) ja Whitman & Mattord (2016, 8) tarkoittavat tiedon oikean, tarkoituksenmukaisen, käsittelijän mahdollisuutta muuttaa, käsitellä, siirtää ja tuhota tieto. Tieto on ehyttä silloin, kun se on kokonaan käytettävissä, muuttumattomana sekä käytettävissä sellaisessa muodossa, joka mahdollistaa tiedonkäsittelyn ilman että tietoa on muutettu mitenkään (Whitman & Mattord 2016, 8; Leppänen 2006, 260). Luottamuksellisuus tarkoittaa Whitmanin & Mattordin (2016, 7) mukaan tiedon käytettävyyden rajaamista niihin henkilöihin, jotka tarvitsevat kyseistä tietoa sekä estää pääsy niiltä, jotka eivät tarvitse. Luottamuksellisuutta voidaan suojata useilla toimenpiteillä, joita ovat Whitmanin & Mattordin (2016, 7) mukaan tiedon luokittelu, tiedon turvallinen varastointi, yleisten turvallisuusohjeiden ja -politiikkojen hyödyntäminen, tiedon loppukäyttäjien kouluttaminen ja tiedon suojaaminen kryptografian periaatteiden mukaisesti.

EK (2017) neuvoo panostamaan toiminnan jatkuvaan varmistamiseen ja jatkuvaan parantamiseen; menetelmien jatkuva seuraaminen ja toimenpiteiden kehittäminen painottuvat tietoturvallisuudessa nopean teknologisen kehityksen takia. Tietoturvallisuus koostuu tietojen merkityksen arvioinnista, tietojen luokittelusta ja käsittelystä, hallinnollisesta tietoturvallisuudesta, tieto- ja yksityisyydensuojasta, teknisestä tietoturvallisuudesta ja järjestelmien ja prosessien jatkuvuuden varmistamisesta (EK 2017). Whitmanin & Mattordin (2016, 4-5) mukaan tietoturvallisuus sisältyy tietoturvallisuusjohtamisen osa-alueisiin, jotka ovat lisäksi tietokoneiden turvallisuus ja tietoverkkojen turvallisuus.

Tietoturvallisuuden johtaminen on osa organisaation johtamista. Tietoturvallisuuden periaatteet voidaan Whitmanin & Mattordin (2016, 42-44) mukaan tiivistää kuuteen elementtiin, jotka ovat suunnittelu, politiikka, ohjelmat, suojeleminen, ihmiset ja projektit. Tietoturvallisuuden suunnittelu koostuu kaikista toimenpiteistä, jotka ovat välttämättömiä tietoturvallisuusstrategian luomiselle, kehittämiselle ja toteuttamiselle. Tietoturvallisuuden strategia

kattaa koko organisaation, joten on tärkeää, että tietoturvajohtaja konsultoi linjaorganisaation keskijohtoa strategian ja politiikan kehittämisessä. Tietoturvapolitiikka koostuu keskeisesti ohjeistosta ja se voi olla koko organisaation kattava, rajattu tiettyyn järjestelmään tai tiettyyn toimintoon. (Whitman & Mattord 2016, 42-44.)

Suojaaminen tarkoittaa Whitmanin & Mattordin periaatteissa (2016, 43) riskiperusteisia toimenpiteitä, joilla hallinnoidaan kokonaisvaltaisesti tietoturvallisuuden suunnittelua. Ihmiset muodostavat tärkeimmän tekijän tietoturvallisuuden johtamisessa, koska organisaatiossa henkilöt käsittelevät tietoa ja henkilöstöturvallisuuden ylläpitäminen tarkoittaa luottamuksellisen ja avoimen ilmapiirin sekä yleisesti turvallisuuskulttuurin rakentamista (Leppänen 2006, 285-286). Projektinhallinnan periaatteiden noudattaminen on tärkeää tietoturvallisuuden hankkeissa, jotta pystytään tunnistamaan ja hallinnoimaan projektille myönnettyjä resursseja, mittaamaan hankkeen edistymistä ja tekemään korjaavia toimenpiteitä hankkeen tavoitteiden saavuttamiseksi. (Whitman & Mattord 2016, 42-44.)

Tietoaineistojen luokittelu on osa keskeinen osa tietoturvallista organisaatiota ja sillä voidaan Leppäsen (2006, 262) ja Whitmanin & Mattordin (2016, 330-331) mukaan hallita tietojen käyttöön, säilyttämiseen, siirtämiseen ja tuhoamiseen liittyviä riskejä ja niiden hallintakeinoja. Leppänen (2006, 262) toteaa, että ensisijainen luokitteluperuste on se, miten julki tuleva tieto vaikuttaa organisaation toimintaan. Esimerkkinä tietoaineistojen luokittelusta on valtionhallinnon viranomaisia koskeva Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (A681/2010), joka säätää salassa pidettävien asiakirjojen luokittelussa neljä suojaustasoa, joissa I -suojaustason asiakirjan oikeudeton käyttö tai paljastuminen voi aiheuttaa erityisen suurta vahinkoa yleiselle edulle. Vastaavasti IV -suojaustason asiakirjan oikeudeton käyttö tai paljastuminen voi aiheuttaa korkeintaan haittaa yleiselle tai yksityiselle edulle, joten voidaan päätellä, että Asetuksen (A681/2010) luokittelu perustuu sen paljastumisen aiheuttamien seurauksien vakavuuteen.

Fyysinen tietoturvallisuus on Leppäsen (2006, 287) mukaan tietoaineistojen ja -välineiden ja niitä ympäröivien tilojen rakenteellista ja toiminnallista suojaamista. Fyysinen tietoturvallisuus tulee liittää osaksi kiinteistöturvallisuutta, koska fyysisiä tietoturvariskejä ovat esimerkiksi paloriskit, vesi- ja kosteusriskit ja sähköriskit. Fyysinen tietoturvallisuus erottuu omaksi alueekseen, koska esimerkiksi sähkön saannin estyminen voi keskeyttää tietoaineistojen tallentamisen ja vaarantaa tietovarastot, mikäli varasähköjärjestelmiä ei ole olemassa tai ne pettävät juuri silloin, kun niitä tarvitsisi. (Leppänen 2006, 287-289.)

SFS-ISO/IEC 27001 -standardi tietoturvallisuuden hallintajärjestelmän vaatimuksista on yksi tietoturvallisuusalan käytetyimmistä Whitmanin & Mattordin (2016, 341) mukaan ja se soveltuu myös korkeakoulujen käyttöön Koskenrannan (2012, 8, 22-23) mukaan. Standardi (SFS-

ISO/IEC 27001) esittää, että organisaation tulisi jatkuvan parantamisen periaatteiden mukaisesti luoda ja toteuttaa tietoturvallisuuden hallintajärjestelmä, joka tukee organisaation liiketoimintaa. Hallintajärjestelmän luomiseksi tulee täyttää vaatimukset, joita ovat muun muassa riskien tunnistaminen ja arviointi, hallintapolitiikan luominen, valita valvontatavoitteet ja saada johto sitoutumaan, tukemaan ja katselmoimaan hallintajärjestelmää varmistaakseen, että järjestelmä on soveltuva. Johto arvioi kehittämistarpeet, joita toteutetaan jatkuvan parantamisen periaatteiden mukaisesti. (SFS-ISO/IEC 27001; Koskenranta 2012, 23-24.)

Tietosuoja ja yksityisyyden suoja työelämässä ovat osa tietoturvallisuutta (EK 2017). Laki ottaa kantaa tietosuojaan siten, että Henkilötietolaki (523/1999) säätää henkilötietojen käsittelystä ja tietojen muodostamista henkilörekistereistä sekä rekisterin ylläpitäjän vastuista. Vastaavasti Laki yksityisyyden suojasta työelämässä (759/2004) säätää henkilötietojen käsittelyn edellytyksien lisäksi kameravalvonnasta työpaikalla ja erinäisten testien ja tarkastuksien tekemisestä sekä niistä syntyvien tietojen käsittelystä.

EU:n uusi tietosuoja-asetus (679/2016) on tullut jo voimaan ja se velvoittaa kaikkia EU:n yrityksiä 25. toukokuuta 2018 alkaen toimimaan asetuksen säädösten mukaisesti, siirtymäajan päätyttyä. Asetuksen tarkoitus on Tietosuojavaltuutetun toimiston (2017, 3) mukaan ajantasaistaa tietosuojan sääntelyä, jotta voidaan vastata teknologian kehitykseen ja henkilötietojen suojaa koskeviin haasteisiin. EU:n asetus (679/2016) velvoittaa muun muassa riskiperusteiseen lähestymistapaan henkilötietojen käsittelyssä ja dokumentoinnin avulla tapahtuvaan osoitusvelvollisuuteen tietosuojaperiaatteiden noudattamisesta (Tietosuojavaltuutetun toimisto 2017, 6-7).

3.7 Kiinteistö- ja toimitilaturvallisuus

EK:n (2017) mukaan toimipaikkoja ja -tiloja tulee suojata riskien arviointiin perustuen kustannustehokkaasti. Kiinteistö- ja toimitilaturvallisuuden tavoitteena on luoda häiriötön ja turvallinen työskentely- ja asiointiympäristö sekä estää organisaatiolle arvokkaan tiedon tai materiaalin anastaminen (EK 2017). Kerkon (2001, 278-289), Leppäsen (2006, 342-374) ja EK:n (2017) mukaan kiinteistö- ja toimitilaturvallisuus on ennen kaikkea rakenteellista turvallisuutta ja turvallisuuden valvontaa. Lisäksi EK (2017) ja Leppänen (2006, 343-356) nostavat esille myös turvallisuusluokittelun ja luokituksenmukaisen suojaamisen, joilla tarkoitetaan kehäsuojaus- ja turvallisuusvyöhykkeiden periaatteita.

Rakenteellisten turvallisuusjärjestelmien tarkoituksena on Leppäsen (2006, 342) mukaan hallita tontin ja kiinteistön alueella olevia riskejä erilaisten rakenteellisten ja teknisten toteutuksien avulla. Turvallisuusjärjestelyillä ohjataan ja hallitaan ihmisten, tavaroiden ja informaation liikkeitä hallinnoitavalla alueella. Kerkon (2001, 277) mukaan organisaation johdon

tulisi määritellä rakenteelliset ja toiminnalliset tasovaatimukset ja että kiinteistö- ja toimitilaturvallisuus otetaan mukaan turvallisuusjohtamiseen. Rakenteelliset turvallisuusmääräykset täyttyvät, kun noudatetaan yleisiä turvallisuusmääräyksiä (Kerko 2001, 277). Rakenteellisia turvallisuusmääräyksiä säätelee erityisesti Ympäristöministeriön asetus rakennusten paloturvallisuudesta (A3/2011).

Kiinteistöturvallisuuden hallitsemiseksi koko kiinteistön tontti ja rakennukset sekä kulkureitit tulee jakaa osiin, joista jokainen sisältää omat rakenteelliset ja toiminnalliset turvallisuusvaatimuksensa. Suojaustasoilla saadaan eroteltua ja pienennettyä organisaation suojeltaviin arvoihin kohdistuvaa riskiä. Esimerkkinä Leppänen (2006, 343-346) esittelee suojaustaso -mallin yhdestä neljään, jolloin ensimmäinen taso on perustaso ja kaikille avointa tilaa, johon ei kohdistu erityisiä riskejä ja nelostaso on vastaavasti täyden suojauksen tila, jossa olevat ja liikkuvat ihmiset, omaisuus ja informaatio ovat täysin valvottuja ja joissa teknisillä järjestelmillä suoritetaan aktiivista valvontaa koko ajan. (Leppänen 2006, 343-346.)

3.8 Pelastusturvallisuus

Pelastusturvallisuudella tarkoitetaan EK:n (2017) mukaan tulipalojen ja muiden onnettomuuksien ehkäisyä sekä nopeaa ja oikeanlaista vastetta onnettomuustilanteessa. Pelastusturvallisuudessa korostuu turvallisuusohjeiston laatiminen ja henkilöstön säännöllinen koulutus onnettomuuksien varalta. Toiminta perustuu onnettomuusriskien hallintaan; ennakointiin, poistamiseen ja pienentämiseen sekä vakuuttamiseen. Pelastuslainsäädäntö säätelee huomattavan paljon pelastusturvallisuutta ja pelastussuunnitelma toimiikin ohjaavana dokumenttina pelastusturvallisuudessa. Paloturvallisuuden tekijät sisältyvät tässä yhteydessä pelastusturvallisuuteen. (EK 2017.)

Valtioneuvoston asetus pelastustoimesta (A407/2011) säätää, että oppilaitoksiin tulee tehdä pelastussuunnitelma, joka sisältää Pelastuslain (L379/2011) mukaisen selostuksen vaarojen ja riskien arvioinnin johtopäätöksistä, rakennuksen ja toiminnassa käytettävien tilojen turvallisuusjärjestelyistä, asukkaille ja muille annettavista ohjeista onnettomuuksien ehkäisemiseksi sekä onnettomuus- ja vaaratilanteessa toimimiseksi. Pelastuslain (L379/2011) 14 § omatoimisesta varautumisesta säätää, että rakennuksen omistajan ja haltijan tulee omalta osin ehkäistä vaaratilanteiden syntymistä, varauduttava henkilöiden, ympäristön ja omaisuuden suojaamiseen vaaratilanteissa, varauduttava sellaisiin pelastustoimenpiteisiin, joihin ne itse kykenevät sekä ryhdyttävä toimenpiteisiin poistumisen turvaamiseksi vaaratilanteissa.

Leppänen (2006, 256) painottaa, että rakennuksen omistaja tai haltija on aina vastuussa pelastusturvallisuudesta, jota valvovat organisaation sisäisten tarkastajien lisäksi ulkopuoliset toimijat, alueen pelastuslaitoksen palotarkastajat ja vakuutusyhtiön edustajat. Leppäsen

(2006, 251) mukaan kannattaisi hyödyntää palotarkastajien osaamista, koska palotarkastuksen lisäksi tarkastaja kykenee antamaan asiantuntevia neuvoja paloturvallisuudesta. Mikäli tarkastuksessa ilmenee puutteita, voi palotarkastaja antaa korjausmääräyksiä tai jopa keskeyttää toiminnan, kunnes turvallisuutta vaarantavat tekijät on korjattu (Leppänen 2006, 251). Vakuutusyhtiön suorittama palotarkastus perustuu vakuutusehtoihin, joissa tuodaan esiin vakuutusyhtiön oikeus tarkastaa vakuutettu kohde siltä osin, että sen toiminta, laitteet ja rakenteet ovat vakuutusehtojen mukaisia (A-vakuutus 2017).

3.9 Tuotannon, toiminnan ja ympäristön turvallisuus

Turvallisten tuotteiden ja palveluiden varmistaminen on tuotannon ja toiminnan turvallisuuden perusta (EK 2017). Leppäsen (2006, 318-319) ja EK:n (2017) mukaan tuotannon ja toiminnan turvallisuus sisältää tuotevastuun ja -turvallisuuden, palvelujen turvallisuuden, logistiikkaturvallisuuden, maksuliikenteen turvallisuuden, arvo-omaisuuden säilytyksen, alihankkijoiden ja sopimuksien hallinnasta sekä vakuuttamisesta. Leppänen (2006, 319) nostaa myös esille, että tuotannon ja toiminnan turvallisuus on myös jatkuvuussuunnittelua ja liiketoimintariskien hallinta, koska sen tarkoitus on organisaation toiminnan häiriöttömyys.

Ympäristöturvallisuuden tavoitteena on EK:n (2017) mukaan ekologisen kestävyyden huomioiminen, asiakkaiden ja yhteiskunnan ympäristöodotuksiin vastaaminen ja ennakointi. Ympäristöturvallisuus tarkoittaa ympäristövastuun ottamista, jatkuvaa prosessien ja parhaiden käytäntöjen kehittämistä, henkilöstön tietoisuuden lisäämistä, avointa viestintää ja sitoutumista standardien periaatteisiin. Ympäristöturvallisuus koostuu esimerkiksi kestävän kehityksen periaatteesta, energiatehokkuudesta, ympäristövaikutusten arvioinnista, ilmoitus- ja lupamenettelyistä, vaarallisten aineiden käsittelystä, ympäristön suojelun hallintajärjestelmästä, ilmastonsuojelusta, kemikaalivalvonnasta, jätehuollosta ja meluntorjunnasta. (EK 2017.)

Koskenranta (2012, 8, 20-21) suosittelee SFS-EN ISO 14001 -standardia ympäristöjärjestelmien vaatimuksista korkeakoulujen turvallisuustoiminnan kehittämistyöhön soveltuvana. Standardi tarjoaa tehokkaan ympäristönhallintajärjestelmän rakenneosat, jotka voidaan yhdistää muiden standardien ja johtamisjärjestelmien kanssa. SFS-EN ISO 14001 -standardi ei määrittele kaikille organisaatioille yhdenmukaista rakennetta, vaan organisaation on luotava, dokumentoitava ja toteutettava itselleen laadunhallintajärjestelmä. SFS-EN ISO 14001 -standardi soveltuu kaikille organisaatioille ja se sisältää esimerkiksi ympäristöpolitiikan, vaatimustenmukaisuuden huomioonottamisen varmistamisen, roolien ja vastuiden määrittelyn sekä standardin edellyttämien dokumenttien hallinnan. (Koskenranta 2012, 20-22.)

3.10 Väärinkäytösten, poikkeamien ja kriisinhallinta sekä varautuminen

Väärinkäytösten ja poikkeamien hallinnan avulla ennaltaehkäistään ja selvitetään EK:n (2017) mukaan rikoksia, väärinkäytöksiä ja muita toimintaan vaikuttavia poikkeamia. Organisaatio suojelee toimintaansa, henkilöstöänsä ja omaisuuttansa sisä- tai ulkopuolisia toimijoita vastaan. Erilaisia rikosriskejä hallitaan vakuuttamisella ja väärinkäytöksiä esimerkiksi viranomaisyhteistyöllä ja ennaltaehkäisevillä toimenpiteillä, kuten teknisillä ratkaisuilla. EK (2017) painottaa haitallisten tapahtumien havainnointia, analysointia ja ennalta estämistä osana haitallisten tapahtumien torjuntaa. Säännölliset tarkastukset ja selvitykset ennaltaehkäisevät väärinkäytöksiä. (EK 2017.)

Varautumisessa ja kriisinhallinnassa on EK:n (2017) mukaan kyse toiminnan jatkuvuuden turvaamisesta kaikissa tilanteissa, jolloin on tärkeää säilyttää toimintakyky ja pyrkiä toipumaan mahdollisimman nopeasti häiriötilanteista. Organisaatio pyrkii tunnistamaan ja ennakoimaan odottamattomia tilanteita sekä suojautumaan niiltä mahdollisimman tehokkaasti. Varautumis- tai valmiussuunnitelman lisäksi tulee jatkuvuussuunnittelun avulla arvioida liiketoimintariskejä ja keskittyä toiminnan keskeytymisiin ja pysähtymisiin. Kriisinhallinta kattaa ennaltaehkäisyn, toiminnan kriisitilanteessa, toipumisen tilanteesta ja oppimisen, jatkuvan parantamisen periaatteiden mukaisesti. (EK 2017.)

4 Turvallisuusjohtamisjärjestelmä

Reason (1997, 194-195) ja Martikainen (2016, 45) ovat todenneet, että turvallisuuskulttuuri on osa organisaatiokulttuuria. Scheinin (2004, 10-11) mukaan organisaatiokulttuuri koostuu johtamisesta ja kulttuurista, joka on tulosta monimutkaisesta ryhmän oppimisprosessista. Kulttuuria on jokaisella sosiaalisella ryhmällä, joka jakaa yhteistä historiaa. Johtajat vastaavasti luovat ja hallitsevat kulttuuria, ja voidaankin nähdä, että johtajien ainoa merkitys on ymmärtää ja toimia kulttuurin mukaisesti, erityisesti kun kulttuuri nähdään tehottomana. Schein (2004, 25-26) kuvaa organisaatiokulttuurin kolmitasoisena mallina, jonka pohjalla ovat artefaktit; näkyvät rakenteet ja toiminnalliset ilmiöt. Toisen tason muodostavat normit ja arvot ja kolmannen tason pohjimmaiset perusolettamukset. (Schein 2004, 10-11, 26.)

Turvallisuuskulttuuri muodostuu Leppäsen (2006, 49) ja Paasosen (2012, 17) mukaan turvallisuutta koskevista asenteista, arvoista ja turvallisuustoimenpiteistä. EK (2017) painottaa hyvän turvallisuuskulttuurin luomista hyvin tärkeänä osana turvallisuuden kehittämisessä. Säteilyturvakeskuksen (2017) mukaan hyvä turvallisuuskulttuuri edellyttää työntekijöiden ja johdon sitoutumista sekä jatkuvaa ylläpitoa. Reasonin (1997, 195-196) mukaan hyvä turvallisuuskulttuuri pitää sisällään myös jatkuvan parantamisen periaatteet, joustavan kulttuurin ja johta-

jat, tehokkaan poikkeamailmoitusjärjestelmän sekä oikeudenmukaisen ja luotettavan ilmapiirin, joka palkitsee turvallisuusilmoituksista. Flink ym. (2007, 244-245) ovat todenneet Reimaniin & Oedewaldiin (2008, 124-125) viitaten, että hyvän turvallisuuskulttuurin tekijöitä ovat muun muassa turvallisuuspolitiikka, vastuiden ja velvollisuuksien määrittely, turvallisuuden mittaaminen ja arviointi sekä hyvä kommunikointi. Booth & Lee (1995, 395) ovat todenneet, että turvallisuuskulttuurin tekijät sisältyvät myös turvallisuusjohtamisjärjestelmään.

Turvallisuusjohtamisjärjestelmän tarkoituksena on tunnistaa, arvioida ja hallita organisaation toimintaan sisältyviä vaaroja (Reiman & Oedewald 2008, 64, Hopkinsin 2000, 86 mukaan). Reiman & Oedewald (2008, 64) ovat todenneet Levään (2003, 38) viitaten, että järjestelmän keskeisin tavoite on varmistaa, että suojaukset onnettomuuksien ehkäisemiseksi ovat olemassa organisaatiossa ja että ne toimivat. Lähtökohtana ovat organisaation toiminnalliset riskit ja näiden riskien arviointi; vaarojen järjestelmällinen tunnistaminen ja todennäköisyyden sekä seurausten arviointi (Reiman & Oedewald 2008, 64).

Turvallisuusjohtamisjärjestelmän taustat tulevat työterveys- ja työturvallisuusjärjestelmistä. Suomen standardisoimisliitto toteaa standardissaan OHSAS 18001, että työterveyttä ja työturvallisuutta tulee suunnitella, toteuttaa ja ohjata organisaatioon integroidun johtamisjärjestelmän puitteissa. Työterveyden- ja työturvallisuuden johtamisjärjestelmän on tarkoitus auttaa organisaatiota kehittämään ja toteuttamaan sellaista politiikkaa ja tavoitteita, joissa otetaan huomioon lakisääteiset vaatimukset ja tiedot työterveyden ja työturvallisuuden riskeistä. (OHSAS 18001.) OHSAS 18001 –standardissa on otettu huomioon SFS-EN 9001- , SFS-EN ISO 14001- ja BS 8800-standardi, jota Levä (2003, 69) kritisoi OHSAS 18001 –standardin lisäksi siitä, että ne eivät ota huomioon suuronnettomuus-, omaisuus-, tai ympäristöriskejä riittävästi. Turvallisuusjohtamisjärjestelmän standardisoinnin painopiste on vain työturvallisuudessa ja työterveydessä Reimanin & Oedewaldin (2008, 64) mukaan.

Turvallisuusjohtamisjärjestelmä voi Boothin & Leen (1995, 395) mukaan kiteyttää neljään toimintoon, joista ensimmäinen on turvallisuuspolitiikka ja suunnittelu, joihin sisältyvät turvallisuustavoitteiden asettaminen, tavoitteiden priorisointi ja turvallisuusohjelmien kehittäminen. Muita toimintoja ovat turvallisuuden organisointi ja viestintä, joihin sisältyvät vastuiden määrittely ja kommunikointikanavien luominen, riskien hallinta, johon sisältyy riskien arviointi ja riskien käsittely sekä toiminnan tarkastelu ja arviointi -kokonaisuus (Booth & Lee 1995, 395). Reimanin ja Oedewaldin (2008, 65) mukaan tähän tulisi lisätä ainakin yleisessä johtamisjärjestelmässä käsiteltäviä asioita, kuten organisaatiorakenne ja vastuualueet sekä toimintatavat ja resurssit. Kerkon (2001, 38-39) mukaan turvallisuusjohtamisjärjestelmässä tulisi huomioida edellisten elementtien lisäksi mittaaminen, koulutus ja katselmointi, jolla tarkoitetaan kaikkea selvitys-, valvonta- ja tarkastustoimintaa, joka on tarpeen päätöksenteossa ja liiketoimin-

nan varmistamisessa. Levä (2003, 37) esittää lisäksi Kirwaniin (1996, 67-92) vedoten turvallisuuden resurssit yhdeksi turvallisuusjohtamisjärjestelmän elementiksi, joka tulee olla mitattavissa budjettivaroina, henkilöstötyövoimana tai molempina. Turvallisuuteen kohdistetut resurssit kuvaavat Levän mukaan (2003, 37) johdon sitoutumista. Myös Paasonen (2012, 89) toteaa, että turvallisuusjohtamisen strategiaprosessissa tulee huomioida resurssit.

Kerkon (2001, 47) mukaan turvallisuusvisioissa, tai turvallisuuspäämäärissä, organisaatio ilmoittaa, mihin se pyrkii ja millainen se haluaa olla 3-5 vuoden päästä. Turvallisuuden päämäärissä ei mietitä, miten tavoitteeseen käytännössä päästään, mutta niiden on silti oltava selkeitä, konkreettisia ja tavoitteellisia. Päätös turvallisuusjohtamisjärjestelmän suunnittelemisesta on hyvä esimerkki turvallisuusvisiosta Kerkon (2001, 47) mukaan. Vastaavasti turvallisuustavoitteet ovat konkreettisempia ja lyhytaikaisempia kuin päämäärät (Kerko 2001, 48). Tavoitteita asetetaan koko organisaatiolle, mutta myös yksittäisille osastoille. Leppänen (2006, 175) korostaa, että turvallisuustoiminnan ja riskienhallinnan tavoitteiden tulee olla integroitu organisaation tavoitteisiin ja strategiaan. Pelkästään päämäärät ja tavoitteet eivät riitä toimintaohjelmien suunnittelemiseksi, vaan tarvitaan myös konkreettinen strategiasuunnitelma, jota ei voida menestyksellisesti toteuttaa tuntematta organisaation strategiaa (Kerko 2001, 47-48). Turvallisuusstrategia tuleekin EK:n (2017) mukaan integroida organisaation strategiaan.

Organisaation johdon työskentelyn on perustuttava, niin turvallisuusasioissa kuin liiketoiminnassakin, valittuihin ja päätettyihin periaatteisiin ja politiikkoihin. Johtoa koskettaa erityisesti tavoitteiden asettaminen, katselmointi tai järjestelmien luominen ja kehittäminen. Johdon tulee suunnata sekä omat että organisaation turvallisuusresurssit sovittujen suunnitelmien ja periaatteiden mukaisesti. Turvallisuuspolitiikka on Leppäsen (2006, 177) mukaan lausuma, jossa on tiivistettynä ne arvot, jotka ohjaavat organisaation turvallisuuskulttuuria. Turvallisuuspolitiikan tarkoituksena on myös määritellä, mitä organisaation turvallisuustoiminta sisältää. (Kerko 2001, 44.)

Turvallisuusjohtamisjärjestelmän toinen toiminto on Boothin & Leen (1995, 395) mukaan turvallisuuden organisointi ja viestintä, joihin sisältyy vastuiden määrittely ja kommunikointikanavien luominen. Kerkon (2001, 48) mukaan turvallisuustoiminta on johdon vastuulla ja se sisältää turvallisuuteen liittyvän strategisen työskentelyn organisoinnin, käytännön turvallisuustoimintojen organisoinnin, organisaation riskienarviointitoiminnan yleisen organisoinnin sekä vastuiden ja velvoitteiden määrittelyn. Strategisen työskentelyn organisointi painottuu kokonaisvaltaisessa turvallisuusjohtamisessa Kerkon (2001, 48) mukaan johtoryhmätyöskentelyyn, jossa tulisi muiden liiketoiminnallisten asioiden lisäksi käsitellä säännöllisesti ja systemaattisesti turvallisuusasiat lähes jokaisessa palaverissa.

Turvallisuusvastuiden organisointi on Levän (2003, 16) mukaan ollut turvallisuusjohtamisjärjestelmien kehittämisessä painopisteenä. Reimanin ja Oedewaldin (2008, 71) mukaan turvallisuuden organisointi on usein keskitetty erilliseen turvallisuusosastoon, joka poikkeaa linjaorganisaatiosta, kuten muutkin tukevat, valvovat ja avustavat toiminnot, esimerkkeinä tekninen tuki tai laadunvalvonta. Tällaisen turvallisuusosaston tehtävänä on tyypillisesti tarjota konsultaatiota operatiivisille yksiköille turvallisuuteen liittyvissä asioissa, ohjata riskien arviointia, tehdä sisäisiä tarkastuksia, kerätä ja analysoida tietoa onnettomuuksista, tapaturmista, läheltä-piti-tilanteista ja muista poikkeamista, huolehtia turvallisuusohjeiden päivityksistä sekä huolehtia viranomaisten kanssa tapahtuvasta viestinnästä ja viranomaisvaatimuksista. Reiman & Oedewald (2008, 73) muistuttavat kuitenkin, että turvallisuusosaston asiantuntijat eivät vastaa juridisesta vastuusta, joka on kuitenkin aina ylimmällä johdolla. (Reiman & Oedewald 2008, 71-73.)

Kerko (2001, 49) näkee, että turvallisuusasiat kuuluvat pääosin linjaorganisaatiolle, eikä turvallisuusorganisaatiolle tai muulle asiantuntijahenkilöstölle. Linjaorganisaatio vastaa toiminnan virheettömyydestä, jatkuvasta parantamisesta, sen edellytysten luomisesta, kuten opastuksesta, ohjeista, riskien arvioinnista ja poikkeamavalvonnasta. Kerko toteaa (2001, 50) kuitenkin, että turvallisuusorganisaatio voi hajauttaa vastuutaan työntekijöille, heidän osaamisensa mukaan. Hyvänä esimerkkinä tietoturvallisuus, jonka ohjeistuksia jokaisen työntekijän on tärkeä noudattaa, mutta asiaan perehtyminen ja osastokohtaiset ohjeet sekä henkilöstön kouluttaminen vaativat erityisvastuuhenkilön. Tällaisella henkilöllä tulee olla käytössään tarpeeksi pohjatietoa, mutta myös johdon myöntämiä valtuuksia. Tärkeintä on kuitenkin, että johto määrittelee turvallisuuden vastuut selkeästi ja yksiselitteisesti sekä linjaorganisaatiolle että turvallisuusorganisaatiolle. Kerko (2001, 49) näkee Reimanin & Oedewaldin (2008, 73) tavoin turvallisuusorganisaation vastuina lakisääteiset vaatimukset, konsultaatiotoiminnan ja asiantuntemuksen. (Kerko 2001, 49-50; Reiman & Oedewald 2008, 73.)

Viestintä on osa turvallisuusjohtamisjärjestelmää (Real & Cooper 2009, 24; Booth & Lee 1995, 395). Real & Cooper (2009) ovat todenneet, että turvallisuusviestintä on väline, jolla voidaan välittää organisaation turvallisuusnormeja ja näkemyksiä henkilöstölle sekä kannustaa positiiviseen turvallisuusilmapiiriin. Koskenranta ym. (2012, 70) suosittelevat korkeakouluille turvallisuusviestinnän tavoitteiden määrittelyä osana muuta viestintää, jolloin turvallisuusviestinnän sisältö noudattaisi turvallisuusjohtamisen osa-alueita. Turvallisuusviestinnän toteutus olisi Koskenrannan ym. (2012, 70) mukaan monikanavaista johdon tukemaa ja eri käyttäjäryhmät huomioivaa toimintaa, jossa korostuu kaksisuuntaisuus ja opiskelijoiden mukaan ottaminen esimerkiksi turvallisuuspoikkeamailmoitusmenettelyjen kautta.

Levä (2003, 56) on todennut SFS-EN 9001-, OHSAS 18001- ja BS 8800 -standardiin vedoten, että organisaation johto tarvitsee tietoa, jotta se voi arvioida tavoitteiden ja päämäärien saavuttamista sekä toteutettujen toimenpiteiden onnistumista. Turvallisuuden mittaamisella ja seurannalla tarkoitetaan niitä tietoja ja menetelmiä, joiden perusteella arvioidaan tavoitteiden saavuttamista, organisaation turvallisuustasoa ja siinä tapahtuneita muutoksia (OHSAS 18001; BS 8800). Kerkon (2001, 52), Levän (2003, 57) ja Reimanin & Oedewaldin (2008, 68-69) mukaan turvallisuutta mitataan reagoivasti, puuttumisen kautta, erilaisilla tapaturma ja onnettomuustilastoilla sekä proaktiivisesti, ennakoivien mittareiden, avulla. Ennakoivat ja ohjaavat mittarit pyrkivät Reimanin ja Oedewaldin (2008, 69) mukaan mittaamaan erityisesti sitä, miten organisaatio tunnistaa toiminnalliset riskinsä ja hallitsee niitä.

Organisaation tunnusluvut saadaan Kerkon (2001, 53) mukaan erilaisista mittareista, ja turvallisuuden raportit koostuvat suurimmaksi osaksi tunnusluvuista. Mittaaminen mahdollistaa siis turvallisuuden eri osa-alueiden seurannan ja onkin tärkeää, että johto saa 1-2 kertaa vuodessa riittävän monipuolisen raportin turvallisuuden eri osa-alueiden tunnusluvuista. Raportointijärjestelmä perustuukin myös turvallisuuden mittaamiseen, jonka tarpeen johdon tulisi tunnistaa. (Kerko 2001, 53.)

Kerkon (2001, 53) mukaan poikkeamavalvonta on tärkeä osa-alue mittaamisessa. Reimanin ja Oedewaldin (2008, 370) mukaan tapahtumien ja vaaratilanteiden raportoinnilla pyritään ensisijaisesti siihen, että tilanteista opittaisiin ja vastaavat ongelmat eivät toistuisi. Vaaratilanteiden ja tapaturmien raportointi on taas Laitisen ym. (2013, 228) mukaan työturvallisuuden perustoimintoja. Vakuutusyhtiö vaatii ilmoituksen henkilövahinkoihin ja työstä poissaoloon johtaneista tapaturmista, minkä takia organisaation tulee ne myös tutkia. Myös pienemmät tapaturmat tulisi silti tutkia, koska silloin saadaan tietoa vaaratekijöistä, jotka voidaan poistaa. Suurin hyöty saadaan, kun kaikki onnettomuus ja läheltä-piti-tilanteet saadaan mukaan raportointijärjestelmään. (Laitinen ym. 2013, 228.)

Reasonin (1997, 195) mukaan onnettomuuksista ja läheltä-piti-tilanteista ilmoittava raportointikulttuuri on välttämätöntä organisaation turvallisuusjärjestelmälle. Reimanin ja Oedewaldin (2008, 370) mukaan läheltä-piti-tilanteella tarkoitetaan tilannetta, joka ei ole johtanut vahinkoon, mutta olisi voinut johtaa. Laitisen ym. (2013, 228) mukaan vaaratilanteiden suuri määrä suhteessa henkilöstöön ilmentää hyvää turvallisuuskulttuuria, koska tilanteiden ilmoittaminen on osoitus siitä, että ilmoittaja on sisäistänyt turvallisuusjohtamisen tavoitteet tarkkaillen työympäristöään. Laitinen ym. (2013, 228) näkevätkin, että vaaratilanneraportoinnin aktiivisuutta voidaan pitää keskeisenä oppivan organisaation turvallisuusmittareista, koska ilmoittaminen ilmentää myös luottamusta ja avointa tiedonkulkua. (Kerko 2001, 53.)

Turvallisuusjohtamisjärjestelmä vaatii dokumentointia Kerkon (2001, 85) mukaan. Dokumentoinnilla kuvataan järjestelmän rakenne ja sisältö, johon sisältyy järjestelmän vastuut, turvallisuusjohtamisen osa-alueiden organisointi ja vaatimukset sekä koko organisaatiota koskettavat turvallisuusohjeet. Dokumenteilla voidaan myös todentaa järjestelmän toimivuus hyödyntäen raportteja, viranomaisselvityksiä, mittareita, riskien arviointeja, pelastussuunnitelmaa, koulutustietoja ja rekistereitä sekä turvallisuussuunnitelmaa. Toimivassa dokumentoinnissa turvallisuusjohtamisjärjestelmä sisältää esimerkiksi kaikki viranomaisten tarvitsemat dokumentit. Dokumentointi tulisi integroida SFS-EN 9001 -laadunhallintajärjestelmään, mikäli sellainen on käytössä. (Kerko 2001, 85-86.)

Turvallisuustoiminnassa on erittäin tärkeää kouluttaminen ja perehdyttäminen, jotka tulisi integroida yleiseen koulutukseen Kerkon (2001, 51) mukaan. Myös Työturvallisuuslaki (738/2002) edellyttää, että työntekijälle pitää antaa tarpeellinen perehdytys turvallisista työmenetelmistä. Eri työtehtävät vaativat erillisen, työtehtävään räätälöidyn, turvallisuuskoulutuksen, jota ei anneta kaikille työntekijöille (Kerko 2001, 51). Turvallisuuskoulutuksen tulisi Koskenrannan ym. (2012, 70) mukaan olla myös riskiperusteista.

Koskenrannan ym. (2012, 70) mukaan korkeakoulun turvallisuusjohtamisjärjestelmän kehittämisessä tulisi nykytilan arvioinnin jälkeen järjestää turvallisuuskoulutusta kaikille organisaatiotasoille. Reiman & Oedewald (2008, 77) toteavat, että koulutusta on monenlaista; ammattiosaamista päivittävää, turvallisuustietoisuutta korostavia seminaareja, uusien organisatoristen toimintatapojen harjoittelua ja tietoa tapahtumista omalla työpaikalla ja muualla. Henkilöstöhallinnon näkökulmasta Ortmeier (2005, 138) esittää, että työntekijä tarvitsee sekä harjoittelua että koulutusta, jotta työn tuottavuus pysyy korkealla ja laadukkaana. Harjoittelu tarjoaa enemmän yleistä tietoa, kun taas harjoittelu vastaavasti tähtää parempaan tiettyjen työtehtävien suorittamiseen (Ortmeier 2005, 138).

Turvallisuuden kehittämisessä EK (2017) nostaa esille laadukkaan turvallisuusohjeiston laatimisen. Koulutuksen lisäksi työn tekemistä säädellään Reimanin & Oedewaldin (2008, 77-78) mukaan ohjeiston avulla, jonka keskeisin tehtävä on tukea työntekijän työsuoritusta ja siten varmistaa työn laatu. Tällainen turvallisuuskäsitys perustuu Reimanin & Oedewaldin (2008, 79) mukaan siihen olettamaan, että ihminen on päätöksiä ja prosesseja hallitseva toimija, jonka toiminnan edistämiseksi on luotu ohjeita.

5 Oppilaitosten turvallisuus

Oppilaitosten toimintaympäristö on Paasosen (2012, 11) mukaan muuttunut, ja ammattikorkeakouluissa on käynnissä rakenteellinen uudistus, jonka tavoitteena on vahvistaa toiminnan laatua, vaikuttavuutta ja kansainvälistä kilpailukykyä (Opetus- ja kulttuuriministeriö 2017).

Uudistusten takia oppilaitokset joutuvat kehittämään ja muuttamaan toimintaansa, suuntaamaan tulevaisuuteen sekä vastaamaan yhä tiukempiin vaatimuksiin. Oppilaitosjohtamisen muutos on tuonut esille turvallisuuskysymykset yhä voimakkaammin, ja useat oppilaitokset ovatkin käynnistäneet omia toimenpideohjelmiaan turvallisuuden kehittämiseksi. (Paasonen 2012, 26.)

Ammattikorkeakoulujen turvallisuus muodostuu monista eri tekijöistä, joista Paasosen (2012, 31) mukaan eduskunta vaikuttaa eniten niihin, koska se säätää lait ja päättää rahoituksesta sekä koulutuspolitiikan linjoista. Opetus- ja kulttuuriministeriö määrittää taas koulutuspolitiikan suuntaviivat ja strategiset linjaukset sekä valvoo valtion budjettiin sidottua koulutustarjontaa. Perustan oppilaitosten turvallisuudelle luo erityissääntelyn velvoitteet koulutuksen järjestämisestä. (Paasonen 2012, 31-32.)

Suomalaisten oppilaitosten turvallisuusjohtaminen on Martikaisen (2016, 6) ja Paasosen (2012, 26) mukaan sirpalemaista eikä kokonaisvaltaista. Paasonen (2012, 26-27) nostaa useita ongelmia, joita ovat muun muassa se, että konkreettisia toimenpiteitä ei ole toteutettu, johtamiseen liittyy puutteita ja oppilaitosten henkilöstön tieto turvallisuusasioista on puutteellista. Paasonen (2012, 29-30) nostaa esille myös ongelmalliset tavoitteet ja päämäärät, sillä turvallisuusinvestointeja on tehty vain sidosryhmien vaatimuksien takia, eikä sillä tavoitteella, että oppilaitos olisi turvallinen paikka työskentelyyn ja opiskeluun. Martikainen (2016b, 15) toteaakin, että oppilaitoksen turvallisuusjohtamisen tulisi olla riskiperusteista.

Ammattikorkeakoululain (932/2014) mukaan jokaisella opiskelijalla on oikeus turvalliseen opiskeluympäristöön. Vastaavasti Työturvallisuuslain (738/2002) mukaan työnantaja on velvollinen huolehtimaan työntekijänsä turvallisuudesta. Suomen perustuslaki (731/1999) mainitsee, että jokaisella on oikeus turvallisuuteen. Martikaisen (2016a, 159) mukaan lainsäädäntö ei kuitenkaan velvoita riskiperusteiseen, kokonaisvaltaiseen turvallisuusjohtamiseen, ja turvallisuutta on kehitettykin oppilaitoksissa, mutta sirpalemaisesti. Martikaisen (2016a, 160) tutkimustulokset viittaavat siihen, että vaikka korkeakoulujen turvallisuusjohtaminen on paljon peruskouluja kehittyneempää, valtaosa suomalaisista korkeakouluista ei todennäköisesti silti yllä kokonaisvaltaisen turvallisuusjohtamisen perustasoon.

Koskenranta ym. (2012, 69-70) ovat antaneet kansainvälisessä selvityksessään suosituksia suomalaisille korkeakouluille turvallisuusjohtamisen kehittämiseksi. Suosituksissa todetaan, että korkeakoulut tarvitsisivat selkeän riskienhallintamallin, jotta sidosryhmien vaatimuksia pystyttäisiin käsittelemään kokonaisvaltaisesti eikä asia kerrallaan, tehottomasti. Suositellun riskienhallintamallin tulisi myös perustua kansainvälisiin standardeihin. Riskienhallinnan tulisi

selvityksen mukaan olla läpinäkyvää, jolloin korkeakouluja ohjattaisiin julkaisemaan merkittävimmät riskinsä ja hallintajärjestelmänsä kuvauksen pääpiirteissään. (Koskenranta ym. 2012, 69-70.)

Turvallisuusjohtamisessa voisi Koskenrannan ym. (2012, 69) mukaan hyödyntää EK:n turvallisuusjohtamisen mallia, joka on todettu toimivaksi. Mallin (EK 2017) osa-alueilla tulisi hyödyntää kansainvälisiä turvallisuusjohtamisen standardeja. Systemaattinen turvallisuusjohtamisen kehittäminen olisi suositeltavaa aloittaa turvallisuustoiminnan arvioinnilla, esimerkiksi Tutor -arviointimenettelyllä. Koskenrannan ym. (2012, 69) mukaan nykytilan arvioinnin ja tavoitteiden asettamisen jälkeen tulisi aloittaa turvallisuusjohtamisjärjestelmän kehittäminen organisaation valitsemalla kansainvälisellä turvallisuusjohtamisstandardin viitekehyksellä. Tutkimuksien mukaan turvallisuuskulttuurin tavoitteellinen kehittäminen kestää 5-10 vuotta. (Koskenranta ym. 2012, 69-70.)

6 Turvallisuusjohtaminen Arcada-ammattikorkeakoulussa

Tämän opinnäytetyön toimeksiantajana on Ammattikorkeakoulu Arcada, joka on vuonna 1996 perustettu ammattikorkeakoulu, jonka toiminta siirtyi Helsingin Arabianrantaan vuonna 2004. Arcadassa on 190 työntekijää ja noin 2500 opiskelijaa ja se tarjoaa ruotsin- sekä englanninkielisiä alempia ja ylempiä ammattikorkeakoulututkintoja mm. insinööri-, tradenomi-, sairaanhoidon-, media-alan ja fysioterapian koulutusohjelmissa. Arcadan opiskelijoista noin 10 % on vaihto-opiskelijoita ja he tulevat yli 40 eri maasta. Tutkinto-ohjelmien lisäksi Arcada tarjoaa erikoiskoulutusta ja suomenkielistä ensi- ja sairaanhoidon kurssikoulutusta (Sjöberg 2017). Arcadassa tehdään myös tutkimus- ja innovaatiotoimintaa esimerkiksi teknisillä aloilla. Ammattikorkeakoulun omistaa Stiftelsen Arcada –säätiö. (Arcada 2016.)

Arcada soveltaa EK:n (2017) turvallisuusjohtamismallia, josta johdetaan turvallisuuden eri osa-alueet. Riskienhallinta ohjaa kaikkea turvallisuusjohtamista. Mallia sovelletaan turvallisuusjohtamisjärjestelmän luomisessa, mutta myös päivittäisen turvallisuuden suunnittelussa, toteutuksessa ja kehittämisessä. Mallin yksi tärkeimmistä osa-alueista on henkilöstöturvallisuus, joka perustuu ennen kaikkea kampuksen 2500 opiskelijaan, joilla on oikeus turvalliseen opiskeluun. Vastaavasti kampuksen suuri käyttäjämäärä luo tarpeen pelastusturvallisuuden erinomaiseen toimivuuteen, jotta hätätilanteessa pystytään evakuoimaan tai suojaamaan käyttäjät sisälle tehokkaasti, henkilövahingot estäen. Työturvallisuus on hyvin tärkeää, koska yksi ammattikorkeakoulun suurimmista voimavaroista on sen työntekijät, jotka mahdollistavat laadukkaan opetuksen jatkuvuuden Arcadassa. Samalla periaatteella tietoturvallisuus mahdollistaa myös henkilöstön työnteon tarjoten sähköiset opetusmateriaalit ja fyysisten tilojen käyttämisen. Arcada soveltaa kuitenkin kaikkia osa-alueita kokonaisvaltaisen turvallisuusjohtamisen periaatteiden mukaisesti. (Arcada 2017.)

Arcada organisoi turvallisuuden vastuitaan mallin avulla siten, että suurin osa vastuusta on operatiivisella linjaorganisaatiolla ja osa turvallisuusyksiköllä tai muulla hallinnolla, kuten henkilöstöhallinnolla. Ylin johto kantaa Arcadassa lopulta vastuun turvallisuudesta, kuten kaikesta muustakin toiminnasta. Arcada on jakanut turvallisuuden vastuitaan myös erikoistilojen vastuuhenkilöille, eri siipien tilavastaaville sekä infopisteelle, joka toimii keskeisessä roolissa raportoinnissa, viestinnässä ja poikkeamavalvonnassa. Eri tilojen vastuuhenkilöt huolehtivat turvallisuudesta omilla vastuualueillaan esimiesasemassa toimivina työntekijöinä. Koulutuksen ja ohjeiston avulla vastuuta jaetaan kaikille työntekijöille, sidosryhmille ja opiskelijoille, jotka saavat räätälöidyn, riskiperusteisen, koulutuksen esimerkiksi teknisten laitteiden tai muiden normaalista poikkeavien toimintojen tai tilojen käyttämiseen. Koulutuksella pyritään myös kehittämään turvallisuuskulttuuria neuvomalla ja ohjaamalla henkilöstöä erilaisista riskeistä ja toimenpiteistä turvallisuuden kehittämiseksi. (Arcada 2017.)

Arcadan turvallisuusorganisaatio koostuu turvallisuuspolitiikan mukaisesti rehtorista, kriisitiimistä ja turvallisuustiimistä. Rehtori johtaa ja on vastuussa Arcadan turvallisuudesta ylimpänä johtona, organisaation toimitusjohtajana. Turvallisuuden operatiivista toimintaa johtaa linjaorganisaation toimialajohtajat omilla hallinnon alueillaan. Turvallisuusyksikkö poikkeaa linjaorganisaatiosta ja sen tehtävänä on antaa konsultaatiota linjaorganisaatiolle, järjestää koulutuksia, laatia ohjeistuksia sekä suunnitella riskienhallintaa ja turvallisuusjohtamista. Arcadan turvallisuuden tärkeimmät tekijät ja mahdollistajat ovat kuitenkin sen päivittäiset jäsenet; sidosryhmät, työntekijät, opiskelijat, vierailijat ja asiakkaat. Arcadan turvallisuuden kehittämisessä halutaan painottaa käyttäjien vastuuta, jotta voitaisiin vaikuttaa positiivisesti organisaation turvallisuuskulttuuriin, turvallisuustietoisuuteen ja erityisesti asenteisiin. (Arcada 2017.)

Arcadaan suoritettiin joulukuussa 2015 turvallisuusjohtamisen auditointi Tutor max -arviointimenetelmällä. Auditoinnissa turvallisuuden nykytila tunnistettiin johdon itsearvioinnissa ja kolmannen osapuolen arvioimana. Menetelmä tarkasteli organisaation turvallisuutta 23 eri kortin avulla kahdeksasta eri arviointialueesta, jotka ovat hallinnollinen johtaminen, toiminnalliset riskit, vaatimusten täyttyminen, dokumentaatio, kiinteistö- ja turvallisuustekniikka, koulutus, viestintä, tulokset ja vaikutukset. (Martikainen & Ranta 2015.)

Arviointimallin on kehittänyt Keski-Uudenmaan pelastuslaitos ja sen tavoitteena on tuottaa organisaatiolle tietoa turvallisuuden kokonaisvaltaisesta tilasta suhteessa lainsäädännön vaatimuksiin. Arviointimallissa johto arvioi organisaationsa turvallisuuden nykytason asteikolla 1-5. Auditoija arvioi samalla asteikolla, jossa arvosana 1 on puutteellinen, 3 lainsäädännön velvoittama perustaso ja arvion 5 saa, mikäli organisaatio on edelläkävijä ja malliorganisaatio kan-

sallisella tasolla, arvioitavan kortin osalta. Edelläkävijän tasolla voidaan puhua turvallisuusjohtamisjärjestelmästä, joka on kiinteä osa yleistä johtamisjärjestelmää. (Martikainen & Ranta 2015.)

Auditoinnissa organisaation johto määrittää jokaiselle arvioitavalle kortille tavoitearvon, johon organisaatio haluaa yltää esimerkiksi kolmen vuoden päästä. Auditoinnin tuloksena Arcada sai kehityskohteet ulkopuolisilta arvioitsijoilta. Nämä kehityskohteet ja auditoinnin tulokset huomioitiin Arcadan (2017) turvallisuuspolitiikkaa laadittaessa. Arcadan turvallisuustyön priorisointi perustuu Tutor- ja riskien arvioinnin tuloksiin ja niiden perusteella saatuihin kehittämisehdotuksiin. (Martikainen & Ranta 2015.)

Tutor max -auditoinnin tuloksien ja kehittämiskohteiden sekä johdon tahdon perusteella Arcadan johto teki päätöksen turvallisuuspolitiikan (liite 1) laatimisesta toukokuussa 2016. Politiikan suunnittelu perustui Arcadan strategiaan ja sen suunnitteluun osallistui turvallisuusjohdon edustajia. Työryhmä kokoontui suunnittelemaan turvallisuuspolitiikan sisältöä, joka muodostui turvallisuuden visiosta, päämäärästä, periaatteista ja tavoitteista sekä turvallisuusorganisaatiosta ja sen vastuista sekä rooleista. Turvallisuuspolitiikka hyväksyttiin rehtorin päätöksellä. Politiikka perustuu siihen, että Arcadan käyttäjiä yritetään saada aktiivisesti mukaan turvallisuustoimintaan ja perustamalla kaikki turvallisuustoiminta riskienhallintaan. Näillä toimenpiteillä pyritään kehittämään Arcadan turvallisuuskulttuuria proaktiiviseksi. (Arcada 2017.)

Arcadan riskienhallinta pyrkii SFS-ISO 31000 -standardin periaatteiden, puitteiden ja riskienhallintaprosessin mukaiseen toimintaan. Tavoitteena on erityisesti jatkuva riskien arviointi ja seuranta. Riskien arviointi kohdistuu koko organisaatioon, sidosryhmät huomioon ottaen, ja arviointia suoritetaan SFS-EN 31010 –riskien arviointimenetelmien sekä potentiaalisten ongelmien analyysin puitteissa. Arcadan riskienhallintaa kehitetään järjestelmällisesti kohti kokonaisvaltaista riskienhallintajärjestelmää. (Arcada 2017.)

Arcadan turvallisuuspolitiikan mukaisesti turvallisuusjohtaminen perustuu riskienarviointiin, minkä takia riskien arviointi -työpajan järjestämisestä tehtiin Arcadassa rehtorin päätös. Arcadan tavoite olla ennaltaehkäisevä kaikilla turvallisuuden osa-alueilla vaatii sen, että koko organisaatio on otettu mukaan arvioimaan riskejä omasta työympäristöstä ja antamaan mahdollisuus kehittää yhteisesti työpaikan oloja sekä varmistamaan turvallinen työympäristö kaikille korkeakouluyhteisön jäsenille. (Arcada 2017.)

Arcadassa tehtiin lokakuussa 2016 Potentiaalisten ongelmien analyysi -riskien arviointityöpaja, johon osallistui koko organisaation kattava edustus eri yksiköistä sekä turvallisuuden sidosryhmistä. Työpaja keskittyi vaarojen tunnistamiseen ja riskianalyysiin. Riskien arviointi

tehtiin 4-5 henkilön pöytäryhmissä ja aiheena oli opetus- ja tutkimustyön jatkuvuus Arcadassa. Tavoitteena oli löytää jokaisen osallistujan oman toiminnan näkökulmasta todellisia riskejä, jotka voisivat aiheuttaa toiminnan keskeytymisen tai pysähtymisen kaikissa olosuhteissa. Tehtävänannon lisäksi ohjeistettiin huomioimaan erityisesti arkiset asiat ja toiminnot, joista muodostuu riskejä. Tällä ohjeistuksella pyrittiin kiinnittämään huomiota jokapäiväisiin asioihin, joita ei välttämättä osata edes mieltää riskeiksi sekä haluttiin korostaa riskien tunnistamisen merkitystä. Vain tunnistettuihin riskeihin voidaan varautua ja vaikuttaa. (Arcada 2017.)

Riskien arvioinnin tavoitteena oli saavuttaa kokonaisvaltainen kuva Arcadan toimintaan kohdistuvista riskeistä, jotta turvallisuusjohtamisen kehittämisen suunta pystyttäisiin määrittelemään mahdollisimman luotettavasti ja kattavasti. Tavoitteena oli myös saada tietoa riskeistä, jotta niille voidaan asettaa korjaavia toimenpide-ehdotuksia tai arvioida riskejä tarkemmin. Lopputuloksena päätettiin useista jatkotoimenpiteistä. (Arcada 2017.)

Työpajan tuloksena saatiin kattava kuva organisaation toimintaan kohdistuvista riskeistä, joiden käsittely kohdistettiin ensisijaisesti johdon määrittelemän riskiarvon ylittäviin riskeihin. Raja-arvon ylittäviin riskeihin asetettiin välittömästi tehtävät toimenpiteet ja aikataulutetut toimenpiteet (taulukko 4), joiden tavoitteena on poistaa tai ainakin pienentää riskejä. Yleisin riskien käsittelymenetelmä oli riskin aktiivisen seurannan aloittaminen poikkeamailmoitusjärjestelmällä. (Arcada 2017.)

Käsittely	Selitys
Seuranta	Riski otetaan seurantaan: ilmoitusjärjestelmällä mitataan riskin esiintyvyyttä ja taloudellisia menetyksiä. Kerran vuodessa suoritetaan katselmus ja päätetään, jatketaanko riskin seurantaa vai tehdäänkö toimenpiteitä. Merkittävissä olosuhdemuutoksissa riskin merkitys arvioidaan uudelleen ja päätetään jatkotoimenpiteistä.
Huomiointi	Riski huomioidaan toiminnassa, mutta sille ei aseteta toimenpiteitä. Riskiä ei pystytä seuraamaan kannattavasti, ja riskin merkitys on vähäinen tai merkityksetön. Riskin tietoinen hyväksyminen.
Toimenpiteet	Riskille asetetaan välittömät toimenpiteet. Toimenpiteitä voidaan lisätä tai riski voidaan siirtää seurantaan tai huomioida, mikäli riskien arvioinnissa tai liiketoiminta-analyysissä riskin taso tarkentuu. Riskin pienentäminen, jakaminen tai poistaminen.
Toimenpiteille aikataulu	Riskin toimenpiteille asetetaan aikataulu. Toimenpiteitä voidaan lisätä tai riski voidaan siirtää seurantaan tai huomioida, mikäli liiketoiminta-analyysissä ilmenee uutta tietoa, joka vaikuttaa riskin tasoon. Riski ei vaadi välittömiä toimenpiteitä.

Käsittely	Selitys
Kyselylomake	Riskien arvioinnin jälkeen suoritetaan liiketoiminta-analyysi, jossa tunnistetaan liiketoiminnan kannalta keskeisimmät prosessit, vakavimmat seuraukset häiriötilanteessa, prosessien väliset riippuvuudet sekä nykyiset ja tarvittavat resurssit, jotka tarvitaan toimintakyvyn säilyttämiseksi ja palauttamiseksi normaalille tasolle, mikäli häiriö toteutuu. Riskin operatiivisen vastuuyksikön työntekijöitä haastatellaan, jonka jälkeen arvioiduille riskeille suoritetaan uusi käsittely ja asetetaan jatkotoimenpiteet.

Taulukko 4: Riskien käsittelytoimenpiteet (Arcada 2017)

Arcadan turvallisuusjohto päätti toteuttaa tammikuussa 2017 erikoistilojen riskien arvioinnin, jonka lisäksi päätettiin välittömänä toimenpiteenä toteuttaa liiketoiminta-analyysi, jotta saataisiin tarkempaa tietoa organisaation kriittisistä prosesseista ja eri yksiköiden sekä prosessien riippuvuussuhteista. Useita riskejä päätettiin jatkokäsitellä liiketoiminta-analyysissä. Analyysissä pyritään saamaan muiden tavoitteiden lisäksi tietoa riskin todellisesta luonteesta ja olemassa olevista hallintakeinoista. Tarve liiketoiminta-analyysille syntyikin arvioiduista riskeistä, joissa ilmeni useita organisaation sisäisiä riippuvuussuhteita sekä tunnistettiin riskien monimutkaiset syyt ja seuraukset, joiden juurisyitä tulisikin analysoida vielä tarkemmin. (Arcada 2017.)

Erikoistilojen riskien arviointi perustuu aikaisemman riskien arviointityöpajan tuloksiin, jossa todettiin useita riskejä, jotka liittyvät tavanomaisesta luokkatilasta poikkeaviin tiloihin, kuten esimerkiksi kemian laboratorioon. Tällaisessa tilassa riskit ovat lähtökohtaisesti suurempia ja niissä on myös enemmän lakisääteisiä velvoitteita työnantajalle. Erikoistilojen riskien arvioinnissa oli mukana määriteltyjen erikoistilojen vastuuhenkilöt ja työpajan ohjasi ja sihteerinä toimivat turvallisuusyksikön edustajat. Työpajan tuloksena päätettiin korjaavista toimenpiteistä, joihin sisältyi muun muassa kattavien ohjeistuksien suunnittelu ja laatiminen. (Arcada 2017.)

Liiketoiminta-analyysi toteutettiin haastattelemalla linjaorganisaation johtoa ja tukipalveluita, kuten henkilöstöhallintoa ja it-yksikköä. Turvallisuusyksikkö kävi myös viestintää eri keskijohdon edustajien kanssa riskeistä ja jatkuvuudesta. Haastatteluissa käytiin läpi systemaattisesti liiketoiminta-analyysin sisältö strukturoidulla lomakkeella (liite 2), jotta toimintaa voitaisiin luotettavasti arvioida suhteessa analyysin tavoitteisiin. (Arcada 2017.)

Liiketoiminta-analyysin johtopäätöksenä todettiin useita riippuvuussuhteita, jotka vaikuttavat toiminnan jatkuvuuteen Arcadassa. Keskeisimmät prosessit, niihin liittyvät riskit, nykyiset resurssit ja tarvittavat resurssit toiminnan jatkumisen varmistamiseksi olivat keskeisimmät analyysin tuotokset. Erilaiset riippuvuussuhteet liittyvät vahvasti henkilöstöön ja IT-palveluihin. Käytännössä ammattikorkeakoulun toiminnan jatkuvuuteen liittyy useita eri tason tekijöitä aina Opetus –ja Kulttuuriministeriön koulutuslinjauksista Eduskunnan koulutusrahoitukseen. Sietokyvyn vahvistaminen ja varautumisen kehittäminen edesauttavat kuitenkin toiminnan jatkuvuuden varmistamista. Analyysin perusteella päätettiin useista kehittämistoimenpiteistä. (Arcada 2017.)

Arcada asettaa Tutor Max -auditoinnin tuloksien, turvallisuuspolitiikan, riskien arvioinnin ja liiketoiminta-analyysin perusteella turvallisuuden toimenpiteet tuleville vuosille. Toimintaohjelma integroidaan Työturvallisuuslain (L738/2002) 9 §:n mukaiseen työsuojelun toimintaohjelmaan, jotta turvallisuusjohtaminen olisi tehokasta ja kokonaisvaltaisempaa resurssien hyödyntämistä. Toimintaohjelma suunnitellaan johdon tahtotilan, myönnettyjen resurssien, tavoitteiden ja hyväksynnän mukaisesti. Toimintaohjelman sisältö voi muuttua, mikäli riskien arvioinnissa saadaan uutta tietoa, joka muuttaa eri riskien tasoa. Vastaavasti kaikissa suurissa muutostilanteissa katselmoidaan toimintaohjelmaa ja suunnitellaan mahdollisista muutoksista. Toimintaohjelmaa tullaan seuraamaan jatkuvasti johdon määrittelemällä tavalla. (Arcada 2017.)

7 Opinnäytetyön prosessi

Toiminnallisen opinnäytetyön tarve syntyi Arcadan johdon tunnistaessa tarpeen turvallisuusjohtamisen kehittämiselle ammattikorkeakoulussa. Arcadan johto on jo aiemmin asettanut tavoitteet turvallisuusjohtamiselle Tutor max -arviointimenettelyssä, jossa tavoitteet toimivat suuntaa-antavina kehittämistyössä. Opinnäytetyön tekijä tunnisti mahdollisuuden opinnäytetyöhön työskenneltyään Arcadan turvallisuusjohtamisen kehittämisen parissa, joten syyskuussa opinnäytetyön suunnitelmaa aloitettiin luonnostelemaan. Koko opinnäytetyön ajan on tekijä myös tehnyt rinnakkain turvallisuusjohtamisen kehittämistyötä Arcadassa. Kehittämistyö tulee jatkumaan opinnäytetyön jälkeen.

Arcadan johto hyväksyi ehdotetun opinnäytetyösuunnitelman loka-marraskuussa 2016, jonka jälkeen työtä aloitettiin tekemään. Käytännössä opinnäytetyötä lähdettiin rakentamaan silloisten toimenpiteiden; riskien arvioinnin tuloksien ja johtopäätöksien sekä liiketoiminta-analyysin suunnitelman pohjalta. Joulu- ja tammikuussa suoritettiin liiketoiminta-analyysi, joka on ohjannut työtä Arcadan toiminnan jatkuvuuden näkökulmasta. Samaan aikaan aloitettiin

myös opinnäytetyön tiedonhankinta, joka on perustunut voimakkaasti luotettavien kirjallisuuslähteiden etsimiseen sekä kansallisten ja kansainvälisten standardien ja lainsäädännön hyödyntämiseen.

Tammikuussa 2017 suunniteltiin myös ammattikorkeakoulujen turvallisuuspäälliköille suunnatut teemahaastattelut, jotka yhdessä benchmarkingin kanssa muodostivat opinnäytetyön kvalitatiiviset tiedonkeruumenetelmät. Benchmarking kohdistui Laurea-ammattikorkeakouluun, joka on kehittänyt monta vuotta systemaattisesti turvallisuusjohtamistaan. Menetelmät valittiin jo aiemmin, koska kvantitatiivisilla menetelmillä ei olisi todennäköisesti saanut tarpeeksi luotettavaa ja määrällisesti laadukasta aineistoa vähän tutkitusta aiheesta, ammattikorkeakoulujen turvallisuusjohtamisesta. Ongelmaksi muodostui myös yleisesti suomalaisten ammattikorkeakoulujen turvallisuusjohtamisen nykytaso, joka yleisesti vaatii vielä kehittämistä.

Helmi- ja maaliskuussa 2017 toteutettiin teemahaastattelut sekä tarkastettiin kattavasti työn teoriakatsaus, jonka jälkeen teoriaa lisättiin työhön aiemmin kerätyistä kirjallisuuslähteistä. Teemahaastattelut analysoitiin sisällönanalyysillä maaliskuun alussa 2017, jonka jälkeen työn tulokset kirjoitettiin auki. Tuloksiin ja teoriaan perustuen tehtiin seuraavaksi johtopäätökset, joiden keskeisimmät tuotokset ovat turvallisuusjohtamisjärjestelmän luomisen mallit, joita voidaan soveltaa missä tahansa suomalaisessa ammattikorkeakoulussa. Tämän jälkeen tuloksia vielä muokattiin, jonka jälkeen haastatelluille lähetettiin sähköpostitse heihin viitatut kohdat opinnäytetyöstä. Vastauksien perusteella tuloksia, menetelmiä ja johtopäätöksiä muokattiin edelleen, sähköpostivastauksien perusteella. Tuloksien korjaamisen jälkeen lähetettiin tiivistelmä ja englanninkielinen tiivistelmä kielen tarkastukseen. Kielen tarkastuksen korjauksien perusteella viimeisteltiin tiivistelmät.

Maaliskuun alussa 2017 tarkastettiin ja muokattiin vielä teoriaosuus valmiiksi. Muut osuudet valmistuivat palaute-ehdotuksien mukaisesti ennen huhtikuuta. Tämän vuoksi tavoiteaika työn valmistumisesta toukokuuhun mennessä nopeutui, ja työ saatiin valmiiksi huhtikuun alussa, jolloin se julkaistiin Theseuksessa. Koko opinnäytetyön ajan on käyty keskustelua opinnäytetyön ohjaajan kanssa työn sisällöstä ja seuraavista toimenpiteistä tarvittaessa, noin kerran kuussa. Opinnäytetyön keskeiset havainnot ja johtopäätökset esiteltiin opinnäytetyöseminaarissa 28.3.2017. Tarkoituksena on myös, että työstä esitettäisiin mahdollisesti johtopäätöksiä Ammattikorkeakoulujen turvallisuusverkoston tapaamisessa toukokuussa 2017.

8 Opinnäytetyössä käytetyt menetelmät

Toiminnallinen opinnäytetyö valikoitui käytettäväksi tutkimuksellisen opinnäytetyön sijasta, koska on luonnollisempaa, että organisaation sisältä kuvattuna, tiiviissä yhteistyössä organisaation kanssa, tehdään toiminnallinen opinnäytetyö. Koska tekijällä ei ole enää objektiivista

kuvaa Arcadasta, jonka toiminta on vaikuttanut jo merkittävästi tekijän asenteisiin ja ajatuksiin, on toiminnallinen muoto lopputuloksen kannalta parempi ratkaisu. Toiminnallisuus korostuu myös opinnäytetyön tavoitteissa, joissa organisaatiolle luodaan tuotoksena pidemmän ajan suunnitelma, jolla ylletään turvallisuusjohtamisjärjestelmään, sekä kehittämisehdotukset, joilla suunnitelman toteuttaminen on mahdollista.

Tiedonkeruumenetelmät valittiin sen perusteella, miten aihetta tulisi lähestyä ammattikorkeakoulujen toiminnan perusteella sekä miten aiheesta pystyisi keräämään tutkimustietoa. Työhön valittiin laadulliset menetelmät, koska aiheeseen on vaikea ja työlästä kerätä määrällisin menetelmin luotettavaa tietoa ammattikorkeakoulujen turvallisuusjohtamisesta, opinnäytetyön puitteessa. Suomalaisten ammattikorkeakoulujen turvallisuusjohtamisen taso on tutkimustulosten mukaan alle lainsäädännön tarkoittaman vähimmäistason, joten opinnäytetyöhön ei olisi saatu tarpeeksi luotettavaa otantaa määrällisen menetelmän toteuttamiseksi. Opinnäytetyössä haluttiin kohdistaa turvallisuusjohtamisjärjestelmän kehittäminen erityisesti ammattikorkeakouluihin, joten muiden oppilaitosten tai alojen turvallisuusjohtamisjärjestelmien luomista ja valmista mallia ei nähty tarkoituksenmukaisena työn kannalta.

Työssä haluttiin keskittyä turvallisuusjohtamisen näkökulmasta hyvin menestyvien ammattikorkeakoulujen toimintaan, minkä takia benchmarking valikoitui tiedonkeruumenetelmäksi ja se kohdistui Laurea-ammattikorkeakouluun, jossa on tehty turvallisuusjohtamisen systemaattista kehittämistä useita vuosia. Haastattelulla kerättiin kaikki benchmarkingin tiedot. Muilla teemahaastatteluilla haettiin erityisesti hyviä käytänteitä sekä yritettiin nähdä erilaisia toimintatapoja, joilla turvallisuusjohtamista ja riskienhallintaa voidaan suunnitella ja toteuttaa. Lomakehaastatteluilla pyrittiin saamaan tarvittavaa tietoa liiketoiminta-analyysin toteuttamiseksi sekä toimenpiteiden kehittämiseksi. Tiedonkeruumenetelmien avulla saadut tulokset analysoitiin aineistolähtöisellä sisällönanalyysillä.

8.1 Toiminnallinen opinnäytetyö

Tutkimuksellisen opinnäytetyön vaihtoehto, toiminnallinen opinnäytetyö, tavoittelee ammatillisessa kentässä käytännön ohjeistamista, opastamista ja toiminnan järkeistämistä. Toiminnallisuuden tuotoksena syntyy, alasta riippuen, perehdyttämisopas, turvallisuusohjeistus tai esimerkiksi tapahtuman, kuten kansainvälisen kokouksen, konferenssin tai seminaarin toteuttaminen. Toteutuksen tuotoksena voi myös olla kirja, opas tai kotisivut. Olennaista on, että toiminnallisessa opinnäytetyössä yhdistyvät käytännön toteutus ja sen raportointi tutkimuksellisin menetelmin. Ammattikorkeakoulun opinnäytetyön peruselementtejä ovat siten työelämälähtöisyys, käytännönläheisyys, tutkimuksellisuuden keinoja hyödyntävä ja riittävällä tasolla alan tietoja ja taitoja hyödyntävä. (Airaksinen & Vilkka 2003, 9-10.)

Toiminnallisen opinnäytetyön raportissa selviää Airaksisen ja Vilkan (2003, 65) mukaan mitä, miksi, ja miten on tehty, millainen oli työprosessi ja millaisiin tuloksiin sekä johtopäätöksiin päädyttiin. Raportissa tulisi olla myös tekijän oma arviointi prosessista, lopputuotoksesta ja oppimisesta. Lukija pystyy raportin avulla päättelemään, miten opinnäytetyössä onnistuttiin. Opinnäytetyötä voisi kuvatakin välineenä, jolla pystyy havainnollistamaan omaa ammatillista osaamista. Raportin lisäksi toiminnalliseen opinnäytetyöhön kuuluu tuotos, joka tehdään työn tilaajaorganisaatiolle, joten se on lähes aina kirjallinen. Tuotos poikkeaa raportista, koska siinä ei käytetä tutkimuksellisuuden menetelmiä samalla tavalla kuin raportissa. (Airaksinen & Vilkka 2003, 65.)

Raportin rakenne noudattaa kertomusta toiminnallisessa opinnäytetyössä. Raportista selviää Airaksisen ja Vilkan (2003, 82-83) mukaan, miten työhön on löytynyt aihe, mitä tutkimuskysymyksiä on lähdetty ratkomaan ja miten tutkimuskysymyksiin on etsitty vastauksia sekä mitä ratkaisuja on tehty, jotta tuotos on saatu aikaan. Opinnäytetyön sisältösuunnitelma tulisi sisältää ainakin johdannon, lähtökohdat, tarkoituksen ja tavoitteet, rajaukset, sisältöön kuuluvat asiat, teoreettinen viitekehys, menetelmien esittely, tuotoksen valmistamiseen liittyvät asiat ja johtopäätökset sekä opinnäytetyön prosessin arviointi. (Airaksinen & Vilkka 2003, 82-83.)

8.2 Laadullisen tutkimuksen periaatteet

Todellisen elämän kuvaaminen on lähtökohta laadulliselle tutkimukselle, jossa aineistonkeruun väline on tutkija itse (Ojasalo ym. 2014, 105). Tämä opinnäytetyö on toteutettu laadullisen tutkimuksen prosessin periaatteiden mukaisesti. Laadullisen tutkimuksen voi nähdä eräänlaisena oppimisprosessina, koska tutkijan näkökulma ja tulkinnat kehittyvät tutkimusprosessin edetessä. Tällaisessa lähestymistavassa tutkimuksen eri vaiheet eivät ole selkeästi jäsenneltävissä, vaan aineistonkeruuta koskevat ratkaisut voivat kehittyä tutkimuksen edetessä. Lähestymistapa vaatii tutkijalta sitä, että hän ymmärtää oman tietoisuutensa kehittymisen tutkimuksen aikana ja on valmis tekemään uusia linjauksia. Tällöin ominaista on myös intensiivinen organisaation sisältä päin kuvattu tutkittavien näkökulma. Aaltolan ja Vallin (2015, 84) mukaan prosessimaisessa lähestymistavassa tutkimuksen reliabiliteetin ongelmallisuus ei keskity mittaamisen luonteeseen, kuten tavallisesti laadullisessa tutkimuksessa, vaan aineiston keruun vaihtelevuuden hallitsemiseen. (Aaltola & Valli 2015, 74-75.)

8.3 Tiedonkeruumenetelmät

Kehittämistyössä on suositeltavaa käyttää monenlaisia tutkimusmenetelmiä, jotka on perinteisesti jaettu määrällisiin ja laadullisiin menetelmiin, joita kutsutaan kvantitatiivisiksi ja

kvalitatiivisiksi menetelmiksi. Laadullisista tutkimusmenetelmistä käytetään tässä toiminnallisessa opinnäytetyössä teemahaastattelua ja benchmarkingia. Määrällisistä menetelmistä käytetään strukturoitua haastattelua. Useampi menetelmä valittiin tutkimuksen validiuden parantamiseksi. Validius eli pätevyys tarkoittaa Hirsjärven ym. (2010, 231) mukaan tutkimusmenetelmän kykyä mitata sitä, mitä on tarkoituskin mitata. Useiden tutkimusmenetelmien käyttämistä kutsutaan Hirsjärven ym. (2010, 233) mukaan triangulaatioksi, jonka avulla voidaan lisätä opinnäytetyön luotettavuutta, reliabiliteettia. (Ojasalo ym. 2014, 105.)

Opinnäytetyön haastattelut suoritettiin yksilöhaastatteluina teemoittain pois lukien liiketoiminta-analyysin haastattelut, jotka tehtiin strukturoidulla haastattelulla. Haastattelu on aineistonkeruumenetelmänä hyvä valinta, kun halutaan korostaa yksilöä, jolla on mahdollisuus tuoda esille itseään koskevia asioita. Haastattelu sopii kehittämistyöhön, koska sillä saadaan kerätyksi nopeasti syvällistä tietoa kehittämisen kohteesta. Haastattelulla on myös mahdollista saada kerätyksi uusia näkökulmia vähän tutkitusta kohteesta, kuten turvallisuusjohtamisjärjestelmästä ammattikorkeakoulussa. (Ojasalo ym. 2014, 106.)

Teemahaastattelu on tyypillinen kvalitatiivinen menetelmä, joka on Hirsjärven ym. (2010, 208) mukaan lomake- ja avoimen haastattelun välimuoto, puolistrukturoitu haastattelu, jossa aihepiirit ovat tiedossa, mutta kysymysten tarkka muoto ja järjestys puuttuvat. Teemahaastattelu valikoitui haastattelumuodoksi sen joustavuuden takia. Hirsjärven & Hurmeen (2014, 48) mukaan teemahaastattelu antaa haastateltavan äänen paremmin kuuluviin ja vapauttaa tutkijan näkökulmasta. Se on haastattelujen tuloksien kannalta tärkeää, koska turvallisuuden johtaminen on subjektiivista suunnittelu- ja toteuttamisvaiheissa, vaikka puitteet ja periaatteet ovatkin yleensä samanlaisia. Tällöin teemakohtainen, strukturoitua haastattelua vapaampi, lähestymistapa tuottaa todennäköisemmin parempia tuloksia. Teemahaastattelu toimii Vilkan ja Airaksisen (2003, 63) mukaan paremmin toiminnallisessa opinnäytetyössä, kun tavoitteena on kerätä tietoa tietystä teemasta. (Hirsjärvi & Hurme 2014, 47-48; Ojasalo ym. 2014, 104.)

Benchmarking selvittää Ojasalon ym. (2014, 186) mukaan syitä, jotka ovat menestyvien organisaatioiden taustalla ja miten kyseisten organisaatioiden hyväksi havaittuja tapoja voidaan soveltaa omaan organisaatioon. Menetelmällä havaituista toimista osaa voidaan soveltaa suoraan, mutta osaa joudutaan räätälöimään omaan toimintaan sopivaksi, muun muassa organisaatiokulttuurien erojen takia. Sen takia on tärkeää tulkita menetelmällä saatuja tuloksia kriittisesti, jotta ei toimintaa ei kopioida suoraan omaan käyttöön vaan asetetaan kerätty tieto kontekstiin, verraten ja hyödyntäen soveltavasti omassa toiminnassa. (Ojasalo ym. 2014, 186.)

Benchmarkingin tavoite tässä opinnäytetyössä on vastata tutkimuskysymykseen, miten turvallisuusjohtamisjärjestelmä luodaan ammattikorkeakouluun, mutta myös selvittää niitä tekijöitä, jotka tekevät turvallisuuden johtamisesta järjestelmällistä ja kokonaisvaltaista. Hyvien käytänteiden ja mahdollisten virheiden välttäminen kuuluvat myös menetelmän tuloksien odotuksiin. Menetelmällä toivotaan myös saavan tietoa, miten vastaava organisaatio on arvioinut oman järjestelmänsä luomista; mitä olisi voinut tehdä toisin ja mitä jäi tekemättä?

Benchmarking voidaan jaotella kolmeen vaiheeseen. Menetelmä aloitetaan Ojasalon ym. (2014, 186) mukaan tunnistamalla kehittämistä kaipaava kohde. Arcadan kokonaisvaltainen turvallisuustyö vaatii käytännössä järjestelmällisen tavan hallita ja johtaa tietoa sekä henkilöitä kokonaisvaltaisen turvallisuusjohtamisen jatkuvassa parantamisessa. Tämän periaatteen kautta Arcadan johto tunnisti tarpeen kehittää turvallisuusjohtamistaan. Seuraavaksi Arcadan oli helppo löytää vertailuorganisaatio, jolla asia, turvallisuusjohtaminen, toimii yleisesti paremmin ja on myös maineeltaan parempi. Opinnäytetyön tekijän kautta löydettiinkin siis Laurea-ammattikorkeakoulu, joka sopii erityisen hyvin benchmarkingin kohteeksi juuri täysin saman alan yhdistävänä tekijänä, mutta myös usean vuoden jatkuneen järjestelmällisen ja tavoitteellisen turvallisuusjohtamisjärjestelmän luomisen takia (Ranta 2017).

Benchmarkingin viimeinen vaihe on Ojasalon ym. (2014, 186) mukaan järjestelmällinen tiedon keruu ja se perustuu Laurean turvallisuusjohtajan teemahaastatteluun, jolla kaikki tieto kerätään. Kerättyä tietoa analysoidaan erityisesti Arcadan tavoitteiden, nykytilan ja johdon tahdon näkökulmasta vertaillen Laurean monen vuoden kehitystyöhön joka Rannan (2017) mukaan jatkuu edelleen. Turvallisuusjohtaja on ollut alusta alkaen luomassa turvallisuusjohtamisjärjestelmää Laureaan, joten hän onkin sopivin taho vastaamaan kysymyksiin Laureassa tapahtuneesta turvallisuuden kehittämistyöstä (Ranta 2017).

8.4 Aineistolähtöinen sisällönanalyysi

Laadullisen aineiston analyysin tarkoitus on Sarajärven ja Tuomen (2012, 108) mukaan, Hämäläiseen viitaten (1987), lisätä informaation arvoa luomalla hajanaisesta aineistosta selkeä, tiivis ja yhtenäinen informaatio. Analyysi perustuu tulkintaan ja päättelyyn, jossa empiirinen aineisto luo pohjan käsitteellisemmälle näkemykselle tutkittavasta ilmiöstä. Analyysilla luodaan selkeyttä kerättyyn aineistoon, jotta voidaan tehdä selkeitä ja luotettavia johtopäätöksiä tutkittavasta ilmiöstä. Aineiston laadullinen analyysi perustuukin loogiseen päättelyyn ja tulkintaan, jossa aineisto hajotetaan osiin, käsitteellistetään ja lopuksi kootaan uudestaan uudella tavalla loogiseksi kokonaisuudeksi. Analyysia tehdään tutkimuksen jokaisessa vaiheessa. Aineistolähtöisessä sisällönanalyysissa saadaan vastaus tutkimuskysymykseen yhdistelemällä käsitteitä. (Sarajärvi & Tuomi 2012, 108-112, Hämäläisen 1987, mukaan.)

Ennen sisällönanalyysin aloittamista tulee määritellä tutkimuskysymyksen perusteella aineistoyksikkö, joka on tässä opinnäytetyössä sana. Laadullisen aineiston sisällönanalyysi aloitetaan aineiston pelkistämisellä, redusoinnilla, jolloin aineistosta karsitaan epäolennainen pois, kuten esimerkiksi litteroitu haastattelu. Pelkistäminen voi olla informaation tiivistämistä tai pilkkomista osiin, jolloin tutkimustehtävä ohjaa pelkistämistä. Auki kirjoitetusta aineistosta etsitään tutkimuskysymystä kuvaavia ilmaisuja, jotka nostetaan erikseen esille. (Sarajärvi & Tuomi 2012, 109-110, Hämäläisen 1987, mukaan.)

Aineiston ryhmittelyssä, klusteroinnissa, aineiston alkuperäisilmaukset käydään läpi ja etsitään samankaltaisuuksia tai eroavaisuuksia kuvaavia käsitteitä. Samaa asiaa tarkoittavat käsitteet jaotellaan ja yhdistetään luokaksi. Luokitteluyksikkönä käytetään tässä opinnäytetyössä käsitettä, kuten jatkuvaa kehittämistä. Luokittelussa yksittäiset tekijät sisällytetään yleisimpiin käsitteisiin, jolloin aineisto tiivistyy jälleen. (Sarajärvi & Tuomi 2012, 110, Hämäläisen 1987, mukaan.)

Sarajärvi & Tuomi (2012, 111) toteavat Hämäläiseen (1987) viitaten, että sisällönanalyysin viimeisessä vaiheessa, abstrahoinnissa, erotetaan tutkimuksen kannalta olennainen tieto, jonka perusteella muodostetaan teoreettisia käsitteitä. Abstrahoinnissa edetään kielellisistä ilmauksista johtopäätöksiin ja käsitteisiin. Abstrahointia jatketaan yhdistelemällä luokituksia, kunnes se ei ole enää sisällön näkökulmasta mahdollista. Abstrahoinnissa empiirinen aineisto yhdistetään teoreettisiin käsitteisiin ja tuloksissa esitetään empiirisestä aineistosta muodostetut käsitteet tai malli. (Sarajärvi & Tuomi 2012, 111-113, Hämäläisen 1987, mukaan.)

9 Tulokset

Tiedonkeruumenetelmillä saadut tulokset perustuvat kolmeen haastatteluun, joista Laurean turvallisuusjohtajan teemahaastattelusta johdetaan opinnäytetyön benchmarkingin tulokset. Tulokset kattavat turvallisuusjohtamis- ja riskienhallintatoiminnan ammattikorkeakoulussa sekä turvallisuusjohtamisjärjestelmään liittyviä elementtejä. Tärkeimmät tulokset keskittyvät turvallisuusjohtamisen ja riskienhallinnan periaatteisiin ja puitteisiin, joiden perusteella ammattikorkeakoulun tulee organisoida, suunnitella ja toteuttaa kehittämistyötänsä.

9.1 Riskienhallinta ja turvallisuusjohtaminen

Riskienhallinta on Rannan (2017) mukaan suomalaisille koulutusorganisaatioille osin vielä haasteellista. Ammattikorkeakoulujen riskienhallinnan tulisi perustua riskienhallinnan periaatteisiin, puitteisiin ja prosesseihin. Riskienhallintatoiminta on johdon tahdosta ja myönnetyistä

valtuuksista sekä resursseista riippuvaista toimintaa, joka mahdollistaa systemaattisen turvallisuusjohtamisen. Riskienhallinnan tulisi olla Hyvösen (2017) mukaan osa ammattikorkeakoulun normaalia, säännöllistä, toimintaa ja riskien arviointia tulisi tehdä koko organisaatiossa. Turvallisuusjohtamisjärjestelmän näkökulmasta tulisi riskienhallintaa myös kehittää määrätietoisesti kohti kokonaisvaltaista riskienhallintajärjestelmää. Laurean johto onkin linjannut riskienhallinnan kehittämiskohteekseen. Riskienhallinta on ennen kaikkea johdon väline päätöksenteon tueksi. (Ranta 2017.)

Suomalaisten ammattikorkeakoulujen turvallisuusjohtamisessa on kehitettävää, vaikka hyvää ja pitkäjänteistä turvallisuustyötä onkin toteutettu. Ammattikorkeakoulun turvallisuusjohtamisen tulisi perustua riskienhallintaan (Ranta 2017; Hyvönen 2017; Sjöberg 2017). Haasteeksi Rannan (2017) mukaan muodostuu se, että koska riskejä ei vielä hallita, ei voida varmuudella tietää, mistä turvallisuusjohtamisen kehittäminen pitäisi aloittaa. Turvallisuusjohtamisen nykytila sekä kehittämisen painopisteet ja tavoitteet eivät ole tällöin vielä selvillä. Johdon vahva tuki on erityisen tärkeää, koska ilman vaadittavia resursseja turvallisuusjohtamisen kehittäminen on mahdotonta. Turvallisuusjohtaminen on Hyvösen (2017) mukaan osa organisaation normaalia johtamista ja laadunhallintaa. EK:n turvallisuusjohtamismallin (2017) mukaisesti turvallisuus perustuu riskienhallinnan lisäksi strategiaan ja malli soveltuu hyvin ammattikorkeakouluihin (Sjöberg 2017; Hyvönen 2017). (Ranta 2017.)

Ammattikorkeakoulun turvallisuusjohtamisessa korostuu Hyvösen (2017) mukaan opiskelijoiden ja työntekijöiden turvallisuus ja hyvinvointi, koska niillä on vaikutusta siihen, miten turvallisena ja hyvinvoivana opiskelu- ja työskentely-ympäristö koetaan. Esimiesten velvollisuutena on huolehtia työntekijöidensä työturvallisuudesta ja työhyvinvoinnista. Sjöberg (2017) painottaa koko ammattikorkeakouluyhteisön mukaan ottamista turvallisuustyöhön, sidosryhmät mukaan lukien, ja koko ammattikorkeakoulun turvallisuuskulttuurin kehittämistä. Koulutus on yksi tärkeimmistä välineistä, joilla turvallisuuskulttuuria voidaan kehittää. Turvallisuuskoulutusta tulisi järjestää kaikille työntekijöille ja opiskelijoille, mutta riskien arvioinnin perusteella tulisi tarjota tietyille henkilöille riskiperusteisesti lisäkoulutusta. (Hyvönen 2017.)

Hyvönen (2017) nostaa esille jatkuvuuden hallinnan tärkeyden ammattikorkeakoulussa. Vaikka Ammattikorkeakoululaissa (L932/2014) puhutaankin varautumissuunnitelmista, tulisi keskittyä ennemmin toiminnan jatkuvuuden turvaamiseen kaikissa tilanteissa, eikä vain poikkeusoloissa. Sjöberg (2017) näkee erityisesti Arcadan näkökulmasta jatkuvuuden hallinnan erittäin tärkeänä, koska Arcada on yhden kampuksen ammattikorkeakoulu ja sen toimintaan sisältyy paljon erilaisia, erityistä osaamista vaativia, koulutusohjelmia ja toimintoja. Sama pätee myös muihin ammattikorkeakouluihin, joissa on jotain erityistä, haavoittuvaista, toimintaa tai muita prosesseja tai toimintoja, joiden ominaisuudet tekevät niistä poikkeuksellisen haavoittuvaisia toiminnan jatkuvuuden kannalta katsottuna (Sjöberg 2017).

9.2 Turvallisuusjohtamisjärjestelmän luominen

Arcadan ja Metropolian turvallisuuspäälliköt Sjöberg (2017) ja Hyvönen (2017) sekä Laurean turvallisuusjohtaja Ranta (2017) korostavat turvallisuusjohtamisen kehittämisessä resursseja; ilman ajallisia ja rahallisia resursseja ei turvallisuusjohtamisjärjestelmää voi alkaa luoda. Johdon tulee itse tunnistaa tarve turvallisuusjohtamisjärjestelmälle, jotta se voi asettaa tavoitteet ja resurssit, joilla ylletään järjestelmään johdon määrittelemässä ajassa. Nykytilan asettaminen ja kehittämistoimenpiteiden määrittely vievät kaikki kohti kokonaisvaltaista turvallisuusjohtamisjärjestelmää. Laureassa on käytössä ASTERI-menetelmä, jolla turvallisuusjohtamisjärjestelmää auditoidaan. (Ranta 2017.)

Yksittäisistä tekijöistä korostuvat henkilöstön sitoutuminen turvallisuuteen, turvallisuuskulttuurin kehittäminen, ja johdon myöntämät resurssit, jotka määrittävät miten turvallisuusjohtamisessa edistytään. Ranta (2017), Hyvönen (2017) ja Sjöberg (2017) toteavatkin, että olennaisempaa on jatkuva kehittäminen sen sijasta, että suhtauduttaisiin turvallisuusjohtamiseen kuin hankkeeseen; turvallisuusjohtamisjärjestelmän kehittämistä ei voida nähdä vain yksittäisinä vaiheina, jotka suoritetaan ja sen jälkeen ne unohdetaan. Turvallisuusjohtamisjärjestelmää voi verrata kokonaisuuteen, joka muodostuu useista eri prosesseista, jotka vaativat jatkuvaa ylläpitoa, kehittämistä sekä seurantaa. Turvallisuusjohtamisjärjestelmän luomisen voisikin kiteyttää systemaattiseksi kehittämistyöksi, joka perustuu ensisijaisesti riskienhallintaan. (Ranta 2017.)

Ranta (2017) kertoi, että Laureaan kohdistui ensimmäinen turvallisuusjohtamisen auditointi vuonna 2011. Se toteutettiin Tutor max - arviointimenettelyllä, joka soveltuu turvallisuusjohtamisen auditointiin erittäin hyvin. Tuolloin tunnistettiin turvallisuusjohtamisen nykytila sekä asetettiin tavoitteet noin kolmen vuoden päähän. Turvallisuusjohtamisen järjestelmällinen kehittäminen aloitettiinkin heti. Laurean johto tunnisti tarpeen systemaattisen turvallisuustyön aloittamiselle, jotta Laurea voisi yltää turvallisuusjohtamisen kehittämistavoitteisiinsa. Nämä priorisoitiin turvallisuusjohtamisen kahdeksan eri osa-alueen mukaan. Turvallisuustyön kehittämistä voidaan kuvailla eri toimintojen ja prosessien systemaattisella hallinnalla taulukon 5 mukaisesti, jolla voidaan hahmottaa karkealla tasolla sitä, mitä Laureassa on tehty viime vuosien aikana. Laurean toiminnan vertaaminen ja aloitetut prosessit perustuvat benchmarkingiin, jotta Arcada pystyisi soveltamaan turvallisuusjohtamisen periaatteita, elementtejä ja prosesseja turvallisuusjohtamisjärjestelmänsä luomiseen. (Ranta 2017.)

Prosessin vaihe/vuosi	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Tutor max -auditointi	X				O					
Turvallisuus-päällikkö ja resurssit	X					O				
Johto tunnistaa tarpeen turvallisuusjohtamisjärjestelmälle	X						O			
Systemaattinen kehittäminen alkaa	X					O				
Turvallisuuspolitiikka luodaan	X					O				
Riskienhallinta-prosessi alkaa	X					O				
Raportointijärjestelmän luominen alkaa	X					O				
Dokumentointi aloitetaan	X					O				
Kriisiviestintää aloitetaan suunnitella	X O									
Vastuiden jakaminen alkaa	X					O				
Lain vaatimuksien seuranta alkaa	X					O				
Jatkuvuudenhallinta-prosessi käynnistyy			X				O			
Riskilähtöinen koulutus aloitetaan pilotteina			X				O			
Proaktiivinen turvallisuusviestintä aloitetaan			X			O				

Prosessin vaihe/vuosi	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Turvallisuustarkastukset aloitetaan			X					O		
Systemaattinen mittaaminen alkaa						X		O		
Turvallisuusjohtaja nimetään osaksi johtoryhmää							X			
Arcada=O Laurea=X										

Taulukko 5: Turvallisuusjohtamisjärjestelmän luominen - prosessien aloitukset Laurea/Arcada (soveltaen Ranta 2017; Arcada 2017; Sjöberg 2017)

Taulukossa 5 on esitetty X:llä se, milloin Laureassa kyseinen prosessi on aloitettu. Ranta (2017) painottaakin: ”Mikään ei ole jäänyt paikoilleen, vaan jatkuvan kehittämisen sykli on käynnissä koko ajan.” O kuvaa vastaavasti Arcadan vastaavan prosessin systemaattisen kehittämisen aloittamista. Turvallisuustarkastuksien ja systemaattisen mittaamisen prosessit ovat kuviossa esitetty aloitettavaksi seuraavien vuosien aikana Arcadassa. Turvallisuuden toimintaohjelma ohjaa tätä kehittämistä. (Sjöberg 2017.)

Laurean ensimmäisinä toimenpiteinä suunniteltiin ja toteutettiin turvallisuuspolitiikka, aloitettiin raportointijärjestelmän luominen sekä jaettiin vastuita nimittämällä kampusten turvallisuusvastaavat, turvallisuuden dokumentointi aloitettiin sekä kriisiviestintää alettiin suunnitella. Lain vaatimuksien seuraaminen on kuulunut turvallisuuspäällikön tehtäviin alusta alkaen. Vuonna 2013 aloitettiin jatkuvuudenhallinnan kehittäminen työpajakokonaisuuden avulla, riskiperusteinen turvallisuuskoulutus sai pilottinsa sekä sisäiset turvallisuustarkastukset ja proaktiivinen viestintä tulivat osaksi toimintaa. Vaikka turvallisuustyön vaikuttavuutta oltiin aloitettu mitata jo aiemmin, vuonna 2016 Laurea aloitti systemaattisen turvallisuuden mittaamisen uuden mittariston turvin ja seuraavana vuonna Ranta kutsuttiin johtoryhmään. (Ranta 2017.)

Kun katsotaan turvallisuusjohtamisen kehittämiseen käytettyjä vuosia, voidaan todeta, että riskilähtöinen turvallisuuskoulutus olisi ollut hyvä pyrkiä aloittamaan nopeammin. Turvallisuuskoulutusta tullaankin jalkauttamaan edelleen kattavammin organisaation kaikille tasoille. Myös muita turvallisuusjohtamisen osa-alueita tullaan Laureassa kehittämään edelleen voi-

mallisesti. Turvallisuudesta viestimistä tullaan kehittämään koko korkeakouluyhteisön suuntaan ja myös turvallisuusasenteita mittaava mittari tullaan jalkauttamaan koko yhteisön turvallisuustyön kehittämiseksi entisestään. Ranta (2017) korostaakin, ettei tämä työ ole koskaan onneksi valmis; uusia asioita tulee turvallisuusalan kehittyessä koko ajan lisää. Tämä antaa tulevaisuudessa myös eri alojen opiskelijoille hyvät mahdollisuudet oppia Laurean tavasta toteuttaa turvallisuutta ja viedä tätä myös työelämän hyödyksi. Lopuksi Ranta vielä pohtii, miten systemaattisesti suomalaiset koulutusorganisaatiot ovat työskentelemässä kohti kokonaisvaltaista turvallisuusjohtamisjärjestelmää. Tämä vienee vielä aikaa, sillä tähän pääseminen vie ainakin kuudesta yhdeksään vuoteen. (Ranta 2017.)

Arcadan systemaattinen kehittäminen on aloitettu pääosin vuonna 2016, viisi vuotta Laurean jälkeen (Sjöberg 2017). Voidaankin vertailla, mitä toimintoja ja prosesseja Laurea on lähtenyt työstämään aloitettuaan systemaattisen kehittämisen ja mihin perustuen. Benchmarking keskittyy tässä opinnäytetyössä kuvaamaan erityisesti sitä, millä periaatteilla ja puitteilla kehittämistä tulisi lähestyä. Tärkeä osa on myös se, mihin suuntaan turvallisuudessa paremmin suoriutuva organisaatio on kehittänyt toimintaansa, mistä Arcada voisi soveltaa omaan toimintaansa.

Benchmarkingin keskeisin tulos turvallisuusjohtamisjärjestelmän luomisessa keskittyy ensimmäisiin vaiheisiin, joissa nykytilan analyysi, riskienhallinta, johdon asettamat tavoitteet ja myöntämät resurssit luovat perustan turvallisuusjohtamisen systemaattiselle kehittämiselle. Ranta (2017) toteaa, että suomalaisten korkeakoulujen olisi tärkeää keskittyä riskienhallinnan suunnitteluun ja sitten sen toteuttamiseen sekä jalkauttamiseen niin, että se kattaisi kaikki kohdeorganisaation keskeiset prosessit. Riskilähtöisyydestä muodostuu näin perusta kaikelle turvallisuustyölle. Sjöbergin (2017) mukaan eri vaiheet tulisi huomioida kehittämisessä perustuen riskien arviointiin ja asetettuihin tavoitteisiin. Mikäli ammattikorkeakoulu haluaa yltää kokonaisvaltaiseen turvallisuusjohtamisjärjestelmään, kaikki toiminnot ja prosessit tulee saada osaksi turvallisuusjohtamista (Sjöberg 2017). Arcadan (2017) turvallisuuden toimintaohjelmassa painottuvatkin proaktiivisen viestinnän kehittäminen sekä turvallisuustarkastuksien ja systemaattisen mittaamisen aloittaminen.

Hyvönen (2017) näkee turvallisuusjohtamisjärjestelmän jatkuvan parantamisen kehänä PDCA-mallin mukaisesti. Järjestelmä perustuu strategiaan ja sen suunnitteluun sisältyy esimerkiksi turvallisuuspolitiikka, turvallisuuden toimintaohjelma, riskien arvioinnit ja jatkuvuuden hallinta. Toteuttaminen perustuu opastukseen, perehdyttämiseen, muutoksiin reagoimiseen, johtamiseen, ohjaamiseen sekä koulutukseen. Auditoinnilla arvioidaan toimintaa ja siihen sisältyvät sisäiset turvallisuuskyselyt henkilökunnalle ja opiskelijoille, sisäiset tarkastukset sekä ulkoiset auditoinnit, kuten palotarkastukset. Sjöberg (2017) korostaa erityisesti mittaamisen ja seuraamisen tärkeyttä, jotta muutoksiin ja uusiin riskeihin pystytään asettamaan tarpeelliset

toimenpiteet. Erilaisilla raporteilla voidaan toteuttaa seuraamista ammattikorkeakoulussa ja erityisesti opiskelijoille kohdistetuilla kyselyillä saadaan hyödyllistä tietoa siitä, missä pitäisi parantaa toimintaa ja millainen on opiskelijoiden turvallisuuden tunne koulussa. (Hyvönen 2017.)

10 Johtopäätökset

Ammattikorkeakoulun turvallisuusjohtaminen ei eroa periaatteiltaan ja puitteiltaan muiden alojen turvallisuusjohtamisesta mitenkään. Lähtökohdat ja toteutus voivat olla erilaiset kuin esimerkiksi turvallisuuskriittisissä organisaatioissa, kuten ydinvoimalassa, mutta periaatteessa systemaattinen turvallisuusjohtaminen tulisi aina perustua riskienhallintaan ja vaatimuksien mukaiseen toimintaan, joka on sekin riskien arviointiin perustuvaa. Turvallisuusjohtaminen on osa kaikkea johtamista eikä erillinen toiminto organisaatiossa. Turvallisuus on linjaorganisaation vastuulla, mutta turvallisuustoimintaan sovelletaan myös matriisiorganisaation ja tiimiorganisaation periaatteita. Esimerkiksi jatkuvuuden hallinnassa tai kokonaisvaltaisessa riskien arvioinnissa työpajakokoonpanoissa ei tarkastella ongelmaa yksiköittäin vaan toimintokeskeisenä kaikkiin vaikuttavana kokonaisuutena. Turvallisuusosaston tai turvallisuuspäällikön tehtävänä on tukea linjaorganisaatiota avustaen ja konsultoimalla vastuuhenkilöitä sekä ohjaamalla riskien arviointia.

Kun turvallisuutta aletaan kehittämään päämääränä turvallisuusjohtamisjärjestelmä, tulee nykytilanne selvittää mahdollisimman tarkasti, jotta tiedetään, mitä ollaan tehty ja missä ovat suurimmat kehityskohteet. Johdon tulisi ottaa kantaa tavoitteisiin ja määritellä resurssit, vaadittu riskitaso, tavoiteltu turvallisuuden taso eri osa-alueilla ja tavoitteet. Tutor max – auditointi tarjoaa tähän valmiin työkalun selvittäen, mikä on oma arvio nykytasosta, todellinen taso ja mikä on haluttu taso esimerkiksi 3-4 vuoden päästä. Turvallisuusjohtamisjärjestelmän luominen aloitetaan ulkopuolisen luotettavan ja osaavan toimijan auditoinnilla, joka kertoo objektiivisen kuvan organisaation turvallisuuden nykytilasta. Vastaavasti eri auditointimalleja käyttämällä tulee huomioida nykytilan analyysi ulkopuolisen auditoijan tuloksien lisäksi.

Kun tavoitteet ja nykytila on analysoitu sekä johto myöntänyt resurssit, tulee seuraavaksi määritellä ne periaatteet, puitteet ja prosessit, joiden mukaan turvallisuusjohtamisen kehittäminen tullaan suunnittelemaan ja toteuttamaan. Käytännössä tämä vaatii turvallisuuspolitiikan ja erityisesti riskienhallintapolitiikan laatimista. Keskeistä molemmissa politiikoissa on se, että niissä määritellään molempien toimintojen tavoitteet, suhteet organisaation johtamiseen ja strategiaan. Mikäli tehdään politiikka tai politiikat, jotka eivät perustu strategiaan, arvoihin ja visioon, voidaan puhua toiminnasta, joka ei ole organisaation tavoitteiden mukaista eikä perusteltua. Molempiin politiikkoihin kuuluvat lisäksi vastuut, organisointi, raportointikäytännöt, mittarit ja päämäärä.

Riskienhallintapolitiikka tarvitaan, jotta pystytään laatimaan riskienhallintasuunnitelma, jolla riskienhallintapolitiikkaa toteutetaan. Toteuttamiseen käytetään SFS-ISO 31000 -standardin riskienhallintaprosessia, jolloin prosessin käsittelytoimenpiteet ovat niitä turvallisuustoimenpiteitä, jotka taas noudattavat turvallisuuspolitiikkaa. Turvallisuuden toimintaohjelmalla vastaavasti toteutetaan turvallisuuspolitiikkaa. Tämä on systemaattisen turvallisuusjohtamisen mukaista.

Kun turvallisuuspolitiikka on laadittu, tulee johdon jakaa turvallisuuden vastuut ja päättää organisoinnista sekä määrittää organisaation toimintaympäristö, jotta keskeiset sidosryhmät tunnistetaan ja otetaan mukaan turvallisuustyöhön. Tämä on erityisen tärkeää ammattikorkeakoulussa, jotta turvallisuuskulttuuria voidaan kehittää koko organisaation kaikki jäsenet huomioiden. Mikäli politiikassa on määritelty jo vastuut ja organisointi, tulisi niitä alkaa jalkauttaa politiikassa määritellyille tahoille. Riippuen organisaatiosta ja politiikasta, tulisi ensimmäisenä varmistaa, että turvallisuusasioita käsittelee ja päättää erikseen määritelty turvallisuusjohto, jota johtaa toimitusjohtaja, joka on ammattikorkeakoulussa rehtori. Ylimmällä johdolla on joka tapauksessa aina vastuu turvallisuudesta ja päätösvaltaisena henkilönä on tärkeää, että rehtori on aina tietoinen riskeistä, toimenpiteistä ja yleisesti turvallisuuden tilasta organisaatiossa. Jotta rehtori saa päätöksenteon tueksi tietoa riskeistä ja turvallisuudesta, tulee turvallisuusjohtoon kuulua myös henkilö, joka raportoi ja välittää tietoa suoraan ylimmälle johdolle. Tällainen henkilö on turvallisuuspäällikkö tai turvallisuusjohtaja. Turvallisuusjohtoon tulisi ottaa mukaan myös muita johtajia, mikä on aina organisaatiokohtaista, mutta perusperiaatteena voidaan noudattaa EK:n (2017) turvallisuusjohtamisen osa-alueiden mukaista jakoa ja kokoonpanoa. Esimerkiksi kiinteistö- ja toimitilaturvallisuudesta vastuussa oleva kiinteistöpäällikkö tai kiinteistöjohtaja tulisi ottaa mukaan myös turvallisuusjohtoon, koska hänellä on eniten tietoa tiloista ja kiinteistöstä.

Kun turvallisuusjohtaminen on organisoitu, aloitetaan varsinainen turvallisuustyö riskienhallintaprosessia noudattamalla SFS-ISO 31000 -standardin puitteissa. Käytännössä organisaation toimintaympäristöä on määritelty jo politiikoissa ja organisoinnissa, mutta riskienhallintaympäristön määrittelemiseksi tulisi tunnistaa riskikriteereihin vaikuttavat tekijät, kuten todennäköisyyden määritteleminen. Riskien arviointi on kuitenkin keskeisessä osassa turvallisuusjohtamisessa ja siihen tulee aina valita sopivin menetelmä. SFS-EN 31010 -standardi sekä potentiaalisten ongelmien analyysi tarjoavat keskeisiä menetelmiä. Tämä on myös tärkein prosessi turvallisuustyössä, sillä onnistuneella riskien arvioinnilla saadaan kustannustehokkaat turvallisuustoimenpiteet tehtyä ja riskitaso pidettyä matalalla, mikä on myös hyvää jatkuvuuden hallintaa. Riskienhallintaprosessia tulee ylläpitää ja seurata, jotka kuuluvat erikseen nimettävälle vastuuhenkilölle.

Kun riskien arviointia on tehty, tulee viimeistään selvittää raportointikäytännöt, mikäli organisoinnissa tätä ei ole huomioitu. Oleellista on, miten turvallisuuspäällikkö raportoi ylimmälle johdolle, miten henkilöstö raportoi johdolle ja miten henkilöstölle raportoidaan. Raportointi on turvallisuuspäällikön ja henkilöstön väline jakaa ylimmälle johdolle tietoa päätöksenteon tueksi, joten raportointi on myös kiinteä osa viestintää, joka tulisi myös aloittaa järjestelmällisesti. Viestintä pitää sisällään lakisääteisiä velvollisuuksia esimerkiksi pelastussuunnitelman ja muiden turvallisuusdokumenttien tiedottamisesta, mutta viestintä on myös väline, jolla voidaan kehittää turvallisuuskulttuuria lisäten ammattikorkeakoulun jäsenien turvallisuustietoisuutta ja sitoutuneisuutta turvallisuuteen. Tiedon liikkuessa tulee myös aloittaa turvallisuuden ja riskien seuranta, jotta voidaan reagoida muutoksiin ja selvittää toimenpiteiden vaikutus toimintaan ja tavoitteisiin. Kun raportteja ja tietoa liikkuu, tulisi myös olla tietoisia, miten seurantaa ja mittaamista toteutetaan.

Turvallisuuden lakisääteisiä vaatimuksia pitäisi alkaa tunnistaa ja tähän tulisi nimetä myös vastuuhenkilö. Osana lakisääteisiäkin vaatimuksia, tulisi turvallisuuden systemaattista dokumentointia aloittaa suunnittelemaan ja toteuttamaan. Käytännössä ammattikorkeakoululla tulisi olla pelastussuunnitelma, joka on yksi ohjaava dokumentti, mutta järjestelmällisessä turvallisuusjohtamisessa dokumentoinnilla katetaan myös paljon vaatimusten mukaisia velvoitteita. Lisäksi turvallisuuden suunnittelu tulisi olla aina dokumentoitua ja selkeästi jäsenneltyä. Vaatimuksia on paljon ja jokaisen ammattikorkeakoulun täytyy tunnistaa oma keskeinen, velvoittava, lainsäädäntö. Esimerkiksi Arcada (2017) huomio paljon teknistä lainsäädäntöä, joka liittyy koulun erikoistiloihin. Sähköturvallisuuslaki (L410/1996) ja Kemikaalilaki (599/2013) säätelevät hyvin paljon Arcadan kemikaalilaboratorion ja sähkölaboratorion työskentelyä yleisesti sekä turvallisuusvaatimuksia (Arcada 2017).

Jatkuvuuden hallintaprosessi tulisi aloittaa, jotta ammattikorkeakoulun toiminta voidaan varmistaa kaikissa tilanteissa. Keskeistä on vaikutusanalyysin, liiketoiminta-analyysin, hyödyntäminen, jotta saadaan tietoa organisaation kriittisistä prosesseista, niihin vaikuttavista tekijöistä, resursseista, joita hyödynnetään tällä hetkellä ja joita tarvitaan lisää. Tärkeää on myös, että tiedetään, miten organisaatio pystyy toipumaan häiriöstä ja palauttamaan toiminta määritellylle tasolle tietyn ajan sisällä. Tämä on osittain myös lakisääteistä, sillä Ammattikorkeakoululaki (932/2014) vaatii ammattikorkeakoulua varautumaan poikkeustilanteisiin. Tärkeämpää olisi kuitenkin nähdä, miten normaaleissa oloissa pystytään varmistamaan toiminnan jatkuvuus. Jatkuvuuden hallinta perustuu riskien arviointiin ja hallintakeinojen hyödyntäminen, jotta häiriöihin voidaan systemaattisesti varautua sekä kyetään vähentämään keskeytyksiä ja niiden seurauksia häiriötilanteissa. Jatkuvuuden hallinta on kattava ja vaativakin prosessi, jota tulee ylläpitää ja seurata resurssien mahdollistamalla tavalla.

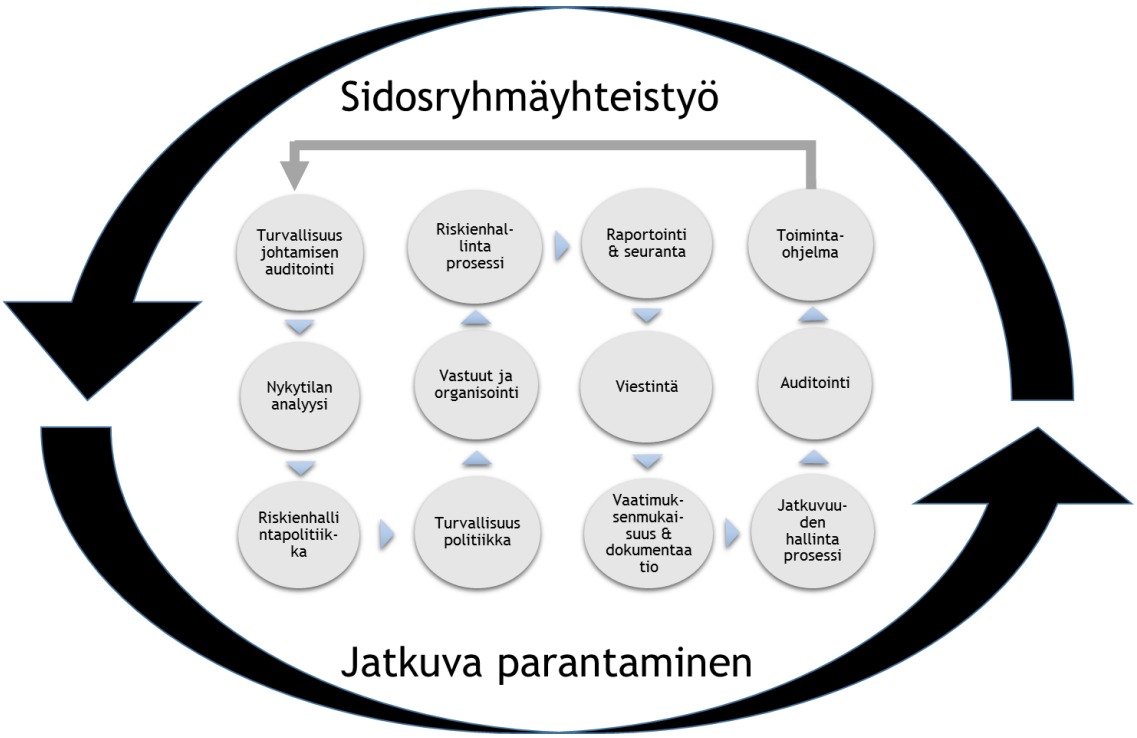
Ammattikorkeakoulu kohtaa erilaisia tarkastuksia, jotka liittyvät rahoitukseen, koulutukseen, laadunhallintaan ja toimintaan ylipäätänsä. Erityisesti laadunhallinnan välineenä turvallisuustarkastukset, auditoinnit, selvittävät miten oikeasti toimitaan. Palotarkastukset ja työsuojeluviranomaisten tarkastukset ovat lakisääteisiä tietoa antavia välineitä, joita tulisi hyödyntää turvallisuustoiminnan mittaamisessa ja raportoinnissa. Käytännössä tässä mallissa esitettynä turvallisuustarkastuksilla viitataan omaehtoiseen, sisäiseen tarkastustoimintaan, jolla pyritään laadunhallintaan ja vaatimuksenmukaisuuksien täyttämiseen. Tarkastukset kuuluvat linjaorganisaatiolle ja esimerkiksi turvallisuusvastuullisille esimiehille, joille turvallisuuspäällikkö antaa ohjausta ja tukea. Käytännössä laajempaa, kaikkien tilojen turvallisuustoimintaa voi esimerkiksi turvallisuuspäällikkö myös auditoida. Tärkeämpää on, että tarkastuksen kohteet ovat organisaation kaikki tasot kattavia, säännöllisiä ja ne tehdään dokumentoidusti, jotta niistä saatavaa tietoa voidaan hyödyntää toiminnan kehittämisessä. Erilaiset koko organisaatiolle tarkoitetut kyselyt voivat myös toteuttaa esimerkiksi vuosittain. Kaiken tarkastustoiminnan tulee joka tapauksessa olla järjestelmällistä ja auditointi -prosessi aloitetaankin systemaattisen tarkastussuunnitelman laadinnalla, johon johto antaa tukensa ja myöntää resurssit.

Riskien arvioinnin ja muiden tietojen perusteella laaditaan turvallisuuden toimintaohjelma, jossa määritellään turvallisuusjohtamisen toimenpiteet, niiden suunnittelun ja toteuttamisen aikataulu sekä toimenpiteiden vastuutoimijat ja muut toimenpiteet. Olennaista on, että toimenpide johdetaan riskitasosta ja arvioiduista riskeistä sekä lainsäädännön vaatimuksista. Tärkeintä on kuitenkin, että ylin johto myöntää ajalliset ja rahalliset resurssit ohjelman läpiviemiseen, jolloin rahalliset resurssit tulisikin kuvata konkreettisesti esimerkiksi vuosibudjettina. Ohjelmalla itsellään tulee olla johdon täysi tuki ja hyväksyntä, jotta ohjelma voidaan laatia. Tutor max -auditoinnissa määritellään tavoitetaso jokaiselle arvioitavalle kohteelle 3-4 vuoden päähän ja tämä asettaa selkeän pohjan myös turvallisuuden toimintaohjelmalle, joka tulisi asettaa organisaatiosta riippuen 3-5 vuoden ajanjaksolle. Tähän vaikuttaa myös yleisesti organisaation strategia, strateginen johtaminen ja ohjelman tulisikin olla yhdenmukainen strategian sekä yleisten toimintaohjelmien kanssa.

Toimintaohjelman päätyttyä tai loppuvaiheessa tulisi suorittaa laajempi turvallisuusjohtamisen auditointi, esimerkiksi Tutor max -mallilla, jotta voidaan nähdä toimenpiteiden vaikutus. Näin turvallisuusjohtamisjärjestelmän luominen voidaan kuvata prosessina, jossa useat eri prosessit ovat systemaattisesti johdettuja ja kehittäminen jatkuvaa. Turvallisuusjohtamisjärjestelmään yltäminen riippuu lukuisista eri tekijöistä, joista resursointi on tärkein.

Turvallisuusjohtamisjärjestelmän luomisen voi hahmottaa askeleittain tapahtuvana prosessina, joka sisältää useita eri prosesseja, jotka tulee aloittaa ja ylläpitää, jotta turvallisuusjoh-

tamisjärjestelmän päämäärä voitaisiin saavuttaa. Kuvio 4 hahmottaa, miten turvallisuusjohtamisjärjestelmää aletaan luoda erilaisia prosesseja hallinnoimalla. Eri pallot kuvastavat prosesseja, joissa tulee noudattaa jatkuvan parantamisen periaatteita ja tehdä tiivistä sidosryhmäyhteistyötä.

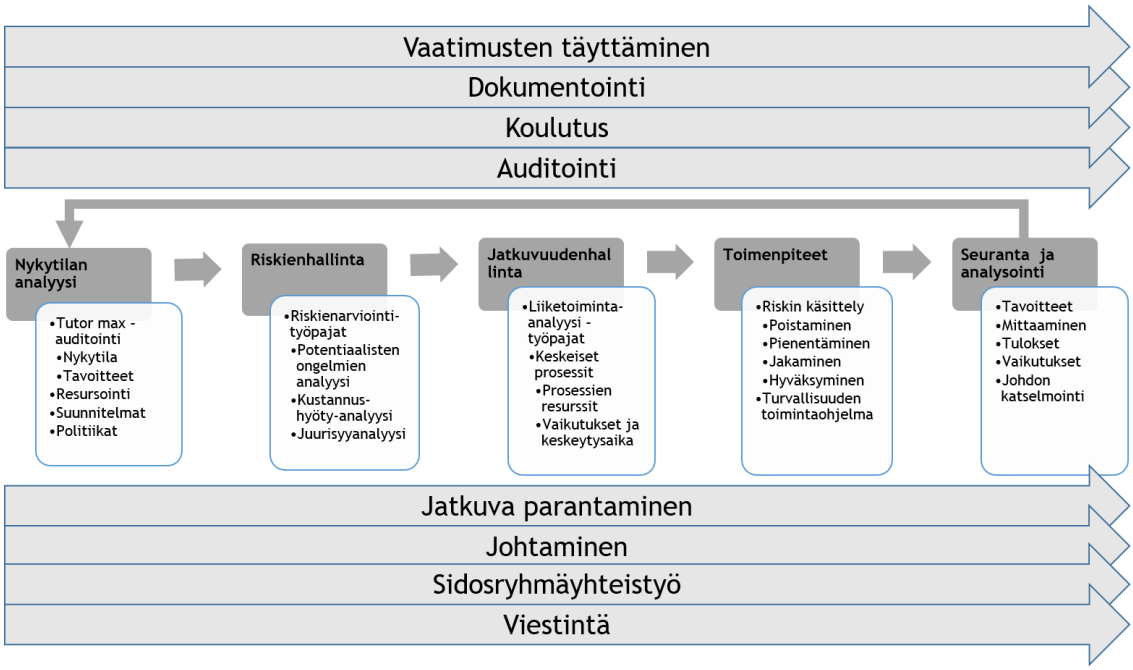


Kuvio 4: Turvallisuusjohtamisjärjestelmän luominen

Mallissa on tärkeintä, että kaikki toiminta tukee jatkuvan parantamisen periaatteita, koska tällöin voidaan varmistaa, että prosessit eivät pysähdy tai keskeydy. Olennaista on tällöin, että kaikki prosessit ovat johdettuja ja vastuutettu. Sidosryhmäyhteistyö on erityisen tärkeää jatkuvan parantamisen lisäksi, jotta kaikki ammattikorkeakoulun jäsenet saadaan sitoutuneiksi turvallisuuteen. Koko ammattikorkeakouluyhteisö tulee ottaa mukaan turvallisuuden kehittämiseen, jotta voidaan varmistua ammattikorkeakoulun turvallisuuskulttuurin kehittämisestä, joka heijastuu suoraan myös turvallisuusjohtamisjärjestelmän luomiseen.

Turvallisuusjohtamisjärjestelmän luominen voidaan hahmottaa myös riskienhallinnan, turvallisuusjohtamisen ja jatkuvuudenhallinnan näkökulmista erilaisina riskien arviointimenetelminä, jotka suoritetaan nykytilan analysoinnin ja toimintaympäristön määrittelemisen jälkeen (kuvio 5). Mallilla halutaan painottaa riskien arvioinnin ja erityisesti työpaja -keskeisten riskien arviointimenetelmien käyttöä, joilla tulokset ovat todennäköisesti erittäin hyviä, kun menetelmät suunnitellaan ja toteutetaan systemaattisesti, osaavassa johdossa ja oikeilla kokoonpanoilla. Resurssit ratkaisevat, sillä riskien arviointia tulee suorittaa jatkuvasti, jotta tiedetään mihin

organisaation tulisi keskittää toimenpiteensä. Näin toiminnasta saadaan myös samalla resurssitehokasta, koska tiedetään mitä lähteä kehittämään sen sijaan, että tehtäisiin asioita sirpalemaisesti ilman selkeitä tavoitteita.



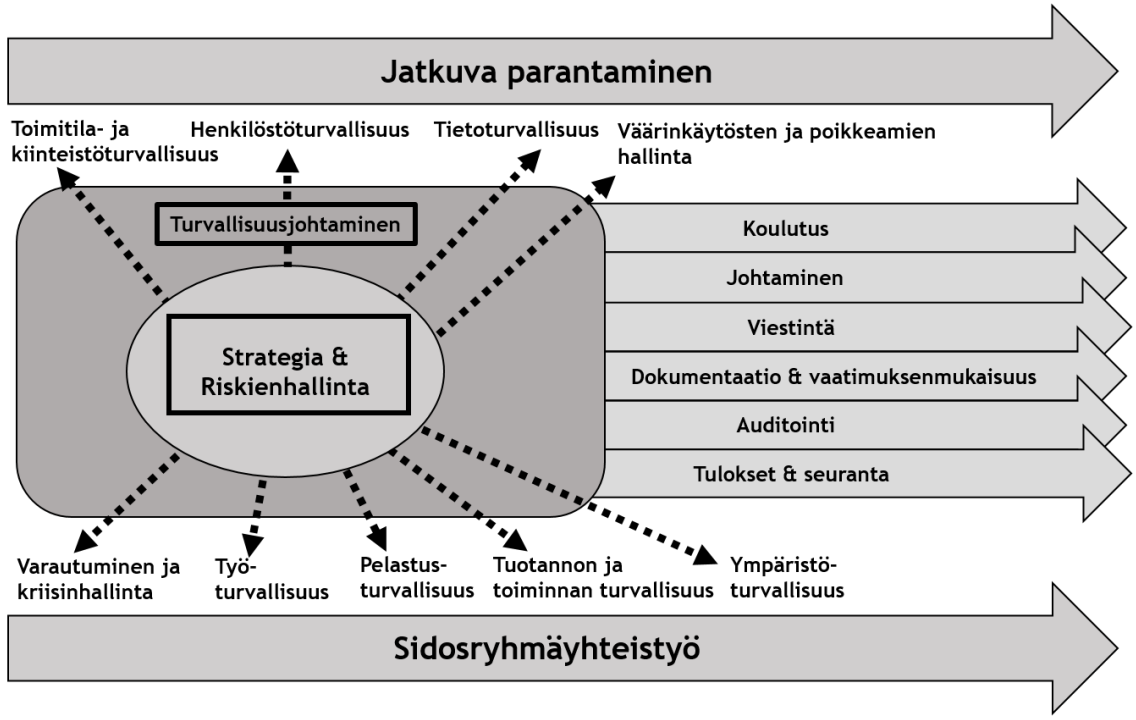
Kuvio 5: Turvallisuusjohtamisjärjestelmän luominen menetelmäkeskeisesti

Malliin on nostettu keskeisimmiksi työpaja -menetelmiksi potentiaalisten ongelmien analyysi, kustannus-hyöty-analyysi, juurisyyanalyysi, liiketoiminta-analyysi ja nykytilan analyysiksi Tutor max -arviointimenettely. Nämä menetelmät ovat lähtökohtaisesti laadullisia ja sopivat ammattikorkeakouluympäristöön hyvin. Ammattikorkeakoulun laadukas toiminta perustuu opetus- ja tutkimustyön mahdollistaviin asiantunteviin henkilöihin, joita kannattaa hyödyntää riskien arvioinnissa. Henkilöstöllä on kattavasti tietoa erilaisista tekijöistä, jotka voivat vaarantaa toimintaa ja jatkuvuutta korkeakoulussa. Riskien arviointityöpaja on erinomainen väline keräämään tietoa henkilöstöltä, joka ei muuten välttämättä osaisi tuoda järjestelmällisesti esille havaintojaan ja tietojaan. Riskien arvioinnilla saadaan myös vahvistettua henkilöstön turvallisuustietoisuutta ja koulutettua henkilökuntaa tunnistamaan erilaisia riskin lähteitä ja riskejä.

Menetelmäkeskeisesti kuvattuna saadaan myös yhdistettyä riskienhallinnan ja turvallisuusjohtamisen näkökulmat. Molempiin kuuluu olennaisesti toimintaympäristön määritteleminen tai nykytilan analyysi. Tärkeintä on kuitenkin hahmottaa, miten riskienhallinnalla vaikutetaan turvallisuusjohtamiseen erilaisilla menetelmillä, jotka tarjoavat tietoa kehittämistä vaativista toiminnoista ja prosesseista. Riskin käsittely koostuukin suurimmaksi osaksi riskin vähentämi-

sestä ja poistamisesta, joita toteutetaan turvallisuusjohtamisella. Turvallisuuden toimintaohjelma kokoaa jäsennellysti ja systemaattisesti kaikki turvallisuusjohtamisen toimenpiteet, joita aletaan suunnitella ja toteuttaa ohjelman mukaisesti. Ohjelma perustuu siten riskien arvioinnin tuloksiin, riskitason ylittävien riskien käsittelemiseen. Riskejä ja toimenpiteitä myös seurataan jatkuvasti ja muutoksiin reagoidaan tarvittaessa. Toimintaohjelman aikana suoritetaan jatkuvasti myös riskien arviointia, jonka tuloksista johdetaan tai muutetaan toimintaohjelman sisältöä. Toimintaohjelman jälkeen on perusteltu aika uudelle kokonaisvaltaiselle turvallisuusjohtamisen auditoinnille ja kattavammalle riskien arvioinnille. Näin malli toimii jatkuvan kehittämisen mukaisesti.

Kokonaisvaltainen turvallisuusjohtamisjärjestelmä huomioi turvallisuusjohtamisen kaikki osa-alueet. Jokainen osa-alue tulisi huomioida, mutta riskien arviointi määrittää, mitkä osa-alueet korostuvat organisaation toiminnassa erityisesti. Kokonaisvaltaista turvallisuusjohtamisjärjestelmää voidaan hahmottaa (kuvio 6) siten, että organisaation strategia ja riskienhallinta ohjaavat turvallisuusjohtamista. Turvallisuusjohtaminen ohjaa taas osa-alueita, joiden vastuu ja toteutus kuuluvat linjaorganisaatiolle.



Kuvio 6: Turvallisuusjohtamisjärjestelmä

Prosessikuvauksessa riskienhallinnan ja turvallisuusjohtamisen mahdollistamia kriittisiä prosesseja ovat, koulutus, johtaminen, viestintä, dokumentaatio, vaatimuksenmukaisuuden seuranta, auditointi, tulokset ja seuranta. Tärkeimmät prosessit kokonaisvaltaisuuden kannalta kiteytyvät kuitenkin sidosryhmäyhteistyöhön ja jatkuvaan parantamiseen. Sidosryhmäyhteistyö on erityisen tärkeää ammattikorkeakoulun turvallisuusjohtamisjärjestelmän kannalta,

koska se mahdollistaa koulun turvallisuuskulttuurin kehittämisen ja sen, että seuranta kattaa kaikki toiminnot ja prosessit, jotka liittyvät ammattikorkeakoulun toimintaan. Näin ennaltaehkäistään tilanne, jossa merkittävän tai sietämättömän riskin olemassaoloa ei tunnisteta eikä siihen varauduta. Pahimmassa tapauksessa riski myös toteutuu aiheuttaen merkittävät henkilövahingot, taloudelliset vahingot tiloille ja omaisuudelle tai toiminnan keskeytymisen.

Turvallisuusjohtamisjärjestelmä luodaan korkeakouluun systemaattisella riskienhallinnalla, resursoinnilla, organisoinnilla ja turvallisuusjohtamisella, joka kattaa kaikki turvallisuusjohtamismallin osa-alueet, riskiperusteisesti. Turvallisuusjohtamisjärjestelmä luodaan ammattikorkeakoulun strategian mukaisesti ja se tuodaan osaksi normaalia korkeakoulun johtamista. Kuten muissakin organisaatioissa, ylin johto ratkaisee lopulta ammattikorkeakoulun turvallisuusjohtamisen kehittämisestä ja turvallisuusjohtamisjärjestelmän luomisesta. Olennaista on kuitenkin, että vaikka ammattikorkeakoulun tavoitteena ei olisikaan turvallisuusjohtamisjärjestelmä, kaikkea turvallisuusjohtamista voidaan alkaa kehittää systemaattisesti riskien arvioinnilla.

10.1 Yhteenveto kehittämishankkeesta

Turvallisuusjohtamisjärjestelmän luominen on ollut jatkumona Arcadan turvallisuuden kokonaisvaltaiselle kehittämiselle, joka on alkanut joulukuussa 2015 Tutor max –auditoinnilla. Kehittäminen jatkuu edelleen. Vuoden 2017 aikana Arcadassa tullaan asettamaan turvallisuuden toimintaohjelma, joka sisältää turvallisuusjohtamisen kehittämistoimenpiteet tuleville vuosille. Tavoitteena on, että Arcadassa yllettäisiin muutaman vuoden kuluttua Tutor max –auditoinnissa johdon määrittelemälle tahtotasolle, joka on jokaisessa arviointikohdassa vähintään perustasossa. Vastaavasti turvallisuusjohtamisjärjestelmän tavoiteaikaa ei tulla määrittelemään tarkasti, vaan tavoite on, että turvallisuusjohtamista kehitetään systemaattisesti kohti turvallisuusjohtamisjärjestelmää. Turvallisuuden toimintaohjelman jälkeen tullaan suorittamaan kokonaisvaltainen turvallisuusauditointi, esimerkiksi Tutor max -menettelyllä, jonka jälkeen asetetaan uudet tavoitteet ja toimenpiteet seuraavaan toimenpideohjelmaan. Turvallisuusjohtamisen kehittäminen on siis jatkuvaa. (Arcada 2017.)

Opinnäytetyössä luodaan vahva teoriaperusta riskienhallinnasta, turvallisuusjohtamisesta ja erityisesti turvallisuusjohtamisjärjestelmän toiminnoista ja prosesseista. Teoria yhdistetään tiedonkeruumenetelmiin, erityisesti benchmarkingiin, jotta on saatu tietoa mitä useamman vuoden turvallisuusjohtamista kehittänyt organisaatio on tehnyt luodessaan turvallisuusjohtamisjärjestelmää. Benchmarkingin suurin hyöty on saavutettu, kun on saatu tietoa, millä periaatteilla ja puitteilla useita vuosia turvallisuusjohtamista systemaattisesti kehittänyt ammattikorkeakoulu on lähestynyt turvallisuusjohtamisjärjestelmän luomista. Laurean turvallisuus-

johtamisen tuloksista ja vaiheiden tarkastelusta on myös saatu tärkeää tietoa, miten järjestelmän voi suunnitella ja toteuttaa systemaattisesti. Haastatteluilla on saatu tietoa Arcadan ja Metropolian turvallisuustoiminnasta sekä toiminnan periaatteista, puitteista ja tavoitteista. Haastattelut kohdistuivat koulujen turvallisuuspäälliköihin, jotka ovat erittäin sopivia haastateltavia organisaation turvallisuusjohtamisesta ja riskienhallinnasta. Haastattelut tarjosivat myös hyvin yksityiskohtaista tietoa siitä, mitä ammattikorkeakoulun toiminta oikeastaan on ja miten turvallisuus liittyy ammattikorkeakoulun toimintaan sekä miten turvallisuutta johdetaan muuhun johtamiseen verrattuna.

10.2 Toimenpide-ehdotukset

Arcada on saanut tämän opinnäytetyön perusteella toimenpide-ehdotukset, jotka tulisi huomioida turvallisuusjohtamisjärjestelmän luomisessa. Näihin sisältyy turvallisuusjohtamisjärjestelmän luomisen prosessiin, johdon rooliin ja tarpeisiin, riskienhallintaan, turvallisuusjohtamisen osa-alueisiin, johtamiseen, raportointiin ja seuraamiseen liittyviä tekijöitä. Opinnäytetyön tekijä on itse suunnittelemassa ja toteuttamassa kehitystoimia, jotka perustuvat tässä opinnäytetyössä esille tulleisiin tarpeisiin. Kaikki toimenpide-ehdotukset arvioidaan Arcadassa, ja osa ehdotuksista tulee mukaan turvallisuuden toimintaohjelmaan, joka ohjaa turvallisuusjohtamisjärjestelmän luomista.

Turvallisuusjohtamisen tärkeimmät toimenpide-ehdotukset perustuvat strategisiin ja hallinnollisiin toimenpiteisiin, erityisesti riskienhallinnan voimakkaaseen kehittämiseen. Olennaista on luoda sellaiset käytännöt, joilla voidaan varmistaa jatkuva kehittäminen ja sidosryhmien yhä vahvempi integroiminen korkeakoulun turvallisuustyöhön. Erilaisten koulutuksien, harjoituksien ja ohjeistuksien avulla pyritään ohjaamaan turvallisuukulttuuria ennaltaehkäisevään tilaan, joka on myös yksi turvallisuuspolitiikan tavoitteista (Arcada 2017).

10.3 Jatkotutkimukset

Luonnollinen jatkotutkimus opinnäytetyölle olisi turvallisuusjohtamisjärjestelmän kehittäminen ammattikorkeakoulussa perustuen tämän opinnäytetyön suunnitelmaan ja ehdotettuihin vaiheisiin. Vaihtoehtoisesti voitaisiin tutkia, miten turvallisuusjohtaminen jalkautetaan kaikille organisaation tasoille ammattikorkeakoulussa, sidosryhmät huomioon ottaen. Vastaavasti voitaisiin toteuttaa myös kvantitatiivinen tutkimus, jossa selvitettäisiin kyselyn avulla turvallisuusjohtamisen nykytasoa eri ammattikorkeakoulujen henkilökunnilta, turvallisuuspäälliköiltä ja johdoilta. Mielenkiintoista olisi myös tutkia ammattikorkeakoulun turvallisuuskulttuuria, asenteita, arvoja ja turvallisuustietoisuutta sekä näiden elementtien vaikutusta ammattikorkeakoulun johtamiseen.

10.4 Oman oppimisen arviointi

Opinnäytetyön tavoite oli selvittää, miten ammattikorkeakouluun luodaan turvallisuusjohtamisjärjestelmä. Toisena tavoitteena oli luoda todistettavasti hyödynnettävä malli, jota pystyisi soveltamaan vähintään suuntaa-antavasti turvallisuusjohtamisjärjestelmän luomisessa suomalaisessa korkeakoulussa. Yhtä tärkeä tavoite oli tuottaa työn tilaajaorganisaatiolle, tekijän työnantajalle, selkeä suunnitelma, jota on helppo lähteä toteuttamaan. Suunnitelmaan sisältyi myös erilliset toimenpide-ehdotukset, joita tullaan sisällyttämään turvallisuuden toimintaohjelmaan. Suunnitelman onnistumista arvioi lähtökohtaisesti Arcadan johto, joka päättää lopullisista toimenpiteistä. Suunnitelman tekemisessä hyödynnettiin erityisesti teoriaa ja tiedonkeruumenetelmiä. Myös toimenpide-ehdotukset ovat linjassa teorian ja menetelmien kanssa. Menetelmät tukivat erittäin hyvin suunnitelman luomista, koska haastateltavilla oli selkeä ja teoriaan perustuva näkemys turvallisuusjohtamisesta ammattikorkeakoulussa.

Voisi todeta, että oppimista tapahtui opinnäytetyön aikana huomattavasti, koska lopputuloksena saatiin johtopäätöksissä kuvaillut mallit turvallisuusjohtamisjärjestelmästä ja sen luomisen prosessista. Tärkeintä oppimista tapahtui todennäköisesti riskienhallinnan ja turvallisuusjohtamisen periaatteiden ja puitteiden selvitystyössä, johon myös johtopäätöksissä kuvaillut mallit pohjautuvat. Kattava teoriatieto perustui osittain onnistuneeseen tiedonhankintaan, mutta suuri osa lähteistä on johdettu jo aikaisemmin opinnoista. Opinnäytetyö antoi myös erittäin hyvät puitteet jatkaa turvallisuuden kehittämistyötä Arcadassa, jolla on erinomainen mahdollisuus saavuttaa turvallisuusjohtamisen tavoitteensa ja päämääränsä, turvallisuusjohtamisjärjestelmä.

Lähteet

Painetut lähteet

Aaltola, J. & Valli, R. 2001. Ikkunoita tutkimusmetodeihin II. Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. Jyväskylä: PS-kustannus.

Airaksinen, T. & Vilkka, H. 2003. Toiminnallinen opinnäytetyö. Jyväskylä: Tammi.

Booth, R. T. & Lee, T. R. 1995. The role of human factors and safety culture in safety management. Journal of Engineering Manufacture, 393-400.

Flink, A., Reiman, T. & Hiltunen, M. 2007. Heikoin lenkki? Riskienhallinnan inhimilliset tekijät. Helsinki: Edita.

Hirsjärvi, S. & Hurme, H. 2014. Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Tallinna: Gaudeamus.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. uudistettu painos. Helsinki: Tammi.

Hopkin, P. 2014. Fundamentals of risk management. 3. painos. Lontoo: KoganPage.

Hopkins, A. 2000. Lessons from Longford. The Esso gas plant explosion. Sydney: CCH.

Huumonen, T., Paasonen, L. & Paasonen, J. (toim.) 2012. Helsinki: Tietosanoma.

Hämäläinen, J. 1987. Laadullinen sosiaalitutkimus käytännössä. Johdatus sosiaalitutkimuksen ”käsitetyötaitoon”. Kuopion yliopiston julkaisuja. Yhteiskuntatieteet. Tilastot ja selvitykset 2/1987. Kuopio: Kuopion yliopisto.

Kerko, P. 2001. Turvallisuusjohtaminen. Porvoo: PS-kustannus.

Kirwan, B. 1996. Safety management assessment and task analysis – a missing link? Teoksessa Hale, A. & Baram, M. 1998. Safety management: the challenge of change. Netherlands: Pergamon.

Koskenranta, H., Paasonen, J. & Ranta, T. 2012. Kansainvälinen selvitys korkeakoulujen turvallisuusjohtamisesta. Espoo: Laurea-ammattikorkeakoulu.

Koskenranta, H. 2012. Turvallisuusjohtamisen standardien kartoitustyöstä. Teoksessa Koskenranta, H., Paasonen, J. & Ranta, T. 2012. Kansainvälinen selvitys korkeakoulujen turvallisuusjohtamisesta. Espoo: Laurea-ammattikorkeakoulu.

Laitinen, H., Vuorinen, M. & Simola, A. 2013. Työturvallisuuden ja -terveyden johtaminen. Helsinki: Tietosanoma.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio. Helsinki: Talentum.

Levä, K. 2003. Turvallisuusjohtamisjärjestelmien toimivuus: vahvuuden ja kehityshaasteet suuronnettomuusvaarallisissa laitoksissa. Väitöstutkimus. TUKES –julkaisu 1/2003. Helsinki: TUKES.

Martikainen, S. 2016a. Development and effect analysis of the Asteri consultative auditing process – safety and security management in educational institutes. Väitöskirja. Lappeenranta: Lappeenrannan teknillinen yliopisto.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. 3. uudistettu painos. Helsinki: Sanoma pro.

Ortmeier, P. 2005. Security management: An introduction. New jersey: Pearson Prentice Hall.

Reason, J. & Hobbs, A. 2003. Managing maintenance error. A practical guide. Hampshire: Ashgate.

Reason, J. 1997. Managing the risks of organizational accidents. Aldershot: Ashgate.

Reiman, T. & Oedewald, P. 2008. Turvallisuuskriittiset organisaatiot. Onnettomuudet, kulttuuri ja johtaminen. 1.painos. Helsinki: Edita.

Sarajärvi, A. & Tuomi, J. 2009. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.

Schein, E. 2004. Organizational culture and leadership. 3.painos. San Francisco: Jossey-Bass.

SPEK. 2014. Kokonaisturvallisuuden sanasto. Helsinki: Suomen pelastusalan keskusjärjestö SPEK.

Vellani, K. 2007. Strategic security management. London: Butterworth-Heinemann.

Whitman, M. & Mattord, H. 2016. Management of information security. 5th edition. Boston: Cengage learning.

Sähköiset lähteet

A-vakuutus. 2017. Paloturvallisuus. Luettu 26.2.2017. https://www.a-vakuutus.fi/a-vakuutus/henkiloliikenne/riskienhallinta/omaisuus-ja-toiminta/paloturvallisuus?id=521412&srcpl=8

AHRQ. 2017. Potential problem analysis. Luettu 14.2.2017. https://healthit.ahrq.gov/health-it-tools-and-resources/workflow-assessment-health-it-toolkit/all-workflow-tools/potential-problem-analysis

ASQ. 2016. Continuous improvement. Luettu 2.12.2016. http://asq.org/learn-about-quality/continuous-improvement/overview/overview.html

Arcada. 2016. Tietoa meistä. Luettu 28.11.2016. https://www.arcada.fi/fi/tietoa-arcadasta

Edilex. 2016. Suomen rakentamismääräyskokoelma. Luettu 13.3.2017. https://www.edilex.fi/rakentamismaaraykset

Elinkeinoelämän keskusliitto. 2017. Yritysturvallisuus. Luettu 17.2.2017. https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

FEMA. 2014. Business impact analysis worksheet. Viitattu 14.12.2016. https://www.fema.gov/media-library/assets/documents/89526

Huoltovarmuuskeskus. 2017. Jatkuvuudenhallinta. Viitattu 25.2.2017. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/

Martikainen, S. (toim.) 2016b. Varautuva, turvallinen koulu. Laurea-ammattikorkeakoulu. Luettu 26.2.2017. http://www.theseus.fi/bitstream/handle/10024/119138/Laurean%20julkaisut%2070.pdf?sequence=1

Opetus- ja kulttuuriministeriö. 2017. Viitattu 23.2.2017. http://www.minedu.fi/OPM/Koulutus/koulutuspolitiikka/Hankkeet/rakenteellinen_kehittaminen/

Real, K. & Cooper, M. 2009. The importance of communication factors to safety climate: an exploratory analysis. Paper presented at the annual meeting of the International Communication Association, Marriott, Chicago, IL 21.5.2009. Viitattu 4.3.2017. http://citation.allacademic.com//meta/p_mla_apa_research_citation/2/9/9/1/4/pages299149/p299149-1.php

Suojelupoliisi. 2017. Henkilöturvallisuusselvitys. Viitattu 21.2.2017. http://www.supo.fi/turvallisuusselvitykset/henkiloturvallisuusselvitys

Suomen Riskienhallintayhdistys. 2017a. Potentiaalisten ongelmien analyysi. Viitattu 2.2.2017. http://www.pk-rh.fi/index.php?page=poa-analyysi

Suomen Riskienhallintayhdistys. 2017b. Riskienhallintapolitiikka. Viitattu 23.2.2017. http://riskikompassi.fi/riskienhallintaprosessi/riskienhallintapolitiikka

Suomen Riskienhallintayhdistys. 2017c. Riskienhallintaprosessin kuvaus. Viitattu 23.2.2017. http://riskikompassi.fi/riskienhallintaprosessi/prosessin-kuvaus

Säteilyturvakeskus. 2017. Turvallisuuskulttuuri. Viitattu 26.2.2017. http://www.stuk.fi/stuk-valvoo/sateilyn-kayttajalle/sateilytoiminnan-turvallisuus/sateilylaitteet-ja-laadunvalvonta/turvallisuuskulttuuri

Tietosuojavaltuutetun toimisto. 2017. Miten valmistautua EU:n uuteen tietosuoja-asetukseen? -Opas. http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/SFk6eA7R1/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Valtiovarainministeriö. 2003. Potentiaalisten ongelmien analyysi teoksessa Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Viitattu 1.3.2017. https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10128

Valtiovarainministeriö. 2016. Toiminnan jatkuvuuden hallinta. Viitattu 25.2.2017. https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229

Lait ja asetukset

Ammattikorkeakoululaki 932/2014. Viitattu 3.12.2016. http://www.finlex.fi/fi/laki/ajantasa/2014/20140932

Henkilötietolaki 523/1999. Viitattu 3.3.2017. http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Kemikaalilaki 599/2013. Viitattu 23.2.2017. http://www.finlex.fi/fi/laki/ajantasa/2013/20130599

Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 679/2016. Viitattu 3.3.2017. http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=FI

Laki yksityisyyden suojasta työelämässä 759/2004. Viitattu 21.2.2017. http://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Pelastuslaki 379/2011. Viitattu 26.2.2017. http://www.finlex.fi/fi/laki/ajantasa/2011/20110379

Suomen perustuslaki 731/1999. Viitattu 23.2.2017. http://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Sähköturvallisuuslaki 1135/2016. Viitattu 23.2.2017. http://www.finlex.fi/fi/laki/ajantasa/2016/20161135

Turvallisuusselvityslaki 726/2014. Viitattu 21.2.2017. http://www.finlex.fi/fi/laki/ajantasa/2014/20140726

Työsopimuslaki 55/2001. Viitattu 3.3.2017. http://www.finlex.fi/fi/laki/ajantasa/2001/20010055

Työturvallisuuslaki 738/2002. Viitattu 3.12.2016. http://www.finlex.fi/fi/laki/ajantasa/2002/20020738

Valtioneuvoston asetus pelastustoimesta 407/2011. Viitattu 26.2.2017. http://www.finlex.fi/fi/laki/ajantasa/2011/20110407

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010. Viitattu 1.3.2017. http://www.finlex.fi/fi/laki/ajantasa/2010/20100681

Ympäristöministeriön asetus rakennusten paloturvallisuudesta 3/2011. Viitattu 21.4.2017. https://www.edilex.fi/data/rakentamismaaraykset/e1_2011.pdf

Standardit

BS 8800: 2004. British Standards Institution. Occupational health and safety management systems. Guide.

ISO 22320: 2011. Societal security- Emergency management -requirements for incident response. International Organization for Standardization. Geneva.

OHSAS 18001: 2007. Työterveys- ja työturvallisuusjohtamisjärjestelmät - vaatimukset. Suomen standardisoimisliitto. Helsinki.

SFS-EN 22301: 2014. Yhteiskunnan turvallisuus - liiketoiminnan jatkuvuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto. Helsinki.

SFS-EN 31010: 2013. Riskienhallinta - riskien arviointimenetelmät. Suomen standardisoimisliitto. Helsinki.

SFS-EN 9001: 2015. Laadunhallintajärjestelmät - vaatimukset. Suomen Standardisoimisliitto. Helsinki.

SFS-EN ISO 14001: 2015. Ympäristöjärjestelmät – vaatimukset ja niiden soveltamisohjeita. Suomen standardisoimisliitto. Helsinki.

SFS-IEC 60300-3-9: 2000. Luotettavuusjohtaminen osa 3: käyttöopas. Luku 9: teknisten järjestelmien riskianalyysi. Suomen Standardisoimisliitto. Helsinki.

SFS-ISO 31000: 2011. Riskienhallinta - periaatteet ja ohjeet. Suomen Standardisoimisliitto. Helsinki.

SFS-ISO/IEC 27001: 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto. Helsinki.

SFS-opas 73: 2011. Riskienhallinta - sanasto. Suomen Standardisoimisliitto. Helsinki.

Julkaisemattomat lähteet

Arcada. 2017. Turvallisuusjohtamisen käsikirja. Viitattu 26.2.2017.

Hyvönen, A. 2017. Metropolia-ammattikorkeakoulu. Turvallisuuspäällikön haastattelu 2.3.2017. Helsinki.

Höök, K. 2016. Avainhenkilöiden hallinta -luento 12.10.2016. Laurea-ammattikorkeakoulu. Espoo.

Martikainen, S. & Ranta, T. 2015. Tutor-arvioinnin tulokset – Ammattikorkeakoulu Arcada 1.12.2015. Viitattu 2.1.2017.

Ranta, T. 2017. Laurea-ammattikorkeakoulu. Turvallisuusjohtajan haastattelu 6.2.2017. Vantaa.

Sjöberg, D. 2017. Arcada-ammattikorkeakoulu. Turvallisuuspäällikön haastattelu 8.3.2017. Helsinki.

Kuviot

Kuvio 1: Riskienhallintaprosessi 12
Kuvio 2: Turvallisuusjohtamisen malli 22
Kuvio 3: Tietoturvallisuuden perusarvot -kolmio..... 29
Kuvio 4: Turvallisuusjohtamisjärjestelmän luominen 62
Kuvio 5: Turvallisuusjohtamisjärjestelmän luominen menetelmäkeskeisesti 63
Kuvio 6: Turvallisuusjohtamisjärjestelmä 64

Taulukot

Taulukko 1: Liiketoiminta-analyysin panokset ja tuotokset 17
Taulukko 2: Seuraus-todennäköisyys riskimatriisi 19
Taulukko 3: POA-analyysin vaiheet 20
Taulukko 4: Riskien käsittelytoimenpiteet 45
Taulukko 5: Turvallisuusjohtamisjärjestelmän luominen - prosessien aloitukset 56

Liitteet

Liite 1: Arcadan turvallisuuspolitiikka 76
Liite 2: Arcadan liiketoiminta-analyysin haastattelukysymykset 77
Liite 3: Teemahaastattelukysymykset - ammattikorkeakoulujen turvallisuuspäälliköt 78
Liite 4: Ammattikorkeakouluun soveltuvia riskien arviointimenetelmiä 79

Liite 1: Arcadan turvallisuuspolitiikka

Säkerhetspolitik
Yrkeshögskolan Arcada Ab

Vision

Arcada är en säker och trygg högskola.

Principer

Inom Arcada upprätthåller och förbättrar vi alla säkerheten genom att följa lagar och instruktioner. Vi är skyldiga att meddela om iakttagna avvikelser och alla anmälningar beaktas och behandlas. Vårt säkerhetsarbete bygger på proaktivitet inom alla delområden.

Målsättningar

Säkerställande av kontinuiteten i undervisnings-, forsknings-, utvecklings- och administrationens verksamhet.
Mätare: Avbrott i verksamheten

Vi är ständigt medvetna om alla faktorer, som kan förorsaka avbrott i verksamheten
Mätare: Anmälningar om säkerhetsavvikelser

Vi strävar efter att fortgående utveckla säkerhetsarbetet i syfte att uppnå kontinuerlig förbättring.
Mätare: Upprättande av en årlig verksamhetsplan och uppföljning av denna

Vi är beredda på hot och avvikelser i vår säkerhetsverksamhet
Mätare: Beredskapsplaner, som grundar sig på riskbedömningar

Vår säkerhetsverksamhet baserar sig på riskbedömningar

Mätare: Riskregister

Alla på Arcada får ändamålsenlig introduktion och utbildning i säkerhetsfrågor

Mätare: Utbildningsregister

Liite 2: Arcadan liiketoiminta-analyysin haastattelukysymykset

Haastattelukysymykset

1) Mitä riskejä kohdistuu teidän osaston toiminnan jatkuvuuteen?
2) Mitkä ovat opetuksen ja tutkimustyön jatkuvuuden kannalta tärkeimmät tekijät teidän yksikön näkökulmasta?
3) Mitkä ovat opetuksen ja tutkimustyön jatkuvuuden kannalta tärkeimmät ja kriittisimmät prosessit tai toiminnot yksikössänne? Mitkä voisivat olla?
4) Mitä vaikutuksia tulee em. prosessien keskeytymisestä todennäköisesti? Mitä seurauksia vakavuudeltaan?
5) Mitä taloudellisia vaikutuksia?
6) Milloin häiriöllä olisi suurin vaikutus(ajankohta)?
7) Milloin toiminta voitaisiin saada palautettua normaalille tasolle?
8) Mikä on prosessin suurin hyväksyttävä keskeytysaika (MAO), jonka organisaatio kestäisi?
9) Mikä voisi olla prosessin toipumisaikatavoite (RTO) eli minkä ajan sisällä tietotekniikka ja erityislaitteet tulisi saada toimimaan häiriön tapahduttua?
10) Mitä resursseja löytyy tällä hetkellä, jotta opetus- ja tutkimustyö pystyvät jatkumaan normaalisti?
11) Mitä resursseja tarvitaan lisää, jotta opetus ja tutkimus pystyvät jatkumaan normaalisti, häiriöstä riippumatta?
12) Mitä resursseja voisi kannattavasti hyödyntää, jotta häiriön taloudelliset ja operatiiviset seuraukset olisivat mahdollisimman vähäiset?
13) Mitkä ovat tärkeimmät ulkoiset ja sisäiset sidosryhmät toiminnan palauttamisessa normaalille tasolle? Millainen on teidän yksikön riippuvuussuhde em. prosesseissa kyseisiin sidosryhmiin?

Liite 3: Teemahaastattelukysymykset - ammattikorkeakoulujen turvallisuuspäälliköt

Teemahaastattelukysymykset – riskienhallinta, turvallisuusjohtaminen ja turvallisuusjohtamis-järjestelmä

Riskienhallinta

- Kerro laajemmin organisaationne riskienhallinnasta?

Turvallisuusjohtaminen

- Kerro laajemmin organisaationne turvallisuusjohtamisesta?

Turvallisuusjohtamisjärjestelmä

- Mitä teidän turvallisuusjohtamisjärjestelmään sisältyy, millainen se on?
- Miten turvallisuusjohtamisjärjestelmänne on luotu vaihe vaiheelta?

Liite 4: Ammattikorkeakouluun soveltuvia riskien arviointimenetelmiä

Potentiaalisten ongelmien analyysi

Potentiaalisten ongelmien analyysi on vaarojen tunnistamismenetelmä, joka hyödyntää eri ammattiryhmien kokemusta ja osaamista. Analyysi perustuu ryhmässä tehtyyn aivoriiheen, jossa tunnistetaan vaaroja, arvioidaan riskejä ja tehdään toimenpide-ehdotuksia riskien käsittelemiseksi (Valtiovarainministeriö 2003, 70-71). Menetelmä soveltuu hyvin laajan kohteen, kuten työpaikan tai osaston keskeisten ongelma-alueiden selvittämiseen. Analyysi soveltuu hyvin myös teknisten järjestelmien ja ihmisten työtoiminnan arviointiin, koska siinä tunnistetaan ja luokitellaan vaaroja yleisellä tasolla. Taulukko 1 esittää järjestyksessään tehtävät vaiheet. (Suomen riskienhallintayhdistys 2017; Laitinen ym. 2013, 296-297.)

Vaihe	**Keskeiset tehtävät**
1. Valmistelu	Resurssit, johdon hyväksyntä, osallistujat ja vetäjä.
2. Vaarojen tunnistaminen	Hiljainen aivoriihi, rajaus, tavoitteet, vaarojen kirjaaminen ja avainsanat.
3. Järjestelmällinen arviointi	Keskustelumuotoinen aivoriihi, uusien vaarojen kirjaaminen, luettelointi ryhmittäin, kirjaaminen analyysin yhteenvetolomakkeille.
4. Vaaroista riskeiksi	Riskien todennäköisyyksien ja seurauksien vakavuuksien arviointi asteikolla 1-3.
5. Riskien käsittely	Toimenpide-ehdotuksien määrittäminen riskitason ylittäville riskeille. Ensisijaisesti ennaltaehkäiseviä toimenpiteitä.
6. Raportointi	Kaikki tuotetut dokumentit, kohteen kuvaus ja rajaus, johtopäätökset, yhteenveto ja jatkotoimenpiteet.

Taulukko 1: POA-analyysin vaiheet (Suomen riskienhallintayhdistys 2017a; AHRQ 2017)

Potentiaalisten ongelmien analyysin valmistelussa tulee huomioida, että analyysiin osallistuu eri asioista tietäviä henkilöitä, joilla on tietoa laadusta tai riskeistä. Mukana tulisi olla laitteiden tai tilojen päivittäisiä käyttäjiä, joilla on todennäköisesti paras tieto tarkasteltavista kohteista ja niihin liittyvistä riskeistä. Osallistujia tulisi olla vähintään kolme tai neljä. Lisäksi työpajalle tarvitaan osaava vetäjä, joka tuntee analyysin menetelmänä hyvin. Vetäjä ei saisi olla johtaja, ettei arvioitsijoiden kesken tule tunnetta siitä, että he eivät voi sanoa jotain, josta voi tulla seurauksia. Riittävät resurssit ja johdon hyväksyntä ovat vaatimuksena työpajalle, kuten riskien arvioinnille yleensäkin. Työpajaan tulisi olla vähintään kaksi tuntia käytettävissä ja häiriöttömät tilat. (Suomen riskienhallintayhdistys 2017; Valtiovarainministeriö 2003, 69-71.)

Työpajan vetäjä kertaa ennen ideointia vielä säännöt, joihin tulisi lukeutua ainakin kertaus rajauksesta ja työpajan tavoitteesta sekä kertoa, että tarkoitus ei ole syytellä tai selitellä vaan keskittyä asioihin ja ongelmiin eikä ihmisiin. Näin työpajassa säilyy avoin ilmapiiri. Työpaja alkaa hiljaisella aivoriihellä, jolloin jokainen osallistuja kirjoittaa lapuille ideoimiaan vaaroja. Laput kiertävät osallistujilta toisille, jolloin jokainen pääsee näkemään muiden ideoimia vaaroja. Vetäjän roolina on tällöin antaa avainsanoja osallistujille, kun vaarojen ideointi alkaa hidastua. (Suomen riskienhallintayhdistys 2017.)

Kun kirjoittaminen hidastuu, siirrytään keskustelumuotoiseen aivoriiheen, jossa osallistujat kertovat oman näkemyksensä ideoimistaan vaaroista. Tavoitteena on selvittää, ovatko vaarat todellisia, mitkä ovat niiden syyt ja seuraukset. Nämä kirjataan myös analyysin yhteenvetolomakkeille. Samalla yritetään löytää uusia vaaroja, lopuksi kaikki vaarat jaetaan ryhmiin esimerkiksi vaarojen syiden perusteella. (Suomen riskienhallintayhdistys 2017.)

Vaarat muunnetaan tämän jälkeen riskeiksi arvioimalla niiden seurauksien vakavuus ja todennäköisyys (taulukko 2) riskimatriisilla. Muita matriiseja voidaan käyttää myös. Esimerkkinä seuraus-hallinta-riskimatriisi, joka perustuu siihen, miten hyvin vaara hallitaan, todennäköisyyden arvioimisen sijasta. Riskiluku saadaan matriisista molemman nimittäjän perusteella, riippumatta kumpaa matriiseista käytetään. Yleisempi riskimatriisi on kuitenkin seurausten vakavuus-todennäköisyys-riskimatriisi, joka perustuu siihen, että todennäköisyys on yhdellä ja seurauksen vakavuus on toisella akselilla. (Suomen riskienhallintayhdistys 2017; Laitinen ym. 2013, 297-298; Valtiovarainministeriö 2003.)

Todennäköisyys	**Seurauksen vakavuus**		
	vähäiset	**haitalliset**	**vakavat**
epätodennäköinen	merkityksetön riski	vähäinen riski	kohtalainen riski
mahdollinen	vähäinen riski	kohtalainen riski	merkittävä riski
todennäköinen	kohtalainen riski	merkittävä riski	sietämätön riski

Taulukko 2: Seuraus-todennäköisyys riskimatriisi (SFS-EN 31010)

Seuraus-todennäköisyysmatriisi on keino yhdistää seuraus ja todennäköisyys riskitason tuottamiseksi. Potentiaalisten ongelmien analyysissä tunnistetaan todennäköisesti useita riskejä, joiden seulontaan matriisi soveltuu sen selvittämiseksi, mitkä riskit tarvitsevat tarkempaa analysointia. Matriisi soveltuu myös määrittämään, onko tietty riski yleisesti hyväksyttävä sen mukaan, missä se matriisissa sijaitsee. Menetelmän käyttämisessä on tärkeää, että matriisi on räätälöity olosuhteisiin ja toimintaympäristöön, jossa sitä käytetään. Menetelmä perustuu siihen, että molemmille, todennäköisyydelle ja seurauksen vakavuudelle räätälöidään asteikot, jotka kattavat erityyppiset seurausluokat ja jotka ovat niin yksiselitteisiä kuin olla ja voi. (SFS-EN 31010.)

Potentiaalisten ongelmien analyysi, kuten seuraus-todennäköisyysmatriisi ovat molemmat helppoja menetelmiä organisaatiolle, jolla ei välttämättä ole resursseja määrällisemmälle analyysille tai jolla ei ole riittävästi yksityiskohtaista tietoa analyysia varten. Toisaalta voi olla vaikeaa saada yhteen järjestelmä, joka soveltuu organisaation kaikkien olosuhteiden alueelle. Ongelmana on myös se, että riskejä ei pystytä yhdistämään, jolloin on tärkeätä hyvä vaaraluettelointi potentiaalisten ongelmien analyysissa. (SFS-EN 31010.)

Johdon määrittelemän riskitason perusteella tehdään toimenpide-ehdotukset riskien käsittelemiseksi. Ensisijaisesti tulee keskittyä riskin poistamiseen tai pienentämiseen, mikäli vain mahdollista. Osa riskeistä tulee ja on kannattavaa myös pitää omalla vastuulla, riippuen määritellystä riskitasosta. (Suomen riskienhallintayhdistys 2017; Laitinen ym. 2013, 301; Valtiovarainministeriö 2003.)

Viimeisenä vaiheena analyysi raportoidaan, johon sisältyy työpajassa arvioidut riskit, vaaraluettelo, toimenpide-ehdotukset ja yhteenvetolomake. Kaikki aineisto tulisi myös säilyttää tulevia riskien arviointeja varten. Tällöin helpointa on sähköinen raportointi työpajasta. Hyvällä raportoinnilla myös edesautetaan analyysin katselmusta ja esittelyä. (Suomen riskienhallintayhdistys 2017; Valtiovarainministeriö 2003, 69, 73.)

Liiketoiminta-analyysi

Liiketoiminta-analyysi, joka on englanniksi business impact analysis, on riskien arviointimenetelmä, joka tunnistaa ja määrittää valmiuksien määrän, joka tarvitaan hallitsemaan avainhäiriöriskejä. Liiketoiminta-analyysi antaa myös tietoa organisaation keskeisten prosessien, toimintojen ja niihin liittyvien resurssien sekä riippuvuussuhteiden tunnistamisessa. Analyysi myös selvittää, miten häiriöt vaikuttavat kriittisten liiketoimintatavoitteiden saavuttamiseen sekä resurssit, jotka tarvitaan palauttamaan toiminta sovitulle tasolle, häiriön tapahduttua. Keskeisimmät tuotokset (taulukko 3) luovat pohjan jatkuvuuden hallinnan suunnittelutyölle. (SFS-EN 31010.)

Panokset	**Tuotokset**
Ryhmän tekemä analyysi.	Luettelo kriittisistä prosesseista ja niiden välisistä riippuvuussuhteista.
Laadittu kyselylomake.	Tunnistettujen kriittisten prosessien tarvitsemat resurssit.
Luettelo haastateltavista, joihin otetaan yhteyttä liittyen keskeisiin prosesseihin.	Keskeytysajan kesto kriittiselle prosessille ja sen tietotekniikan palautumisajat.

Tiedot tavoitteista, toiminnoista ja riippuvuussuhteista.	Prosessien keskeytymisestä johtuvien taloudellisten ja toiminnallisten vaikutusten dokumentit.
Prosessien menettämisestä johtuvat taloudelliset ja toiminnalliset seuraukset.	
Yksityiskohdat toiminnoista, prosesseista ja tukiresurssit.	
	

Taulukko 3: Liiketoiminta-analyysin panokset ja tuotokset (SFS-EN 31010)

Analyysiä käytetään määrittämään prosessien ja niihin liittyvien resurssien kriittisyys sekä palautumisajanjaksot sen varmistamiseksi, että tavoitteissa pysytään. Liiketoiminta-analyysi voidaan toteuttaa kyselylomakkeilla, haastatteluina ja työryhmissä. Menetelmän keskeiset vaiheet ovat:

1. Määritetään keskeiset prosessit sekä niiden kriittisyys riskin perusteella.
2. Määritetään häiriön taloudelliset ja toiminnalliset seuraukset tietyssä prosessissa, tiettynä ajanjaksona.
3. Tunnistetaan riippuvuussuhteet sisäisten ja ulkoisten sidosryhmien kanssa.
4. Määritetään nykyiset ja tarvittavat resurssit toiminnan jatkamiseksi hyväksyttävällä tasolla, häiriön tapahduttua.
5. Tunnistetaan vaihtoehtoisia prosesseja tai kiertoteitä, mikäli nykyiset prosessit ovat riittämättömiä häiriöstä palautumiseksi.
6. Suurimman hyväksyttävän keskeytysajan, jonka organisaatio kestää, määrittäminen prosesseille.
7. Toipumisaikatavoitteiden määrittäminen erikoislaitteille ja tietotekniikalle. Toipumisaika tarkoittaa aikaa, jonka sisällä organisaatio pyrkii palauttamaan erityislaitteet ja tietotekniikan toimimaan.
8. Prosessien nykyinen valmiustaso mahdollisissa häiriötilanteissa. Esimerkkeinä varalaitteet tai varahenkilöjärjestelyt.
   (SFS-EN 31010.)

Kustannus-hyötyanalyysi

Kokonaiskuluja vertailtaessa odotettuihin kokonaishyötyihin voidaan käyttää Kustannus-hyötyanalyysiä, jonka tarkoituksena on selvittää paras tai kannattavin vaihtoehto. Analyysiä voi-

daan käyttää päätettäessä siitä, käsitelläänkö riskiä tai päätettäessä eri toimintavaihtoehtojen väliltä. Määrällinen kustannus-hyötyanalyysi yhdistää kustannuksien rahallisen arvon ja hyödyt kaikille osapuolille, jotka on sisällytetty mukaan. Saadusta nettonykyarvosta tulee panos riskejä koskevaan päätöksentekoon. (SFS-EN 31010.)

Analyysi aloitetaan tunnistamalla sidosryhmät, jotka saattavat kokea kustannuksia tai hyötyjä. Seuraavaksi tunnistetaan vaihtoehtojen suorat ja välilliset hyödyt ja kustannukset kaikille osapuolille, mikä pitää huomioida päätöksenteossa siitä, käsitelläänkö riskiä. Määrällisessä analyysissä tunnistetuille kustannuksille ja hyödyille määritetään rahallinen arvo, mitä varten löytyy erilaisia standarditapoja, kuten vastikkeiden käyttäminen. Mikäli kustannus syntyy lyhyellä aikavälillä ja hyöty jakautuu pitemmälle aikavälille, tulee hyödyt diskontata vastaamaan tämän päivän arvoa, jotta saadaan pätevä vertailu. Kaikki kustannukset ja hyödyt ilmaistaan nykyarvona, joka voidaan yhdistää sidosryhmien nettonykyarvon saamiseksi. Positiivinen nettonykyarvo tarkoittaa, että toiminta on hyödyllistä. (SFS-EN 31010.)

Kustannus-hyötyanalyysin tuotoksena saadaan tieto eri vaihtoehtojen tai toimenpiteiden suhteellisista kustannuksista ja hyödyistä, jotka ilmaistaan määrällisesti nettonykyarvona tai hyödyn ja kustannusten nykyarvon suhteena. Menetelmä tarjoaa läpinäkyvyyttä päätöksentekoon ja mahdollistaa hyötyjen ja kustannuksien vertailun rahassa. Analyysi vaatii myös yksityiskohtaisen tiedon keräämistä, mikä voi olla arvokasta tietämättömyyden paljastamisessa sekä tiedon välittämisessä. (SFS-EN 31010.)

Juurisyyanalyysi

Juurisyiden analyysi pyrkii tunnistamaan taustalla olevat tai alkuperäiset riskien syyt sen sijaan, että keskittyisi vain välittömiin oireisiin. Jatkuva parantaminen ja ennaltaehkäisy ovat tarpeen, koska korjaava toimenpide ei ole yhtä tehokasta riskien hallintaa. Tämän takia juurisyyanalyysi soveltuu hyvin määrittelemään sitä, missä on todellisuudessa parantamisen varaa sen sijaan, että tehtäisiin jatkuvasti väliaikaisia, korjaavia, toimenpiteitä. Turvallisuuspohjaista analyysiä käytetään erityisesti onnettomuustutkintaan, mutta myös työturvallisuuden analysointimenetelmänä. Analyysissä hyödynnetään kaikkia todisteita, jotka on kerätty vikaantumisista ja tappioista sekä mahdollisten hypoteesien testaamisen tuloksista. (SFS-EN 31010.)

Kun analyysin tarve on tunnistettu, asiantuntijaryhmä aloittaa menetelmän määrittelemällä tavoitteet ja laajuus analyysille sekä keräämällä tiedot ja todisteet. Järjestelmällinen analyysitekniikka juurisyiden määrittämiseksi voi koostua esimerkiksi vikapuuanalyysista tai ”minkä vuoksi” –menetelmästä, jossa pyritään kuorimaan syitä ja alisyitä kerros kerrokselta. Syiden arviointi etenee selkeistä fyysisistä syistä inhimillisiin syihin ja lopulta taustalla vaikuttaviin

johtamis- tai perussyihin. Asiantuntijoiden on kyettävä poistamaan syiden aiheuttajat, jotta korjaavat toimenpiteet olisivat hyödyllisiä. Lopputuloksena saadaan johtopäätökset vikaantumisista tai menetyksiin johtaneista todennäköisimmistä juurisyistä sekä korjaavat toimenpiteet, jotka kohdistuvat juurisyihin. Mikäli sopivia asiantuntijoita on käytettävissä ja on tarpeeksi aikaa arvioinnille, menetelmällä saadaan järjestelmällinen analyysi ja dokumentoidut lopulliset korjaavat toimenpidesuositukset. (SFS-EN 31010.)

Vikapuuanalyysi

Vikapuuanalyysi on tekniikka, joka tunnistaa ja analysoi tekijöitä, jotka voivat vaikuttaa tiettyyn epätoivottuun tapahtumaan. Syytekijät tunnistetaan päättelemällä, järjestellään loogisesti ja esitetään kuvallisena puukaaviona, joka kuvaa syitä ja niiden suhdetta huipputapahtumaan, epätoivottuun tapahtumaan. Analyysiä voidaan käyttää tunnistamalla mahdolliset syyt ja polut, jotka johtavat vikaantumiseen ja siten valintaan erilaisten suunnitteluvaihtoehtojen väliltä. (SFS-EN 31010.)

Menetelmä aloitetaan määrittelemällä huipputapahtuma, vikaantuminen. Huipputapahtuma voi myös olla laajempi useiden vikojen seuraus. Tämän jälkeen tulee tunnistaa välittömät syyt tai vikaantumismuodot, jotka johtavat huipputapahtumaan. Vastaavasti jokainen syy tai vikaantumismuoto tulee analysoida tunnistaen, mistä niiden vikaantuminen taas johtuu. Vaiheittainen tunnistaminen jatkuu alemmille tasoille, kunnes jatkoanalyysit eivät tuota mitään. Alimman tason tapahtumia ja syytekijöitä pidetään perustapahtumina, joissa ei ole tarvetta lisäanalyysille. Mikäli perustapahtumien todennäköisyyksiä pystytään määrittämään, saadaan huipputapahtuman todennäköisyys laskettua. Analyysi onkin hyvin järjestelmällinen, mutta riittävän joustava, jotta inhimilliset ja fysikaalisetkin ilmiöt saadaan luettua mukaan analyysiin. (SFS-EN 31010.)