# Turvallisuusauditointi - uhka vai mahdollisuus?

**Kriittiset tekijät auditoitavan valmistautumisessa**

**16. Turvallisuusjohdon koulutusohjelma**

**Kehitysprojektin raportti**

**Sami Leppämäki**

**Puolustusvoimat**

**Jyväskylä 7.7.2020**

**Aalto University Professional Development – Aalto PRO**

## Tiivistelmä

Auditointeja hyödynnetään turvallisuusjohtamisen valvonnassa ja kehittämisessä. Kehitysprojektissa oli tavoitteena tutkia auditoitavan valmistautumisen vaikutusta auditoinnin sujuvuuteen ja se toteutettiin laadullisena tutkimuksena soveltaen kriittisten tapahtumien menetelmää. Tiedonhankinta toteutettiin haastattelemalla kolmea kokenutta asiantuntijaa.

Aineistosta tunnistettiin 33 kriittistä tapahtumaa, joista laadittiin kuvaukset. Aluksi kuvaukset luokiteltiin auditointiprosessien mukaisiin valmistautumisen aktiviteetteihin: sisällön määrittäminen, suunnitelman laatiminen, osallistujien valitseminen, ja materiaalien kerääminen. Seuraavaksi muodostettiin neljä auditoinnin sujuvuuteen vaikuttavaa tekijää: johdon sitoutuminen, turvallisuusjohtamisen laatu, auditoinnin merkityksellisyys, ja auditointiosaaminen. Lopuksi tunnistettiin mihin aktiviteetteihin eri tekijät ovat yhteydessä.

Kehitysprojektissa tunnistettujen tekijöiden avulla auditoitava voi valmistautumisvaiheessa vaikuttaa auditoinnin sujuvuuteen. Tulosten perusteella johtamisen voidaan sanoa olevan tärkeä taustatekijä auditoinnin sujuvuudelle. Tulosten luotettavuuden ja yleistettävyyden arvioitiin riittävän toimeksiantajan toimintaympäristössä. Laadittua ohjetta voidaan hyödyntää auditointeihin valmistautumisessa vaatimuskehikon rinnalla.

## Abstract

Audits are used to control and develop security management. The purpose of this study was to examine what the target of the audit can do during the preparation phase to achieve smooth-running security audit. This qualitative study utilises the critical incident method. Data was collected by interviewing three experienced specialists.

In the data analysis phase, 33 critical incidents were identified, and descriptions were formulated for them. First, the descriptions were classified according to the activities of audit preparation: specify scope, prepare plan, select participants and collect information. Then, the factors affecting the smooth-run of an audit were categorised into four data based classes: management commitment, security management quality, audit significance and audit competence. Finally, the relations between the activities and the factors were perceived and described.

During the study, four factors that audit targets can use to influence the smooth-run of the audits during the preparation phase were identified. The results indicate that management is the crucial factor for the smooth-run of the audit. The dependability and generalisability of the results are adequate in the context of this study. The results of the study were developed into a preparation guideline, which can be used alongside the requirements framework during the preparation phase of the audit.

## Sisältö

# 1 Johdanto

Turvallisuusauditointeja hyödynnetään yleisesti turvallisuusjohtamisen valvonnassa ja kehittämisessä. Niiden järjestämiseen voi olla monia syitä, kuten organisaation turvallisuuden kypsyyden arvioiminen, haavoittuvuuksien tunnistaminen, standardeihin vertaaminen tai lainmukaisuuden varmistaminen. Turvallisuuden hallintajärjestelmään kohdistuvan auditoinnin järjestäminen on usein organisaation tietoturvallisuus- tai turvallisuuspäällikön tehtävä. Turvallisuusauditoinnin järjestäminen voidaan kokea epämiellyttävä tehtävänä tai jopa uhkana, jos auditoijan tunnistamien turvallisuuspuutteiden epäillään kohdistuvan organisaation sijasta suoraan tietoturvallisuus- tai turvallisuuspäällikköön. Turvallisuusauditointi tulisi nähdä mahdollisuutena nostaa esiin hyvin tehdyt asiat ja tunnistaa osa-alueita, joita täytyy vielä parantaa. Jotta tähän voidaan päästä, auditoijan ja auditoitavan vuorovaikutuksen tulee olla avointa ja rakentavaa. Myös turvallisuusauditoinnin vaatima työmäärä voidaan nähdä suurena odotettuihin hyötyihin nähden. Auditointitilaisuuden yhteinen aika tulee hyödyntää mahdollisimman hyvin vaatimustenmukaisuuden tarkastamiseen. Tällöin aikaa ei jouduta käyttämään valmistautumisen puutteiden selvittämiseen.

Tässä kehitysprojektissa tutkittiin turvallisuusauditoinnin sujuvuuteen vaikuttavia tekijöitä ja sitä, miten näihin tekijöihin voidaan vaikuttaa jo auditointiin valmistautumisessa. Turvallisuusauditointeja on monenlaisia ja eri tasoisia. Tässä kehitysprojektissa käsitellään turvallisuuden hallintajärjestelmien auditointeja. Raportissa *auditoinnilla* tarkoitetaan edellä mainitun kaltaista turvallisuusauditointia ja *turvallisuuden hallintajärjestelmällä* tarkoitetaan tiedon suojaamiseksi toteutettua johtamisjärjestelmää.

Huomioimalla sujuvuuteen vaikuttava tekijät valmistautumisessa, auditoitavan on mahdollista saavuttaa parempi pääoman tuottoaste (return of investment, ROI) auditoinnille. Tuottoaste paranee lyhyempien ja lukumäärältään

vähempien auditointitilaisuuksien kautta, todenmukaisemman auditoinnin tuloksen myötä sekä auditoinnin havaintojen parempana hyödynnettävyytenä toiminnan kehittämisessä. Valmistautumisen toimenpiteistä on laadittu auditoinnin vaatimuskehikosta riippumaton ohje auditoivalle. Raportissa *vaatimuskehikolla* tarkoitetaan joko turvallisuuden hallintajärjestelmän perustana tai auditoinnin kriteerinä olevia vaatimuksia, jotka perustuvat tiettyyn standardiin tai muuhun yleisesti käytössä olevaan määrittelyyn.

## 1.1 Toimeksiannon tausta

Puolustusvoimien tehtävänä on Suomen sotilaallinen puolustaminen, muiden viranomaisten tukeminen, osallistuminen aluevalvontayhteistyöhön tai muuhun kansainvälisen avun antamiseen ja kansainväliseen toimintaan sekä osallistuminen kansainväliseen sotilaalliseen kriisinhallintaan ja sotilastehtäviin muussa kansainvälisessä kriisinhallinnassa (Finlex 551/2007 §2). Tietoon kohdistuvat uhkat ovat kasvaneet ja nousseet merkittävämpään roolin koko yhteiskunnassa (SUPO 2019). Näistä aiheutuvat turvallisuusriskit ovat tulleet todennäköisemmiksi ja vaikutukseltaan vakavimmiksi. Vaatimuskehikkoon perustuvaa turvallisuuden hallintajärjestelmää voidaan hyödyntää kokonaisvaltaisena turvallisuuden hallintavälineenä ja sitä kautta yhtenä keinona edellä mainittujen riskien hallinnassa.

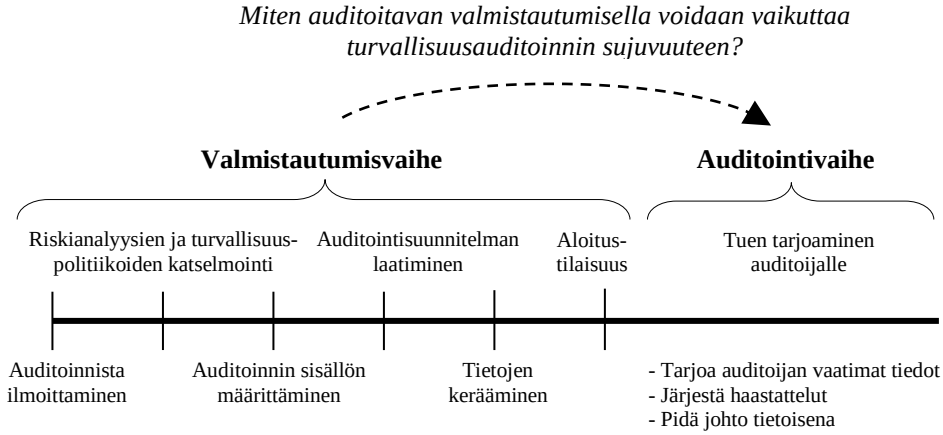
Auditoinnit ovat yksi keino tarkastaa turvallisuuden hallintajärjestelmän toiminta sekä varmistaa hallinnan lain- ja vaatimustenmukaisuus (Goel et al. 2006, 1). Puolustusvoimissa auditointeja hyödynnetään sisäisesti vaatimustenmukaisuuden varmistamisessa ja toiminnan kehittämisessä. Jos Puolustusvoimat luovuttaa turvallisuusluokiteltuja tietoaineistoja kumppanille, on Puolustusvoimilla lakisääteinen velvoite varmistua kumppanin kyvystä suojata tietoja (Finlex 2019/1101). Puolustusvoimiin voi myös kohdistua ulkopuolisen suorittamia turvallisuusauditointeja esimerkiksi tietoturvallisuussertifikaatteihin liittyen tai muiden viranomaisten lakisääteisistä tehtävistä johtuen (Finlex 2011/1406 ja 2004/588).

Edellä kuvatusta johtuen Puolustusvoimissa toteutetaan erilaisia auditointeja: 1) sisäisiä auditointeja, joissa auditoija ja auditoitava ovat omasta organisaatiosta; 2) ulkopuolisiin organisaatioihin kohdistuvia auditointeja, joissa Puolustusvoimat toimi auditoijana sekä 3) Puolustusvoimiin kohdistuvia auditointeja, joissa ulkopuolinen toimii auditoijana. Auditoinneissa käytetään erilaisia vaatimuskehikoita. Erilaiset auditoinnit ja arviointikehikot asettavat

omat haasteesta auditointiprosessin läpivientiin niin auditoijan kuin auditoitavan näkökulmasta. Aikaisempi tutkimus keskittyy tarkastelemaan auditointiprosessia auditoijan näkökulmasta (Goel et al. 2006, 3). Tässä kehitysprojektissa tutkittiin auditointiprosessia auditoitavan valmistautumisen näkökulmasta.

## 1.2 Kehitysprojektin tavoite

Kehitysprojektin tavoitteena oli selvittää, mikä on valmistautumisen merkitys auditoinnin sujuvuuteen auditoitavan näkökulmasta (kuva 1). Kehitysprojektissa *sujuvuudella* tarkoitetiin auditoinnin etenemisestä ja tulosten oikeellisuutta, ei auditoinnin lopputulosta. Tulosten perusteella laadittiin valmistautumisohje auditoitavalle osapuolelle (liite). Ohjeessa kuvattiin, mitä valmistautumisessa tulee huomioida auditoinnin sujuvuuden varmistamiseksi. Ohje on auditoinnin vaatimuskehikosta riippumaton ja tarkoitettu käytettäväksi sen rinnalla valmistautumisessa.




**Kuva 1** Auditointiprosessi (Goel et al. 2006) ja kehitysprojektin tutkimuskysymys

Kehitysprojektin päätutkimuskysymys oli (kuva 1):
*Miten auditoitavan valmistautumisella voidaan vaikuttaa turvallisuusauditoinnin sujuvuuteen?*

Kehitysprojektin apututkimuskysymykset olivat:
*1) Mistä aktiviteeteista koostuu auditoitavan turvallisuusauditointiin valmistautuminen?*
*2) Mitkä tekijät vaikuttavat turvallisuusauditoinnin sujuvuuteen?*
*3) Miten sujuvuuteen vaikuttavia tekijöitä voidaan huomioida auditoitavan valmistautumisessa?*

Kehitysprojekti rajattiin vaatimuskehikkoon perustuviin turvallisuuden hallintajärjestelmän auditointeihin (VAHTI 2/2010, Katakri 2015, ISO/IEC 27001). Auditointiprosessin tarkastelu kohdennettiin varsinaiseen auditointivaiheeseen ja sitä edeltävään valmistautumisvaiheeseen. Raportissa *auditointiprosessilla* tarkoitetaan kolmesta peräkkäisestä vaiheesta muodostuvaa prosessia: 1) valmistautumisvaihe, 2) auditointivaihe ja 3) seurantavaihe. Kehitysprojektissa tarkasteltiin sekä Puolustusvoimien sisäisiä auditointeja, että ulkopuolisen organisaation Puolustusvoimiin tekemiä tai Puolustusvoimien ulkopuoliseen organisaatioon tekemiä auditointeja. Kehitysprojektin tuotti uutta tietoa auditoitavan valmistautumisen merkityksestä auditoinnin sujuvuuteen. Kehitysprojektin nosti esiin auditointien sujuvuuteen vaikuttavia tekijöitä, joihin auditoitava voi vaikuttaa omassa valmistautumisessaan. Tutkimustulokset perustuvat asiantuntijoiden yleiseen kokemukseen ja ne eivät ole sidottu vain Puolustusvoimien toimintaympäristöön.

## 1.3 Raportin rakenne

Luvussa 2 esitellään käytetyt tutkimusmenetelmät ja niiden soveltaminen sekä perustelut menetelmien valinnoille. Luvussa 3 kuvataan kehitysprojektin tulokset. Luvussa 4 arvioidaan tulosten merkittävyyttä ja luotettavuutta sekä esitetään mahdollisuuksia jatkotutkimukselle. Liitteessä on tulosten perusteella laadittu valmistautumisohje auditoivalle.

# 2 Menetelmät

Kehitysprojektissa käytettiin laadullista tutkimusotetta soveltaen Flanaganin (1954) kehittämää kriittisten tapahtumien menetelmää (critical incident technique, CIT). Tätä tutkimusmenetelmää voidaan soveltaa erilaisiin tutkimustarkoituksin ja käyttää osana tutkimusmenetelmien kokonaisuutta. (Jaakola et al., 2014). Aineiston kerääminen toteutettiin kokeneiden auditointiasiantuntijoiden teemahaastatteluina. Aineisto analysoitiin kolmessa vaiheessa. Ensin laadittiin kriittisten tapahtumien kirjalliset kuvaukset haastattelutallenteiden pohjalta. Seuraavaksi luokiteltiin valmistautumisen toimenpiteet valmistautumisvaiheen aktiviteetteihin soveltaen aiemmassa tutkimuksessa kuvattua auditointiprosessia. Kehitysprojektissa *aktiviteetillä* tarkoitetaan valmistautumisvaiheen toimintoja, kuten suunnitelman valmistelu, joita voi olla käynnissä useita yhtä aikaa. Sen jälkeen luokiteltiin sujuvuuteen vaikuttavat asiat tekijöihin aineistolähtöisesti. Raportissa *tekijällä* tarkoitetaan auditoinnin sujuvuuteen vaikuttavien asioiden luokkia. Lopuksi tunnistettiin aktiviteettien ja tekijöiden väliset yhteydet.

## 2.1 Laadullinen tutkimusote

Kehitysprojektissa valittiin käytettäväksi laadullista tutkimusotetta, koska tutkittiin monimutkaista ilmiötä, jota ei tunnettu hyvin. Aikaisemmissa tutkimuksissa asiaa ei ole tarkasteltu auditoitavan näkökulmasta (Goel et al. 2006, 3). Kirjallisuushaun perusteella tutkimuksia turvallisuuden hallintajärjestelmän auditointien sujuvuudesta oli tehty vähän, poikkeuksena Rajamäen (2014) tekemä tutkimus Katakri auditoinneista. Toisena tutkimusotteen valinnan tavoitteena oli ymmärtää ilmiötä prosessissa toimivien näkökulmasta. Auditoinnin sujuvuuteen vaikuttaville tekijöille tai toimenpiteille ei asetettu hypoteeseja, vaan ne muodostettiin aineiston pohjalta.

## 2.2 Kriittisten tapahtumien menetelmä

Kriittisten tapahtumien menetelmän juuret ovat toisen maailman sodan aikaisessa Yhdysvaltain ilmailupsykologian ohjelmassa (Bott & Tourish 2016, 277). Menetelmää on käytetty osana sotilaslentäjien koulutusta 1950-luvulla, jolloin Flanagan tutki miten lentäjien inhimillistä toimintaa voitiin parantaa tunnistamalla edistävästi tai estävästi vaikuttavia tapahtumia. Termillä kriittinen tarkoitetaan inhimillisen toiminnan merkittävää ja ratkaisevaa roolia toiminnan tavoitteeseen tai lopputulokseen. Tapahtuman kokija määrittelee tapahtumat ja niiden kriittisyyden tapahtumille antamansa merkittävyyden perusteella. Menetelmä korostaa tutkimukseen osallistuvan näkökulmaa ja kokemusta. Se mahdollistaa uuden tiedon esiin saamisen vaikeasti ennalta määriteltävistä ilmiöistä. (Jaakola et al., 2014 157-160.)

Kaikkien kriittisten tapahtumien taustatekijöinä on kulttuuri, kokemus, kyvykkyys, suhde, luottamus, tunteet, yhteydenpito tai suhtautuminen (Serrat, 2017, 1078). Kriittisten tapahtumien menetelmän joustavuudesta johtuen sitä on sovellettu useilla eri tieteenaloilla. Tutkimuksessaan Bott ja Tourish (2016, 276) toteavat menetelmän soveltuvan hyvin johtamisen ja organisaatioiden laadulliseen tutkimiseen. Kriittisten tapahtumien menetelmä on hyvin soveltuva väline kuvaamaan ammatillisia käytänteitä (Hettlage & Steinlin, 2006, 5).

Flanaganin (1954) kehittämä kriittisten tapahtumien menetelmä koostuu viidestä vaiheesta: 1) toiminnan tarkoitus ja tavoite, 2) suunnitelma ja tietotarpeet, 3) aineistonkeruu, 4) aineiston analysointi, ja 5) tulosten tulkinta ja raportointi. Ensimmäisessä vaiheessa määritellään tutkittavan ilmiön tarkoitus ja tavoite, joista voidaan tehdä havaintoja ja päätelmiä. Toisessa vaiheessa laaditaan suunnitelma, miten kriittisiä tapahtumia tutkitaan ja mitä tietoja niiden tutkimiseen tarvitaan. Kolmannessa vaiheessa suoritetaan aineiston kerääminen. Tavoitteena on saada mahdollisimman täydellinen kuvaus tapahtumista. Neljännessä vaiheessa ainestoa analysoidaan valituilla menetelmillä. Analysoinnin tavoitteena on saada esiin toiminnan onnistuneisuuteen vaikuttavia tekijöitä. Viidennessä vaiheessa esitetään tulosten tulkinta ja raportointi. Tarkoituksena on kuvata koko tutkimusprosessi ja tulosten kokoaminen sekä arvioida saatuja tuloksia. (Jaakola et al., 2014 158-159.)

Kehitysprojektin osalta tutkittavan toiminnan tarkoitus ja tavoite on esitelty raportin johdanto luvussa. Suunnitelma ja tietotarpeet, aineistonkeruu ja aineiston analysointi vaiheet on esitelty raportin menetelmät luvussa. Tutkimuksen tulkinta ja raportointi on esitelty raportin tulokset luvussa ja raportti kuvaa tutkimusprosessin kokonaisuudessaan.

## 2.3 Aineiston kerääminen

Kehitysprojektin tiedonhankinta toteutettiin haastattelemalla kokeneita auditoinnin asiantuntijoita. Kriittisten tapahtumien menetelmässä haastateltava määrittää tapahtumat. Flanaganin (1954, 327) mukaan kriittisen tapahtuman tunnistaa sen muistettavuudesta, joka aiheutuu henkilön tapahtumalle antamasta merkityksestä. Haastattelun valinnalla aineistonkeruun menetelmäksi tavoiteltiin ymmärrystä siitä, miten auditoinnin asiantuntijat konstruoivat auditoinnin tilanteiden ja asioiden merkityksiä sekä minkälaisen merkityksen he niille antavat. Aineistonkeruun edustavuuden kannalta keskeistä ei ole tutkimukseen osallistuvien määrä, vaan havaittujen tapahtumien määrä (Flanagan 1954, 343).

Kehitysprojektissa haastateltiin kolmea Puolustusvoimissa työskentelevää asiantuntijaa. Kaikki haastateltavat ovat suorittaneet Puolustusvoimien turvallisuustarkastajan pätevyyteen vaadittavan koulutuksen ja ovat toimineet Puolustusvoimien toimivaltaisena turvallisuustarkastajana. Lisäksi kaikki haasteltavat ovat osallistuneet ISO/IEC 27001 standardin auditointikoulutuksiin ja osa on osallistunut myös Katakrin eri versioiden kehittämiseen. Haastateltavilla on kokemusta yhteensä yli vuoden 50 vuoden ajalta turvallisuuden hallintajärjestelmien auditoinneista, joko päätehtävänään tai merkittävänä osana muuta tehtävää. Haastateltavilla on kokemusta sekä auditoijan että auditoitavan rooleissa toimimisesta, painottuen auditoijan rooliin. Haastateltavien kokemus muodostuu Puolustusvoimien sisäisistä auditoinneista, Puolustusvoimien ulkopuoliseen organisaation kohdistamista auditoinneista, ulkopuolisien organisaation tekemistä Puolustusvoimiin kohdistuvista auditoinneista sekä ulkopuolisen organisaation toiseen ulkopuoliseen organisaation toteuttamista auditoinneista. Kokemusta on eniten Puolustusvoimien ulkopuoliseen kohdistamista auditoinneista ja vähiten ulkopuolisen toiseen ulkopuoliseen kohdistamista auditoinneista. Kaikilla haastateltavilla on kokemusta VAHTI 2/10, Katakri 2015 ja ISO/IEC 27001 vaatimuskehikoiden

käyttämisestä auditoinneissa, kokemuksen painottuessa Katakrin mukaisiin auditointeihin.

Haastattelutyypiksi valittiin teemahaastattelu, jossa haastattelun aihepiirit eli teemat ovat etukäteen määriteltyjä. Teemojen käsittelyn järjestys ja laajuus voivat vaihdella haastattelusta toiseen. Haastattelutyypin valinnan tavoitteena oli korostaa haastateltavien näkemyksen ja kokemuksen merkitystä kriittisten tapahtumien tunnistamisessa. Haastattelun teemat ja teemoihin johdattavat kysymykset laadittiin soveltaen aiempaa auditointien ja kriittisen tapahtumien menetelmän kirjallisuutta (Suduc et al., 2010, 46 ja Hettlage & Steinlin, 2006, 9). Haastattelun teemat pohjautuivat turvallisuusauditointien päätavoitteisiin (Suduc et al., 2010, 46):

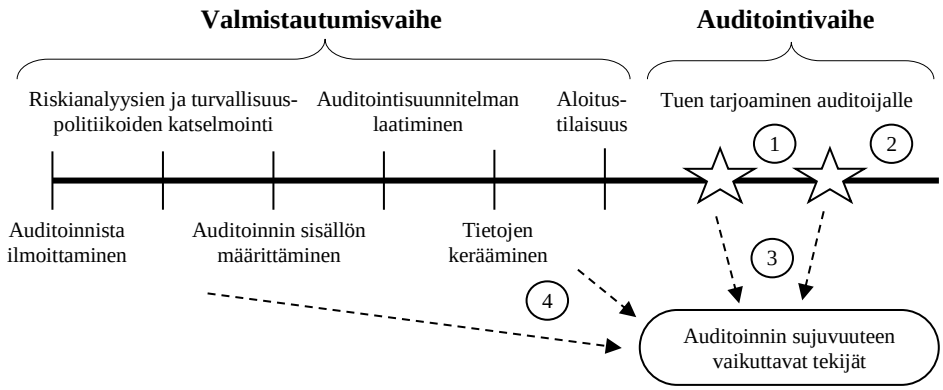
1) Turvallisuuspolitiikan ja -ohjeiden olemassa olon tarkastaminen, vaikuttavuuden arviointi sekä puutteiden tunnistaminen,
2) Riskien ja haavoittuvuuksien tunnistaminen sekä ymmärtäminen
3) Hallinnollisten, toiminnallisten ja teknisten hallintakeinojen katselmointi sekä vaatimustenmukaisuuden varmistaminen
4) Suositusten ja korjaavien toimenpiteiden laatiminen

Jokaisella teemalle laadittiin samankaltaiset teemaan johdattelevat kysymykset, esimerkkinä teeman kolme mukaiset kysymykset: *”Kuvaile merkittävä tapahtuma, joka on vaikuttanut positiivisesti tai negatiivisesti turvallisuusauditoinnin sujuvuuteen hallinnollisten, toiminnallisten ja teknisten hallintakeinojen katselmoinnissa tai vaatimustenmukaisuuden varmistamisessa?”* ja *”Mikä valmisteluvaiheessa sai sen aikaan (positiivinen) tai olisi voinut sen estää (negatiivinen)?”*. Haastateltaville lähettiin etukäteen tutkimuksen esittely ja haastatteluohje, joka sisälsi teemat ja niihin johdattavat kysymykset.

Kriittisten tapahtumien menetelmässä ei ole oleellista tunnistaa miten asiat tapahtuivat vaan mikä sai ne aikaan (Jaakola et al., 2014 159). Kun haastattelussa tunnistettiin positiivisesti auditoinnin sujuvuuteen vaikuttanut tapahtuma, niin tarkasteltiin, mikä valmisteluvaiheen toimenpide sai sen aikaan. Kun tunnistettiin negatiivisesti auditoinnin sujuvuuteen vaikuttanut tapahtuma, niin tarkasteltiin, mikä valmisteluvaiheen toimenpide olisi voinut sen estää. Asiatuntijoiden haastattelut tallennettiin aineiston jatkokäsittelyä varten.

## 2.4 Aineiston analysointi

Aineiston analysoinnin tavoitteena oli tuoda aineistoon selkeyttä, järjestystä ja rakennetta sekä tuottaa uutta tietoa auditointien sujuvuuteen vaikuttavista tekijöistä. Tekijöille ei asetettu hypoteeseja, joten analysointi toteutettiin aineistolähtöisesti ilman teoreettisia etukäteisolettamuksia. Myöskään haastattelun teemoja ei käytetty aineiston analysoinnissa. Aineiston analysoinnin ensimmäisessä vaiheessa haastattelutallenteista tunnistettiin auditoinnin sujuvuuteen vaikuttavat kriittiset tapahtumat ja laadittiin niistä kirjalliset kuvaukset. Laaditut kriittisten tapahtumien kuvaukset koostuivat neljästä alakohdasta: 1) tapahtuma, 2) seuraus, 3) syy, ja 4) toimenpide. Kuvausten laatimista varten, luotiin jokaiselle osalle apukysymys, johon kuvauksessa vastattiin. Tapahtuman kuvauksessa vastattiin kysymykseen: 1) *”Mikä tapahtuma vaikutti auditoinnin sujuvuuteen?”*, seurauksen kuvauksessa kysymykseen: 2) *”Miten tapahtuma vaikutti auditoinnin sujuvuuteen?”* syyn kuvauksessa kysymykseen: 3) *”Mikä asia johti tapahtumaan?”* ja toimenpiteen kuvauksessa kysymykseen: 4) *”Miten tapahtuma tulee huomioida auditointiin valmistautumisessa?”* (kuva 2). Kuvaukset laadittiin 33 tapahtumasta.




**Kuva 2** Kriittisten tapahtumien kuvausten laatiminen

Aineiston analysoinnin toisessa vaiheessa tapahtumaan johtaneet syyt ja toimenpiteet auditoinnin sujuvuuden varmistamiseksi luokiteltiin. Sujuvuuden varmistamisen toimenpiteet luokiteltiin valmistautumisvaiheen aktiviteetteihin Goel et al. (2006, 3-8) auditointiprosessia mukaillen. Tapahtumaan johtaneesta syistä luotiin auditoinnin sujuvuuteen vaikuttavien tekijöiden luokat. Aineiston analyysin kolmannessa vaiheessa tarkasteltiin aktiviteettien ja tekijöiden välisiä yhteyksiä. Tarkastelussa selvitettiin millä aktiiviteeteillä on yhteys eri tekijöihin. Lopuksi kuvattiin miten yhteys vaikuttaa auditoinnin sujuvuuteen.

# 3 Tulokset

Kehitysprojektin tulokset esitellään kolmessa osassa. Ensimmäisenä esitellään valmistautumisvaiheen aktiviteetit. Toisena esitellään auditointien sujuvuuteen vaikuttavat tekijät. Lopuksi esitellään tekijöiden ja aktiviteettien välinen yhteys.

## 3.1 Valmistautumisen aktiviteetit

Auditoinnin sujuvuuden varmistamisen toimenpiteet luokiteltiin valmistautumisvaiheen aktiviteetteihin soveltaen Goel et al. (2006, 3-8) auditointiprosessia. Tulokseksi saatiin seuraavat valmistautumisen aktiviteetit: 1) sisällön määrittäminen, 2) suunnitelman laatiminen, 3) osallistujien valitseminen, ja 4) materiaalien kerääminen. Seuraavana käsitellään aktiviteetit tarkemmin.

*Sisällön määrittäminen*

Auditoinnin sisällön määrittämiseen kuuluu auditoinnin tarkoituksen ja merkityksen selventäminen, mihin auditoinnilla pyritään ja miksi se on tärkeä kohdeorganisaatiolle. Näiden merkitys korostuu, jos auditoitavalla ei ole aikaisempaa kokemusta turvallisuusauditoinneista. Vaatimusasetanta tulee selkiyttää auditointiprosessin aluksi, eli mikä on auditoinnissa käytettävä vaatimuskehikko ja millä tasolla vaatimuksia tarkastellaan. Samalla tulee tehdä auditoinnin rajaus, eli mitä toimintoja tai organisaation osia auditoinnissa tarkastellaan. Tässä kehitysprojektissa auditoinnin *sisällön määrittämisellä* tarkoitetaan auditoinnin tarkoituksen ja merkityksen selventämisestä, käytettävien vaatimusten määrittämistä ja auditoinnin kohteen rajaamista.

*Suunnitelman laatiminen*

Aineistossa olevien tapahtumien perusteella auditointisuunnitelman laatimiseen kuuluu auditoitavien toimintojen tarkempi suunnittelu, kuten minkälaisissa osissa asioita on tarkoituksenmukaista käsitellä. Turvallisuuden hallintajärjestelmä ja sen liittyminen muihin hallintajärjestelmiin, kuten riskienhallintaan, täytyy kuvata ja järjestelmien ylläpitäminen täytyy selventää. Lisäksi tulee arvioida turvallisuuden hallinnan todellinen tila ja tunnistaa mahdolliset puutteet dokumentaatiossa tai turvallisuuden toteutuksessa sekä laatia niistä korjausesitykset. Tulokseksi saatiin, että auditoinnin *suunnitelman laatimisella* tarkoitetaan auditoitavien toimintojen suunnittelua, turvallisuuden hallintajärjestelmän kokonaisuuden kuvaamista ja turvallisuuden tilan tunnistamista.

*Osallistujien valitseminen*

Auditointiin osallistuvien valintaan kuuluu aineiston perusteella, että tunnistetaan mihin toimintoihin auditointi kohdistuu ja valitaan näistä toiminnoista vastaavat henkilöt auditointiin. Osallistujien valinnassa on huomioitava, että mukana on riittävästi kokemusta auditoinneista ja hallintajärjestelmistä. Resursseista päättävän tahon on hyvä olla edustettuna tai selvä mandaatti annettuna jollekin muulle auditointiin osallistuvalle. Perehdytyksessä osallistujille selvennetään auditoinnin tarkoitus ja merkitys sekä auditoinnin toteutustapa. Aineistoon perustuen voidaan todeta, että *osallistujien valitsemisella* tarkoitetaan auditoitavista osa-alueista vastaavien henkilöiden ja johdon tai resursseista vastaavien tahojen valintaa auditointitiimiin sekä auditointitiimin perehdyttämistä auditoinnin tarkoitukseen ja toteutustapaan.

*Materiaalien kerääminen*

Aineiston pohjalta auditointimateriaalin keräämiseen kuuluu aineistosuunnittelu eli miten tarkasteltavat asiat esitellään auditoitavalle ja mitä tietoa niiden todentamiseksi tarvitaan. Turvallisuuden hallintajärjestelmän toiminnasta ja sen liittymisestä organisaation muuhun toimintaan on syytä olla kokonaiskuvaus. Lisäksi aineistosuunnittelun mukaiset materiaalit ja tiedot toimitetaan auditoijalle etukäteen. Yhteenvetona voidaan todeta, että auditoinnin *materiaalien keräämisellä* tarkoitetaan auditointiaineiston suunnittelua ja keräämistä sekä sen toimittamista auditoijalle etukäteen.

## 3.2 Sujuvuuteen vaikuttavat tekijät

Auditointien sujuvuuteen vaikuttavien tapahtumien ja niihin johtaneiden syiden analysoinnissa toistuivat tietyt asiat. Näistä muodostettiin neljä aineistolähtöistä tekijää: 1) johdon sitoutuminen, 2) turvallisuusjohtamisen laatu, 3) auditoinnin merkityksellisyys, ja 4) auditointiosaaminen. Seuraavassa käsitellään tekijät tarkemmin.

### 3.2.1 Johdon sitoutuminen

Johdon sitoutuminen vaikuttaa turvallisuusauditoinnin sujuvuuteen monin tavoin. Voi esimerkiksi olla, että auditoija ja auditoitava eivät pääsee yhteisymmärrykseen resursseja vaativista korjaavista toimenpiteistä. Tämä voi johtua siitä, auditoitavalla ei ole valtuuksia resurssipäätöksiin. Jos johto ei osallistu tai ei ole sitoutunut auditointiin, resursseja vaativat auditoinnin suositukset ja korjaavat toimenpiteet eivät välttämättä etene auditoinnin jälkeen. Johto voi olla sitoutunut vain ulkoisiin auditointeihin eikä näe sisäisiä auditointeja toiminnan kehittämisen välineenä. Tällöin voidaan joutua käyttämään ulkoista auditoijaa tarkastamaan sisäiset havainnot ja raportoimaan ne johdolle. Johdon sitoutumisen puutteesta kertoo myös tilanne, jossa johtamisen- ja organisaation hallinnan toimintojen kuten kokonaisriskienhallinnan tarkastelu joudutaan tekemään vain turvallisuuden toimijoiden kanssa, vaikka tarkasteluun tarvittaisiin keski- ja ylintä johtoa.

Yhteenvetona voidaan todeta, että *johdon sitoutumisella* tarkoitetaan johdon osallistumista auditointiin, tuen ja päätöksentekomandaatin antamista auditointiin osallistuville sekä asianmukaisen painoarvon antamista auditoinnin tuloksille. Johdon sitoutumisen puute ilmenee esimerkiksi auditoinnin suositusten ja korjaavien toimenpiteiden toimeenpanon vaikeutena. Toisaalta johdon sitoutuminen mahdollistaa organisaation johtamisen tarkastelun osan turvallisuuden hallintaa tai keskustelut investointeja vaativista korjaavista toimenpiteistä.

### 3.2.2 Turvallisuusjohtamisen laatu

Myös turvallisuusjohtamisen laatu vaikuttaa auditointien sujuvuuteen monin tavoin. Jos turvallisuusjohtamisen laatu on heikko, auditoitavat eivät esimerkiksi tiedä kuka vastaa mistäkin turvallisuuden osa-alueesta tai kenen pitäisi vastata auditoijan kysymyksiin. Tämä voi johtua siitä, että auditoitavilla ei

ole osaamista ja kokemusta auditoinneista tai turvallisuuden hallinnasta. Turvallisuusjohtamisen korkea laatu näkyy siinä, että auditoitavat pystyvät omaaloitteisesti kertomaan turvallisuuden toteutuksen ja sen hallinnan sekä pystyvät osoittamaan todentamiseen tarvittavat dokumentaatiot ja muutoshistoriat. Auditoitavan yleinen kokemus hallintajärjestelmien auditoinneista auttaa auditoitavaa esittelemään turvallisuuden hallintajärjestelmää oikealla tasolla auditoijalle.

Auditoitavan turvallisuusjohtamisen heikko laatu voi ilmetä siinä, että auditoitava on luonut materiaalit pelkästään auditointia varten, mutta ei osaa kertoa miten turvallisuuden hallintajärjestelmä toimii suhteessa organisaation muuhun toimintaan. Tai auditoitava pystyy listaamaan suojattavat kohteet, arvioidut riskit tai tunnistetut haavoittuvuudet, mutta ei pysty kertomaan, miten niitä hallitaan. Tällöin tietoturvapolitiikka ja -ohjeistus vastaavat yksittäisiin vaatimuksiin, mutta eivät muodosta tavoitteisiin ohjaavaa turvallisuuden hallintajärjestelmää.

Edellä olevaan pohjautuen *turvallisuusjohtamisen laadulla* tarkoitetaan, että auditoitavat ymmärtävät turvallisuuden hallinnan periaatteet ja turvallisuuden toteutuksen omassa organisaatiossa. Korkealaatuinen turvallisuusjohtaminen mahdollistaa paremman kokonaiskuvan esittämisen hallintajärjestelmän toiminnasta auditoijalle. Lisäksi turvallisuusjohtamisen korkea laatu mahdollistaa oikeiden henkilöiden valinnan auditointiin. Toisaalta heikko laatu voi estää joidenkin tarvittavien osa-alueiden auditoinnin, jos auditoitavat eivät osaa kertoa vaadittavista asioita eivätkä pysty esittämään tarvittavia tietoja.

### 3.2.3 Auditoinnin merkityksellisyys

Aineistoon perusteella myös auditoinnin merkityksellisyys vaikuttaa auditoinnin sujuvuuteen. Jos auditoinnin merkityksellisyys koetaan epäselvänä, auditoitava organisaatio ei tue auditointivaiheen läpivientiä tai koko auditointiprosessia. Auditoitavat suhtautuvat negatiivisesti auditointiin ja eivät ymmärrä miksi heidän pitää avata omia toimintatapojaan auditoijalle tai pitävät koko auditointia turhana. Jos auditoinnin tarkoitusta turvallisuustoiminnan tarkastuksena ei ole ymmärretty, voi olla, että auditointimateriaalit on laadittu vain auditointia varten ja niitä ei ole mitenkään jalkautettu. Voi olla myös, että auditoitava tietää, että dokumentaatio ei ole kunnossa, mutta kertoo silti sen olevan kunnossa ja kokeilee tyytyisikö auditoija kerrottuihin vastauksiin.

Tulosten perusteella *auditoinnin merkityksellisyys* tarkoittaa, että auditointiin osallistuva henkilöstö ymmärtää mihin turvallisuusauditoinnilla pyritään ja miksi se on tärkeä kohdeorganisaatiolle. Jos ne ovat epäselviä auditoitavat ei vastaa auditoijan kysymyksiin, vaan kritisoivat auditoinnin pitämistä ja eivät suostu avoimesti avaamaan omaa toimintaa auditoijalle. Tällöin auditoija ei pysty tarkastamaan toiminnan vaatimustenmukaisuutta tai todentamaan kerrotun mukaista toimintaa.

### 3.2.4 Auditointiosaaminen

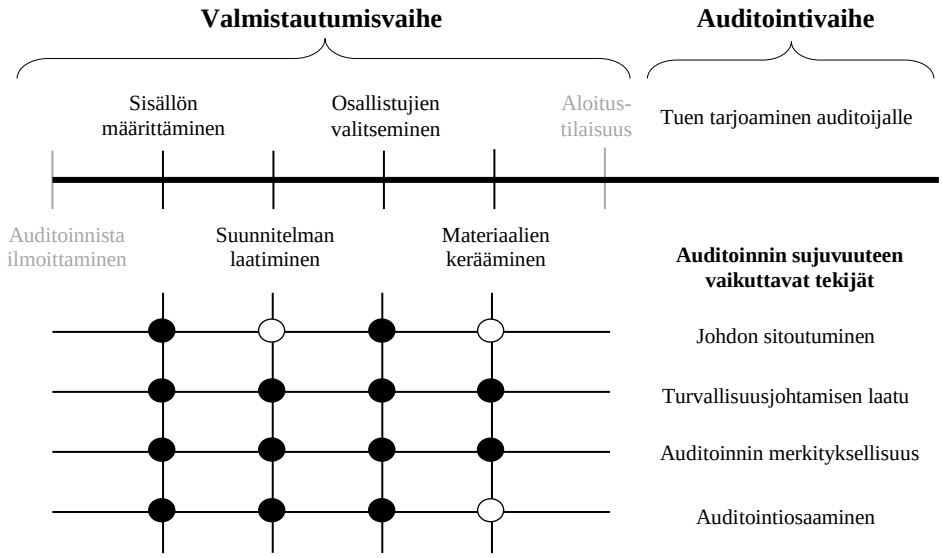
Myös auditointiosaaminen vaikuttaa turvallisuusauditoinnin sujuvuuteen. Jos auditoitava ei tunne turvallisuuden asiakasvaatimuksia, auditoitava ei voi osata kertoa miten niitä on sovellettu. Auditoitava voi kokea turvallisuuden asiakasvaatimukset liian vaativiksi eikä osaa tunnistaa yrityksen muiden hallintajärjestelmien myötävaikutusta turvallisuuden hallinnan kokonaisuuteen. Tällöin auditoinnista voidaan luopua jo etukäteen. Samoin voi käydä, jos turvallisuusvaatimuksia ei ole sovitettu toimintaympäristöön ja kohdeorganisaation kokoon pienissä organisaatioissa. Jos auditoinnissa käytettävät vaatimukset ja niiden soveltaminen ovat epäselviä, niin auditoinnin vaatimustaso voi vaihdella auditoijan mukaan tai auditoinnista toiseen.

Edellä esitettyyn perustuen *auditointiosaamisella* tarkoitetaan sitä, että auditoitava tuntee auditoinnin vaatimuskehikon ja osaa soveltaa sitä omassa toimintaympäristössään. Jos vaatimukset ovat epäselviä, auditointien tulosten vertailu on hankalaa ja seuraavassa auditoinnissa voidaan kirjata poikkeamia edellisessä auditoinnissa hyväksytyistä asioista. Se voi myös ilmetä niin, että auditoitava ei osaa valmistautua esittelemään turvallisuusvaatimusten soveltamista ja vaatimusten soveltamista joudutaan tekemään auditoinnissa tapauskohtaisesti.

## 3.3 Toimenpiteet sujuvuuden varmistamiseksi

Tässä luvussa tarkastellaan auditoinnin sujuvuuteen vaikuttavien tekijöiden ja valmistautumisen aktiviteettien välistä yhteyttä (kuva 3). Kehitysprojektissa huomattiin, että sujuvuuteen vaikuttavat tekijät tulee huomioida valmistautumisen eri aktiviteeteissä. Osa tekijöistä kaikissa aktiviteeteissä ja osa tietyissä aktiviteeteissa. *Huomioiminen* tarkoittaa valmistautumisvaiheen aktiviteetin tiettyä toimenpidettä, jolla voidaan sujuvoittaa auditointivaihetta. Auditoinnin sujuvuuteen vaikuttamisen toiminta-ajatus on seuraavan lainen:

Aktiviteetti → Toimenpide → Tekijä → Auditoinnin sujuvuus. Valmistautumisvaiheen tietyissä aktiviteeteissä tehdyillä toimenpiteillä voidaan vaikuttaa tiettyihin sujuvuuteen vaikuttaviin tekijöihin ja sitä kautta auditointivaiheen sujuvuuteen.




**Kuva 3** Sujuvuuteen vaikuttavien tekijöiden ja valmistautumisvaiheen aktiviteettien välinen yhteys

Auditoinnin sisällön määritellyssä ja osallistujien valitsemisessa tulee huomioida kaikki neljä sujuvuuteen vaikuttavaa tekijää. Auditoinnin suunnitelman laatimisessa tulee huomioida turvallisuusjohtamisen laatu, auditoinnin merkityksellisyys ja auditointiosaaminen. Auditointimateriaalin keräämisessä on huomioitava turvallisuusjohtamisen laatu ja auditoinnin merkityksellisyys (kuva 3). Seuraavissa alaluvuissa käydään läpi nämä toimenpiteet valmistautumisen aktiviteetti kerrallaan.

### 3.3.1 Sisällön määrittäminen

Auditoinnin sisällön määrittelyssä tulee huomioida kaikki neljä auditoinnin sujuvuuteen vaikuttavaa tekijää (taulukko 1). Jos turvallisuusjohtamisen laatu on matala, auditoinnin rajaus voi jäädä epäselväksi. Tällöin auditointi ei kohdistu oikeaan osaan organisaatiossa tai auditoinnissa ei tarkastella kohteen kannalta oikeita asioita.

Auditoinnin tarkoitus ja merkitys tulee selkiyttää organisaatiolle jo auditoinnin sisällönmäärittelyn yhteydessä. Jos auditoinnin merkityksellisyyttä ei ymmärretä, auditoitava saattaa kiistää auditoinnin oikeutuksen ja olla tekemättä

yhteistyötä auditoijan kanssa. Tunnistettuja turvallisuuspuutteita saatetaan myös peitellä. Johto täytyy saada sitoutumaan auditointiin jo sisältöä määriteltäessä, jotta johdon tuki on käytettävissä auditoinnin tuloksesta riippumatta. Jälkikäteen voi olla vaikeaa saada riittäviä resursseja auditoinnin suosituksille ja korjaaville toimenpiteille. Jos johto ei reagoi sisäisen auditoinnin tuloksiin, voidaan auditointi joutua toistamaan ulkopuolisen tahon toimesta.

**Taulukko 1** Tapahtumakuvasten jakautuminen tekijöihin ja aktiviteetteihin

| | Sisällön määrittäminen | Suunnitelman laatiminen | Osallistujien valitseminen | Materiaalien kerääminen |
|---|---|---|---|---|
| Johdon sitoutuminen | 10 | - | 9, 27, 31 | - |
| Turvallisuus-johtamisen laatu | 8 | 20, 23, 30 | 1, 2 | 3, 15, 16, 17, 18, 19, 33 |
| Auditoinnin merkityksellisyys | 4, 24, 29 | 13, 14, 21, 22 | 5,12, 28 | 6 |
| Auditointi-osaaminen | 7, 25, 32 | 26 | 11 | - |

Auditoinnissa käytettävät vaatimukset ja niiden soveltaminen tulee olla selvillä viimeistään auditoinnin sisällön määrittelyn yhteydessä. Sisällön määrittelyssä tarvitaan auditointiosaamista etenkin, jos turvallisuusauditointi toteutetaan eri vaatimuskehikolla kuin mihin organisaation turvallisuuden hallintajärjestelmä perustuu. Mikäli osaamisessa on puutteita, auditoitava ei välttämättä tunne turvallisuuden asiakasvaatimuksia tai ei osaa kertoa miten turvallisuusvaatimuksia on sovellettu. Tällöin auditoitava ei voi valmistautua esittämään organisaation turvallisuuden toteutusta auditoinnin vaatimuskehikkoa vasten.

### 3.3.2 Suunnitelman laatiminen

Auditoinnin suunnitelman laatimisessa tulee huomioida sujuvuuteen vaikuttavista tekijöistä turvallisuusjohtamisen laatu, auditoinnin merkityksellisyys ja auditointiosaaminen (taulukko 1). Jos turvallisuusjohtamisen laatu on korkea, turvallisuuden hallintajärjestelmä ohjaa organisaation toimintaa ja sitä on ylläpidetty tarpeen mukaan. Turvallisuusasioita on myös käsitelty johdon kanssa. Tällöin auditoinnin suunnittelu on helppoa koska turvallisuuden hallinta on osa jokapäiväistä tekemistä.

Kun auditoinnin merkityksellisyys on ymmärretty, auditoinnin suunnittelu perustuu todenmukaiseen turvallisuuden tilannekuvaan. Jos merkityksellisyys on epäselvä, saatetaan laatia erilaisia ohjeistuksia tai jopa koko turvallisuuden hallintajärjestelmä vain auditointia varten. Tällöin organisaation toiminta ei vastaa auditoinnissa esitettyä dokumentaatiota.

Jos organisaatiossa ei ole erillistä turvallisuuden hallintajärjestelmää, vaan turvallisuutta hallitaan osana muita johtamisjärjestelmiä, auditointiosaamisen merkitys korostuu. Turvallisuuden hallinnasta voidaan joutua tekemään erillinen kuvaus, jolla kokonaisuus esitellään auditoijalle. Hyvällä auditointiosaamisella pystytään tulkitsemaan auditoinnin vaatimustaso oikein.

### 3.3.3 Osallistujien valitseminen

Kaikki neljä auditoinnin sujuvuuteen vaikuttavaa tekijää tulee huomioida osallistujien valitsemisessa (taulukko 1). Auditointiin osallistuvat valitaan työtehtäviensä perusteella. Mukana täytyy olla sekä auditoitavista asioista vastaavia henkilöitä, että niiden käytännön toteutukseen osallistuvia. Jos organisaation turvallisuusjohtaminen on korkealla tasolla, näiden roolien määrittäminen on helppoa.

On myös syytä varmistua, että resursseista vastuussa olevia johtajia osallistuu auditointiin. Vaihtoehtoisesti voidaan antaa selvä mandaatti resurssipäätösten tekemiseen jollekin auditointiin osallistuvalle. Näiden lisäksi mukaan tulee valita henkilöitä vahvalla auditointiosaamisella, jos sitä ei muuten ole riittävästi valittavassa osallistujajoukossa.

Osallistujien perehdyttämisessä on syytä varmistua, että auditoinnin tarkoitus on kaikille osallistujille selvänä. Myös auditoinnin toteutustapa on hyvä käydä läpi kaikkien osallistujien kanssa. Näin varmistetaan, että kaikki osallistujat ymmärtävät auditoinnin merkityksen organisaatiolle sekä osaavat valmistautua ja toimia valitun toteutustavan mukaisesti.

### 3.3.4 Materiaalien kerääminen

Auditointimateriaalin keräämisessä on huomioitava turvallisuusjohtamisen laatu ja auditoinnin merkityksellisyys (taulukko 1). Jos auditoinnin tarkoitus on epäselvä, niin auditoitava ei tunnista tarvittavia tietoa tai ei toimita niitä

etukäteen. Auditointia varten tarvittava materiaali kerätään auditoinnin tarkoitusta vastaavasti ja sen perustella tulisi pystyä tekemään tarkoituksen mukaiset arviot auditoitavasta kohteesta.

Jos turvallisuusjohtamisen laatu on korkea, auditoitava pystyy tunnistamaan helposti tarvittavat dokumentaatiot ja esittämään ne oma-aloitteisesti auditoijalle. Puutteet turvallisuusjohtamisessa voivat johtaa siihen, että turvallisuuden hallintajärjestelmän eri elementit, kuten jäännösriskien hallinta tai suojattavien kohteiden hallinta, on laadittu toisistaan irrallisina osioina ja turvallisuuden hallintajärjestelmän rajapintoja muihin johtamisen hallintajärjestelmiin ei ole kuvattu. Ellei turvallisuusjohtamisen laatu ole korkea, erikseen auditointia varten kerätty materiaali ei muodosta selkeää kuvaa turvallisuuden hallinnan kokonaisuudesta. Tällöin voidaan joutua laatimaan erillinen kokonaiskuvaus auditoijaa varten.

# 4 Pohdinta

Kehitysprojektin tavoitteena oli selvittää, mikä on auditoitavan valmistautumisen vaikutus turvallisuusauditoinnin sujuvuuteen. Haastatteluaineiston perusteella määriteltiin valmistautumisen aktiviteetit, sujuvuuteen vaikuttavat tekijät ja niiden väliset yhteydet. Tulosten perusteella laadittiin valmistautumisohje auditoitavalle (liite). Ohjeessa kuvattiin, miten auditoinnin sujuvuuden vaikuttavat tekijät tulee huomioida auditoitavan valmistautumisessa. Laadittu ohje soveltuu turvallisuuden hallintajärjestelmän auditoinneille riippumatta arviointikehikosta ja organisaatiosta.

## 4.1 Tutkimuskysymykseen vastaaminen

Kehitysprojektin päätutkimuskysymys muotoiltiin tavoitteen mukaisesti: *Miten auditoitavan valmistautumisella voidaan vaikuttaa turvallisuusauditoinnin sujuvuuteen?*

Kehitysprojektin tutkimuskysymykseen vastataan kolmen asetetun apututkimuskysymyksen kautta. Ensimmäisenä vastataan valmistautumisen aktiviteetteihin ja toisena auditoinnin sujuvuuteen vaikuttaviin tekijöihin. Lopuksi kolmantena vastataan sujuvuuteen vaikuttavien tekijöiden ja auditoinnin valmistautumisen aktiviteettien välisiin yhteyksiin.

Kehitysprojektin ensimmäinen apututkimuskysymys oli:
*Mistä aktiviteeteistä koostuu auditoitavan turvallisuusauditointiin valmistautuminen?*

Valmistautumisen aktiviteettien luokittelun pohjana käytettiin Goel et al. (2006, 3-8) auditointiprosessin aktiviteetteja soveltuvin osin. Osa-alueet muotoutuivat aineiston perusteella seuraavasti: 1) sisällön määrittäminen, 2) suunnitelman laatiminen, 3) osallistujien valitseminen, ja 4) materiaalien kerääminen.

Kehitysprojektin toinen apututkimuskysymys oli:
*Mitkä tekijät vaikuttavat turvallisuusauditoinnin sujuvuuteen?*

Auditointien sujuvuuteen vaikuttavien tapahtumien ja niihin johtaneiden syiden analysoinnissa toistuivat tietyt asiat. Näistä muodostettiin neljä aineistolähtöistä tekijää: 1) johdon sitoutuminen, 2) turvallisuusjohtamisen laatu, 3) auditoinnin merkityksellisyys, ja 4) auditointiosaaminen.

Kehitysprojektin kolmas apututkimuskysymys oli:
*Miten sujuvuuteen vaikuttavia tekijöitä voidaan huomioida auditoitavan valmistautumisessa?*

Kehitysprojektissa huomattiin, että mitkä sujuvuuteen vaikuttavat tekijät tulee huomioida kussakin valmistautumisen aktiviteetissa. Sisällön määrittelyssä ja osallistujien valitsemisessa tulee huomioida kaikki neljä sujuvuuteen vaikuttavaa tekijää. Suunnitelman laatimisessa tulee huomioida turvallisuusjohtamisen laatu, auditoinnin merkityksellisyys ja auditointiosaaminen. Materiaalin keräämisessä on huomioitava turvallisuusjohtamisen laatu ja auditoinnin merkityksellisyys. Toimenpiteet auditoinnin sujuvuuden varmistamiseksi on esitelty valmistautumisen osa-alueittain kehitysprojektin tuloksissa. Lisäksi liitteenä olevassa ohjeessa on kuvattu toteutusesimerkkejä.

## 4.2 Rajoitukset

Tutkimusmenetelmäksi valittu laadullinen tutkimus rajoittaa tulosten yleistettävyyttä. Menetelmään päädyttiin, koska teoriaa turvallisuusauditointien sujuvuudesta ei ollut käytettävissä ja toisaalta tavoitteena oli ymmärtää ilmiötä prosessissa toimivien näkökulmasta. Aineistonhankinta toteutettiin teemahaastatteluin, joissa teemoille oli laadittu niihin johdattelevat puolistrukturoidut apukysymykset seuraavasti: *Kuvaile merkittävä tapahtuma, joka on vaikuttanut positiivisesti tai negatiivisesti turvallisuusauditoinnin sujuvuuteen [teemassa]?”* ja *”Mikä valmisteluvaiheessa sai sen aikaan (positiivinen) tai olisi voinut sen estää (negatiivinen)?”*. Aineiston analysointi aloitettiin laatimalla tapahtumien kuvaukset vastamaalla seuraaviin kysymyksiin: 1) *”Mikä tapahtuma vaikutti auditoinnin sujuvuuteen?”*, 2) *”Miten tapahtuma vaikutti auditoinnin sujuvuuteen?”*, 3) *”Mikä asia johti tapahtumaan?”* ja 4) *”Miten tapahtuma tulee huomioida auditointiin valmistautumisessa?”*. Tapahtumien kuvasten laadinnassa todettiin haasteita aineistojen jä-

sentämisessä jälkikäteen neljän edellä esitetyn kysymyksen kautta. Teemahaastatteluiden aineistosta ei selvästi löytynyt vastausta jokaiseen neljään kysymykseen. Epäselväksi jäi, johtuiko se siitä, että asia ei ollut tiedossa haastateltavalla vai siitä, että asiaa ei käsitelty haastattelussa. Tapahtumakuvausten laatimista varten luotujen neljän kysymysten käyttäminen haastattelujen ohjaamisessa olisivat parantaneen kehitysprojektin validiteettia ja uskottavuutta. Tällöin aineiston kerääminen olisi voinut kohdistua paremmin siihen mitä oli tarkoitus tutkia ja tapahtumien kuvaukset olisivat voineet vastata paremmin haastateltavien näkemystä.

Kriittisten tapahtumien menetelmässä aineiston edustavuuden kannalta keskeistä on havaittujen tapahtumien määrä, ei tutkimukseen osallistuvien määrä. Kehitysprojektissa haastateltiin kolmea henkilöä, joilla on pitkäaikainen kokemus tutkittavasta ilmiöstä. Kerätyn aineiston perusteella muodostettiin 33 auditoinnin sujuvuuteen vaikuttanutta kriittistä tapahtumaa. Osin haastateltavien kuvaamissa tapahtumissa oli samankaltaisuuksia muiden haastateltavien tapahtumien kesken. Toisaalta kaikilta haastateltavilta saatiin tapahtumia, joita ei tullut muilta haastateltavilta. Näin voidaan todeta, että uusien haastateltavien myötä tutkittavasta ilmiöstä olisi todennäköisesti saatu lisää tietoa. Täten arvioitiin, että aineisto ei riitä tutkimusongelman selittämiseen eikä aineiston kyllääntymistä saavutettu.

Auditoitavalle laadittu valmistautumisohje (liite) ei ole tarkoitettu käytettäväksi itsenäisenä ja ainoa ohjeena auditointiin valmistautumisessa. Sitä tulee soveltaa auditoinnissa käytettävän vaatimuskehikon rinnalla ja mahdollisten muiden ohjeiden tukena auditointiin valmistautumisessa. Vaatimuskehikon kautta määrittyy auditoinnin lopputulos ja liitteen ohjeen avulla voidaan vaikuttaa siihen, miten sujuvasti vaatimuskehikon määrittelemään lopputulokseen voidaan päästä.

## 4.3 Tulosten merkitys

Kehitysprojektin tavoitteena oli nostaa esiin asioita, jotka parantavat auditoinnin sujuvuutta riippumatta siitä vaikuttavatko ne auditoinnin lopputulokseen. Auditoitavalle laaditut ohjeet painottuvat usein asioihin, joilla yritetään vaikuttaa suoraan auditoinnin lopputulokseen. Turvallisuusauditoinnin prosessia on tutkittu verrattain vähän ja aikaisempi tutkimus on keskittynyt pääasiassa auditoijan näkökulmaan. Auditoinnin sujuvuuteen vaikuttavia tekijöitä ei ole aikaisemmin tutkittu juurikaan. Kehitysprojektin tunnistettiin

neljä auditoinnin sujuvuuteen vaikuttavaa tekijää, joiden kautta auditoitava voi vaikuttaa auditoinnin sujuvuuteen omalla valmistautumisellaan.

Tulosten perusteella johtamisen voidaan sanoa olevan tärkeä taustatekijä auditoinnin sujuvuudelle. Turvallisuusjohtamisen laatu kertoo myös johtamisenkin laadusta. Lisäksi muut löydetyt tekijät ovat sellaisia, joihin organisaatiossa voidaan vaikuttaa johtamisella. Johdon sitoutuminen auditointiin osoittaa kiinnostusta ja toisaalta esimerkillä johtamista. Merkityksellisyyden osoittaminen on johdon tehtävä laajemminkin organisaation tavoitteiden saavuttamisessa. Henkilöiden oikeanlainen sijoittaminen eri tehtäviin osaamisensa mukaan ja toisaalta henkilöstön osaamisen kehittäminen ovat keskeisiä lähijohtamisen tehtäviä.

## 4.4 Tulosten luotettavuus

Laadullisen tutkimuksen luotettavuutta voidaan arvioida monin keinoin. Reliabiliteetin ja validiteetin käsitteitä on käytetty perinteisesti arvioitaessa määrällisen tutkimuksen luotettavuutta. Kuitenkin myös laadullisessa tutkimuksessa tulosten luotettavuutta voidaan arvioida reliabiliteetin ja validiteetin käsitteitä soveltaen, kuten tässä kehitysprojektissa on tehty validiteettiin painotuen. Lisäksi tuloksia on arvioitu myös uudempien luotettavuuden käsitteiden kautta kuten uskottavuuden, vakuuttavuuden ja vahvistuvuuden. Lopuksi on arvioitu myös tulosten hyödynnettävyyttä ja yleistettävyyttä.

Tulosten reliabiliteettia eli tutkimustulosten toistettavuutta parannettiin haastatteluiden tallentamisella ja kirjoittamalla auki sujuvuuteen vaikuttavien tekijöiden ja valmistautumisen osa-alueiden luokat sekä tapahtumakuvasten osioiden määrittelyt. Reliabiliteettia olisi pystytty edelleen parantamaan haastattelua kehittämällä esimerkiksi esitestauksen avulla, jolloin olisi pystytty parantamana haastattelukysymyksiä. Kaikki haastateltavat olivat toimineet sekä auditoijana että auditoitavana, kokemuksen kuitenkin painottuessa merkittävästi auditoijana toimimiseen.

Tulosten validiteettia eli kuvausten ja tulkinnan oikeellisuutta arvioitiin erikseen. Kuvauksen validiteetin suurimmat haasteet liittyivät aineiston tarkkuuteen ja kattavuuteen. Aineiston tarkkuuden heikkoutena oli edellä mainittu haastattelukysymysten epämääräisyydestä johtunut tapahtumakuvausten epätarkkuus. Aineiston tarkkuutta olisi voinut parantaa käyttämällä tapahtumakuvausten luontiin laadittuja kysymyksiä jo haastattelu vaiheessa. Koska

haastateltavien kertomissa tapahtumissa löytyi toisistaan poikkeavia tapahtumia, niin aineisto ei ollut kyllääntynyt. Tällöin aineiston kattavuus ei ole riittävä kuvaamaan tutkittavaa ilmiötä kokonaisuudessaan. Kattavuutta olisi parantanut tapahtumien määrän lisääminen joko pidentämällä haastatteluaikaa tai haastattelemalla useampia henkilöitä. Lisäaineiston analysointi olisi vaatinut merkittävästi lisää resursseja. Aineiston epätarkkuus on voinut johtaa kuvausten tulkintaan tutkijan omien käsitysten suuntaan heikentäen tulkinnan validiteettia.

Tulosten uskottavuutta olisi parantanut tehtyjen tulkintojen oikeellisuuden varmistaminen haastateltavilta ja samalla olisi saatu palautetta mahdollisesta tutkijan omien käsitysten vaikutuksesta tulosten validiteettiin. Tulosten vakuuttavuudessa havaittiin haasteita kehitysprojektin esittelyissä, jonka myötä kehitysprojektissa tunnistettujen luokkien kuvauksia ja tulosten esittelyä yleisesti muokattiin helpommin ymmärrettävään muotoon. Kehitysprojektissa ei löydetty aihetta käsitellyttä aikaisempaa tutkimusta, joihin saatuja tuloksia olisi voinut verrata tulosten vahvistuvuuden arvioimiseksi. Yleisesti tulosten pätevyyttä ja luotettavuutta parannettiin kuvaamalla perusteellisesti aineiston hankinnassa ja analysoinnissa käytetyt menetelmät ja periaatteet.

*Tulosten hyödynnettävyys*

Laadittua ohjetta voidaan hyödyntää käytännön tasolla Puolustusvoimien valmistautumisessa sisäisiin auditointeihin sekä ulkoisiin auditointeihin, jotka kohdistuvat Puolustusvoimiin. Ohjetta on mahdollista myös jakaa tarvittaessa ulkopuolisen organisaation tueksi sen valmistautuessa Puolustusvoimien suorittamaan turvallisuusauditointiin. Ohje soveltuu turvallisuuden hallintajärjestelemän auditointiin valmistautumiseen riippumatta käytettävästä vaatimuskehikosta.

Tuloksia voidaan hyödyntää Puolustusvoimien turvallisuusauditointiprosessien kehittämisessä. Niitä on mahdollista hyödyntää myös laajemmin turvallisuuden johtamisen ja hallintajärjestelmien parantamisessa tunnistettujen tekijöiden avulla.

*Tulosten yleistettävyys*

Laadullisessa tutkimuksessa yleistämisellä ei tarkoiteta tilastollisista merkittävyyttä. Perusteellisella yksittäisen tapauksen tutkimuksella, voidaan kuitenkin saada esille se, mikä ilmiössä saattaa toistua yleisemmässäkin tarkastelussa. Sisäisellä yleistettävyydellä tarkoitetaan tulkintojen yleistettävyyttä tutkittavassa tilanteessa. Haastateltavat valittiin sillä perusteella, että heidän kokemus edustaa mahdollisimman hyvin turvallisuusauditointeja Puolustusvoimien toimintaympäristössä. Täten tulosten voidaan olettaa olevan sisäisesti yleistettäviä Puolustusvoimien toimintaympäristössä.

Ulkoisella yleistettävyydellä tarkoitetaan tulkintojen yleistettävyyttä tutkittavan tilanteen yli. Lähtökohtaisesti ei ole syytä olettaa, että tulokset olisivat ulkoisesti yleistettävissä. Haastateltavat omaavat pitkäaikaisen kokemuksen ja tuoreen käytännön näkemyksen turvallisuusauditoinneista. Osalla haastateltavissa on auditointikokemusta myös Puolustusvoimien toimintaympäristön ulkopuolisista auditoinneista. Lisäksi kaikki haastateltavat olivat osallistuneet Puolustusvoimien ulkopuolisiin auditointikoulutuksiin. Haastateltavat ovat käyttäneet laajemminkin valtionhallinnossa käytettyjä vaatimuskehikoita (VAHTI 2/2010 ja Katakri 2015) ja laajasti myös yritysmaailmassa käytettyä vaatimuskehikkoa (ISO/IEC 27001). Haastateltavien pitkäaikaisen ja monipuolisen kokemuksen johdosta aineiston tulkinnoissa voi olla piirteitä, jotka saattavat toistua yleisemmässä tarkastelussa.

Teoreettisella yleistettävyydellä tarkoitetaan tulkintojen yleistettävyyttä muihin tutkimuksiin verrattuna. Vertailukohteeksi ei löydetty soveltuvia tutkimuksia. Täten tulkintojen ei voida olettaa olevan teoreettisesti yleistettävissä.

## 4.5 Suositukset jatkotutkimukselle

Kehitysprojektia voi jatkaa määrällisellä tutkimuksella, jossa varmennetaan tekijöiden vaikuttavuutta auditoinnin sujuvuuteen tilastollisesti. Tekijöille ja sujuvuudelle voidaan laatia väittämien avulla mittarit. Mukaan voisi ottaa myös taloudellista vaikutusta kuvaavia mittareita. Määrällisellä tutkimuksella voitaisiin todeta myös, miten voimakkaasti eri tekijät vaikuttavat auditoinnin sujuvuuteen. Kysely voidaan toteuttaa sekä auditoitaville että auditoijille useista eri auditointitilanteista.

Tutkimusta voi laajentaa ottamalla mukaan teoriaa tekijöiden taustaksi. Motivaatio- tai johtamisteoriat voivat sopia tekijöiden tarkempaan teoreettiseen tarkasteluun. Tällöin voitaisiin ymmärtää syvällisemmin tekijöiden taustalla vaikuttavia asioita ja selvittää niiden vaikutusta yleisemmässä kontekstissa.

## 4.6 Yhteenveto

Hyvällä valmistautumisella auditoitava voi varmistaa auditoinnin sujuvuutta. Tässä työssä on esitelty tekijöitä, joiden avulla auditointivaihe voi olla sujuvampi. Turvallisuuden hallintajärjestelmän auditoinnin järjestäminen on usein turvallisuudesta vastaavan päällikön tehtävänä. Tekijöiden huomioiminen mahdollistaa valmistautumistyön suuntaamisen tarvittaviin aktiviteetteihin, jolloin auditointiin käytetyille panostuksille on mahdollista saada parempi pääoman tuottoaste. Riippumatta siitä, mikä on auditoinnin tavoitteena, sujuvuuteen vaikuttavien tekijöiden huomioimisella valmistautumisvaiheessa voidaan saavuttaa todenmukaisempi lopputulos auditointivaiheessa. Se voi tarkoittaa parempaa turvallisuuden kypsyyden tilannekuvaa, vakavampien haavoittuvuuksien tunnistamista, laadukkaampaa vertailua standardeihin tai kattavampaa lainmukaisuuden varmistamista. Tällöin auditoinnin havainnot ovat paremmin hyödynnettävissä toiminnan kehittämisessä. Tuottoaste voi parantua myös lyhyempien ja lukumäärältään vähempien auditointien kautta. Sujuvuuteen vaikuttavien tekijöiden huomioimisella on mahdollista parantaa myös auditoijan ja auditoitavan välistä luottamusta.

*Turvallisuusauditointi - uhka vai mahdollisuus?*

Turvallisuusauditoinnin järjestäminen saatetaan pitää uhkana, jos auditoijan tunnistamien puutteiden koetaan kohdistuvan organisaation sijasta suoraan turvallisuudesta vastaaviin henkilöihin. Auditoinnin vaatima työmäärä voidaan nähdä uhkana, jos sitä pidetään suurena odotettuihin hyötyihin nähden. Turvallisuusauditointi tulisikin nähdä mahdollisuutena nostaa esiin hyvin tehdyt asiat ja tunnistaa osa-alueita, joita täytyy vielä parantaa. Avoin ja rakentava vuorovaikutus auditoijan ja auditoitavan välillä edesauttaa tilanteen näkemistä mahdollisuutena. Kun johto on sitoutunut auditointiin, turvallisuusjohtaminen on laadukasta, auditoinnin merkityksellisyys on selvä ja osallistujilla on riittävästi osaamisesta auditoinneista, on helpompi nähdä turvallisuusauditointi positiivisena asiana. Tällöin turvallisuusauditointi näyttäytyy auditoitavalle enemmän mahdollisuutena oman turvallisuuden hallinnan kehittämiselle kuin kritiikkinä tai uhkana puutteiden paljastumiselle.

# Lähteet

Bott, G., & Tourish, D. (2016). The critical incident technique reappraised. *Qualitative Research in Organizations and Management: An International Journal*.

Finlex 1101/2019. Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2019/20191101, haettu 4.6.2020.

Finlex 1406/2011. Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista, saatavilla https://www.finlex.fi/fi/laki/ajantasa/2011/20111406, haettu 4.6.2020.

Finlex 551/2007. Laki puolustusvoimista, saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2007/20070551, haettu 4.6.2020.

Finlex 588/2004. Laki kansainvälisistä tietoturvallisuusvelvoitteista, saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2004/20040588, haettu 4.6.2020.

Flanagan, J. C. (1954). The critical incident technique. *Psychological bulletin*, *51*(4), 327.

Goel, S., Pon, D., & Menzies, J. (2006). Managing information security: Demystifying the audit process for security officers. *Journal of Information System Security*, *2*(2), 25-45.

Hettlage, R., & Steinlin, M. (2006). The critical incident technique in knowledge management-related contexts. *), Ingenous peoples knowledge. Swiss Association for International Cooperation: Zurich*.

Jaakola, A. M., Vornanen, R., & Pölkki, P. (2014). Kriittisten tapahtumien menetelmä lastensuojelun sosiaalityötä koskevassa tutkimuksessa. *Janus Sosiaalipolitiikan ja sosiaalityön tutkimuksen aikakauslehti*.

Rajamäki, J. (2014, September). Challenges to a smooth-running data security audits. Case: A Finnish national security auditing criteria KATAKRI. In *2014 IEEE Joint Intelligence and Security Informatics Conference* (pp. 240-243). IEEE.

Serrat, O. (2017). The critical incident technique. In *Knowledge Solutions* (pp. 1077-1083). Springer, Singapore.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economia*, 14(1), 43.

SUPO 2019. Kansallisen turvallisuuden katsaus, Suojelupoliisi, saatavilla: https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/78653_20191205_Supo_kansallinen_turvallisuus_web.pdf?f546eb9c6979d788, haettu 4.6.2020.

VAHTI 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, saatavilla: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet, haettu 4.7.2020.

Katakri 2015 – tietoturvallisuuden auditointityökalu viranomaisille, saatavilla: https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille, haettu 4.6.2020.

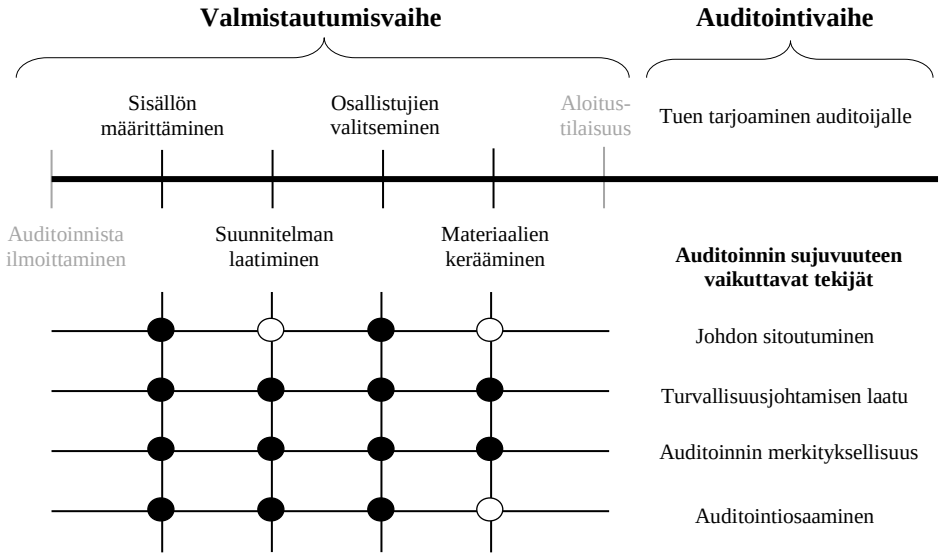
ISO/IEC 27001:2017 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Vahvistettu 03.03.2017.

# Liitteet

## Auditoitavan valmistautumisohje

Ohjeessa on kuvattu, miten auditoinnin sujuvuuden vaikuttavat tekijät tulee huomioida auditoitavan valmistautumisessa. Ohje soveltuu tiedon suojaamiseksi toteutetun turvallisuuden hallintajärjestelmän auditoinneille riippumatta arviointikehikosta ja organisaatiosta. Se on tarkoitettu käytettäväksi auditoinnin vaatimuskehikon rinnalla ja mahdollisten muiden ohjeiden tukena auditointiin valmistautumisessa. Vaatimuskehikon kautta määrittyy auditoinnin lopputulos ja tämän ohjeen avulla voidaan vaikuttaa siihen, miten sujuvasti vaatimuskehikon määrittelemään lopputulokseen voidaan päästä.

Ohjeessa auditointiprosessi koostuu kahdesta peräkkäisestä vaiheesta: 1) valmistautumisvaihe ja 2) auditointivaihe. Ohjeen toimita-ajatus on seuraava: Aktiviteetti → Toimenpide → Tekijä → Auditoinnin sujuvuus. Valmistautumisvaiheen tietyissä aktiviteeteissä tehdyillä toimenpiteillä voidaan vaikuttaa tiettyihin sujuvuuteen vaikuttaviin tekijöihin ja sitä kautta auditointivaiheen sujuvuuteen (kuva 1).




**Kuva 1** Kussakin aktiviteetissa huomioitavat sujuvuuteen vaikuttavat tekijät

Ohjeessa aktiviteetilla tarkoitetaan seuraavia valmistautumisvaiheen toimintoja: 1) sisällön määrittäminen, 2) suunnitelman laatiminen, 3) osallistujien valitseminen, ja 4) materiaalien kerääminen (kuva 1). Valmistautumisohje koostuu neljästä aktiviteettien mukaan laaditusta ohjekortista. Aktiviteettien tarkemmat määritelmät löytävät kyseisestä ohjekortista.

Ohjeessa tekijällä tarkoitetaan seuraavia auditoinnin sujuvuuteen vaikuttavia tekijöitä: 1) johdon sitoutuminen, 2) turvallisuusjohtamisen laatu, 3) auditoinnin merkityksellisyys, ja 4) auditointiosaaminen (kuva 1). Ohjekorteissa on käyty läpi kussakin aktiviteetissa huomiotavat tekijät (kuva 1). Osa tekijöistä tulee huomioida kaikissa aktiviteeteissa ja osa vain tietyissä aktiviteeteissa Tekijöiden osalta on kuvattu määritelmät, niiden huomioiminen yleisesti kyseisessä aktiviteetissa ja toteutusesimerkkejä valmistautumisen toimenpiteistä auditointivaiheen sujuvuuden varmistamiseksi.

**1) Sisällön määrittäminen**

Auditoinnin tarkoituksen ja merkityksen selventäminen, käytettävien vaatimusten määrittäminen ja auditoinnin kohteen rajaaminen.

- Selvennetään mihin auditoinnilla pyritään ja miksi se on tärkeä organisaatiolle.
- Määritetään mitkä on käytettävät vaatimukset ja millä tasolla niitä tarkastellaan.
- Rajataan mitä toimintoja tai organisaation osia auditoinnissa tarkastellaan.

Näiden selventämisen tärkeys korostuu, jos auditoitavalla ei ole aikaisempaa kokemusta turvallisuusauditoinneista.

Auditoinnin sisällön määrittelyssä tulee huomioida kaikki neljä auditoinnin sujuvuuteen vaikuttavaa tekijää: johdon sitoutuminen, turvallisuusjohtamisen laatu, auditoinnin merkityksellisyys ja auditointiosaaminen.

**Toimenpiteet auditoinnin sujuvuuden varmistamiseksi**

| | |
|---|---|
| Johdon sitoutuminen | *Johdon sitoutuminen*<br><br>Johdon oma osallistuminen auditointiin, tuen ja päätöksentekomandaatin antaminen auditointiin osallistuville sekä asianmukaisen painoarvon antaminen auditoinnin tuloksille.<br><br>• Mahdollistaa turvallisuuden hallinnan tarkastelun osana organisaation johtamista sekä keskustelut investointeja vaativista korjaavista toimenpiteistä.<br>• Mahdollistaa auditoinnin suositusten ja korjaavien toimenpiteiden sujuvan toimeenpanon.<br><br>*Johdon sitoutuminen sisällön määrittelyssä*<br><br>Johto on sitoutettava auditointiin jo sisältöä määriteltäessä, jotta johdon tuki on käytettävissä auditoinnin tuloksesta riippumatta. Jälkikäteen voi olla vaikeaa saada riittäviä resursseja auditoinnin suosituksille ja korjaaville toimenpiteille.<br><br>*Toteutusesimerkkejä*<br><br>• Auditoinnin tarkoitus ja merkitys on selvennetty johdolle |
| Turvallisuusjohtamisen laatu | *Turvallisuusjohtamisen laatu*<br><br>Auditoitavat ymmärtävät turvallisuuden kokonaishallinnan periaatteet ja turvallisuuden toteutuksen omassa organisaatiossa.<br><br>• Mahdollistaa hallintajärjestelmän toiminnan kokonaisuuden kuvaamisen.<br>• Mahdollistaa oikeiden henkilöiden valinnan auditointiin<br>• Mahdollistaa oma-aloitteisen turvallisuuden hallinnan tilannekuvan esittämisen.<br><br>*Turvallisuusjohtamisen laatu sisällön määrittelyssä*<br><br>Jos turvallisuusjohtamisen laatu on matala, auditoinnin rajaus voi jäädä epäselväksi. Tällöin auditointi ei kohdistu oikeaan osaan organisaatiossa tai auditoinnissa ei tarkastella kohteen kannalta oikeita asioita.<br><br>*Toteutusesimerkkejä*<br><br>• Auditoinnin rajaus on tehty auditoinnin sisällön määrittelyn yhteydessä. |

| | |
|---|---|
| Auditoinnin merkityksellisyys | *Auditoinnin merkityksellisyys*<br><br>Auditointiin osallistuva henkilöstö ymmärtää mihin turvallisuusauditoinnilla pyritään ja miksi se on tärkeä kohdeorganisaatiolle.<br><br>• Mahdollistaa auditoitavan organisaation tuen auditointiprosessille ja auditointitilaisuuden läpiviennille.<br>• Mahdollistaa todenmukaiseen tilannekuvaan perustuvan valmistautumisen ja auditoinnin.<br><br>*Auditoinnin merkityksellisyys sisällön määrittelyssä*<br><br>Auditoinnin tarkoitus ja merkitys tulee selkiyttää auditoinnin sisällön määrittelyn yhteydessä. Jos auditoinnin merkityksellisyyttä ei ymmärretä, auditoitavat saattavat kiistää auditoinnin oikeutuksen ja olla tekemättä yhteistyötä auditoijan kanssa. Tunnistettuja turvallisuuspuutteita saatetaan myös peitellä.<br><br>*Toteutusesimerkkejä*<br><br>• Auditoinnin tarkoitus ja merkitys on selkiytetty auditointiprosessin alussa. |
| Auditointiosaaminen | *Auditointiosaaminen*<br><br>Auditoitavat tuntevat auditointikehikon vaatimukset ja osaavat soveltaa niitä omassa toimintaympäristössään.<br><br>• Mahdollistaa vaatimusten soveltamisen eri vaatimuskehikoiden välillä<br>• Mahdollistaa auditoinnin tulosten vertailun edellisiin auditointeihin, vaikka vaatimukset ja/tai toimintaympäristö olisi muuttunut.<br><br>*Auditointiosaaminen sisällön määrittelyssä*<br><br>Auditointiosaamisesta tarvitaan, jotta auditoitava voi valmistautua esittämään organisaation turvallisuuden hallinnan toteutuksen auditoinnin vaatimuskehikkoa vasten. Osaamisen tarve korostuu etenkin, jos turvallisuusauditointi toteutetaan eri vaatimuskehikolla kuin mihin organisaation turvallisuuden hallintajärjestelmä perustuu. Jos osaamisessa on puutteita, auditoitava ei ymmärrä heille asetettuja vaatimuksia eikä osaa kertoa miten vaatimuksia on sovellettu.<br><br>*Toteutusesimerkkejä*<br><br>• Käytettävät vaatimukset ja vaatimustasot on selkiytetty sisällön määrittelyn yhteydessä. |

**2) Suunnitelman laatiminen**

Auditoitavien toimintojen suunnittelu, turvallisuuden hallintajärjestelmän kokonaisuuden kuvaaminen ja turvallisuuden tilanteen tunnistaminen.

- Kuvataan turvallisuuden hallintajärjestelmä ja sen ylläpitäminen sekä sen liittyminen muihin hallintajärjestelmiin kuten riskienhallintaan.
- Arvioidaan turvallisuuden hallinnan tila ja tunnistetaan puutteet dokumentaatiossa tai turvallisuuden toteutuksessa sekä laaditaan korjausesitykset.

Auditoinnin suunnitelman laatimisessa tulee huomioida sujuvuuteen vaikuttavista tekijöistä turvallisuusjohtamisen laatu, auditoinnin merkityksellisyys ja auditointiosaaminen.

**Toimenpiteet auditoinnin sujuvuuden varmistamiseksi**

Turvallisuusjohtamisen laatu

*Turvallisuusjohtamisen laatu*

Auditoitavat ymmärtävät turvallisuuden kokonaishallinnan periaatteet ja turvallisuuden toteutuksen omassa organisaatiossa.

- Mahdollistaa hallintajärjestelmän toiminnan kokonaisuuden kuvaamisen.
- Mahdollistaa oikeiden henkilöiden valinnan auditointiin
- Mahdollistaa oma-aloitteisen turvallisuuden hallinnan tilannekuvan esittämisen.

*Turvallisuusjohtamisen laatu suunnitelman laatimisessa*

Jos turvallisuusjohtamisen laatu on korkea, turvallisuuden hallintajärjestelmä ohjaa organisaation toimintaa ja sitä on ylläpidetty tarpeen mukaan. Turvallisuusasioita on myös käsitelty johdon kanssa.

*Toteutusesimerkkejä*

- Sisällön määrittelyn perusteella on laadittu suunnitelmat auditoitaville toiminnoille.
- Hallintajärjestelmä ja sen liittyminen organisaation muuhun toimintaan on kuvattu.
- Hallintajärjestelmää on ylläpidetty dokumentoidusti.

Auditoinnin merkityksellisyys

*Auditoinnin merkityksellisyys*

Auditointiin osallistuva henkilöstö ymmärtää mihin turvallisuusauditoinnilla pyritään ja miksi se on tärkeä kohdeorganisaatiolle.

- Mahdollistaa auditoitavan organisaation tuen auditointiprosessille ja auditointitilaisuuden läpiviennille.
- Mahdollistaa todenmukaiseen tilannekuvaan perustuvan valmistautumisen ja auditoinnin.

*Auditoinnin merkityksellisyys suunnitelman laatimisessa*

Jos auditoinnin merkityksellisyys ymmärretään, auditoinnin suunnittelu perustuu todenmukaiseen turvallisuuden tilannekuvaan. Jos merkityksellisyys on epäselvä, saatetaan laatia erilaisia ohjeistuksia tai jopa koko turvallisuuden hallintajärjestelmä vain auditointia varten. Tällöin organisaation toiminta ei vastaa auditoinnissa esitettyä dokumentaatiota.

Toteutusesimerkkejä

- Tilanteen arviossa on käytetty jalkautettuja ja käytössä olevia toimintatapoja.
- Vaatimustenmukaisuuden todentaminen on suunniteltu ja puutteet dokumentaatiossa on tunnistettu.
- Hallintajärjestelmä ja sen ylläpitäminen on kuvattu.

| | |
|---|---|
| Auditointiosaaminen | *Auditointiosaaminen*<br><br>Auditoitavat tuntevat auditointikehikon vaatimukset ja osaavat soveltaa niitä omassa toimintaympäristössään.<br><br>• Mahdollistaa vaatimusten soveltamisen eri vaatimuskehikoiden välillä<br>• Mahdollistaa auditoinnin tulosten vertailun edellisiin auditointeihin, vaikka vaatimukset ja/tai toimintaympäristö olisi muuttunut.<br><br>*Auditointiosaaminen suunnitelman laatimisessa*<br><br>Hyvällä auditointiosaamisella pystytään tulkitsemaan auditoinnin vaatimustaso oikein. Auditointiosaamisen merkitys korostuu, jos organisaatiossa ei ole erillistä turvallisuuden hallintajärjestelmää, vaan turvallisuutta hallitaan osana muita johtamisjärjestelmiä. Tällöin turvallisuuden hallinnasta voidaan joutua laatimaan erillinen kuvaus kokonaisuuden esittämiseksi auditoijalle.<br><br>*Toteutusesimerkkejä*<br><br>• Organisaation turvallisuuden hallinta on arvioitu auditoinnin vaatimuskehikon näkökulmasta<br>• Turvallisuuden hallinnan rajapinnat on tunnistettu. |

**3) Osallistujien valitseminen**

Auditoitavista osa-alueista vastaavien henkilöiden ja johdon tai resursseista vastaavien tahojen valinta auditointitiimiin sekä auditointitiimin perehdyttäminen auditoinnin tarkoitukseen ja toteutustapaan.

- Valitaan auditoitavista toiminnoista vastaavat henkilöt auditointiin.
- Varmistutaan osallistujien riittävästä auditointi- ja hallintajärjestelmäosaamisesta
- Osallistetaan resursseista päättävä taho tai vaaditaan mandaatti muille osallistujille.
- Perehdytetään osallistujille auditoinnin merkitys ja toteutustapa.

Auditoinnin osallistujien valitsemisessa tulee huomioida kaikki neljä auditoinnin sujuvuuteen vaikuttavaa tekijää: johdon sitoutuminen, turvallisuusjohtamisen laatu, auditoinnin merkityksellisyys ja auditointiosaaminen.

**Toimenpiteet auditoinnin sujuvuuden varmistamiseksi**

| | |
|---|---|
| Johdon sitoutuminen | *Johdon sitoutuminen*<br><br>Johdon oma osallistuminen auditointiin, tuen ja päätöksentekomandaatin antaminen auditointiin osallistuville sekä asianmukaisen painoarvon antaminen auditoinnin tuloksille.<br><br>• Mahdollistaa turvallisuuden hallinnan tarkastelun osana organisaation johtamista sekä keskustelut investointeja vaativista korjaavista toimenpiteistä.<br>• Mahdollistaa auditoinnin suositusten ja korjaavien toimenpiteiden sujuvan toimeenpanon.<br><br>*Johdon sitoutuminen osallistujien valitsemisessa*<br><br>Resursseista vastuussa olevien johtajien tulee osallistua auditointiin. Vaihtoehtoisesti voidaan antaa mandaatti resurssipäätösten tekemiseen muille auditointiin osallistuville.<br><br>*Toteutusesimerkkejä*<br><br>• Johdon tulee olla mukana auditointiin valmistautumisessa ja on osallistuttava auditointitilaisuuteen.<br>• Ellei resursseista päättävä taho ole edustettuna, on mandaatti annettu jollekin muulle auditointiin osallistuvalle.<br>• Osallistujiksi on valittu tarkasteltavista osa-alueista vastaavat johtajat |
| Turvallisuusjohtamisen laatu | *Turvallisuusjohtamisen laatu*<br><br>Auditoitavat ymmärtävät turvallisuuden kokonaishallinnan periaatteet ja turvallisuuden toteutuksen omassa organisaatiossa.<br><br>• Mahdollistaa hallintajärjestelmän toiminnan kokonaisuuden kuvaamisen.<br>• Mahdollistaa oikeiden henkilöiden valinnan auditointiin<br>• Mahdollistaa oma-aloitteisen turvallisuuden hallinnan tilannekuvan esittämisen.<br><br>*Turvallisuusjohtamisen laatu osallistujien valitsemisessa*<br><br>Auditointiin osallistuvat tulee valita työtehtäviensä perusteella. Mukana täytyy olla sekä auditoitavista asioista vastaavia henkilöitä, että niiden käytännön toteutukseen osallistuvia. Jos organisaation turvallisuusjohtaminen on korkealla tasolla, näiden roolien määrittäminen on helppoa.<br><br>*Toteutusesimerkkejä*<br><br>• Osallistujiksi on valittu auditoitavista toiminnoista vastaavat henkilöt.<br>• Osallistujien riittävästä auditointi- ja hallintajärjestelmäosaamisesta on varmistettu. |

| | |
|---|---|
| Auditoinnin merkityksellisyys | *Auditoinnin merkityksellisyys*<br><br>Auditointiin osallistuva henkilöstö ymmärtää mihin turvallisuusauditoinnilla pyritään ja miksi se on tärkeä kohdeorganisaatiolle.<br><br>• Mahdollistaa auditoitavan organisaation tuen auditointiprosessille ja auditointitilaisuuden läpiviennille.<br>• Mahdollistaa todenmukaiseen tilannekuvaan perustuvan valmistautumisen ja auditoinnin.<br><br>*Auditoinnin merkityksellisyys osallistujien valitsemisessa*<br><br>Osallistujien perehdyttämisessä on syytä varmistua, että auditoinnin tarkoitus on kaikille osallistujille selvänä. Myös auditoinnin toteutustapa on hyvä käydä läpi kaikkien osallistujien kanssa. Näin varmistetaan, että kaikki osallistujat ymmärtävät auditoinnin merkityksen organisaatiolle sekä osaavat valmistautua ja toimia valitun toteutustavan mukaisesti.<br><br>*Toteutusesimerkkejä*<br><br>• Auditoinnin tarkoitus ja merkitys on perehdytetty auditointiin osallistuville.<br>• Osallistujien ymmärtäminen toteutustavan valinnalle on varmistettu. |
| Auditointiosaaminen | *Auditointiosaaminen*<br><br>Auditoitavat tuntevat auditointikehikon vaatimukset ja osaavat soveltaa niitä omassa toimintaympäristössään.<br><br>• Mahdollistaa vaatimusten soveltamisen eri vaatimuskehikoiden välillä<br>• Mahdollistaa auditoinnin tulosten vertailun edellisiin auditointeihin, vaikka vaatimukset ja/tai toimintaympäristö olisi muuttunut.<br><br>*Auditointiosaaminen osallistujien valitsemisessa*<br><br>Osallistujiksi tulee lisäksi valita henkilöitä vahvalla auditointiosaamisella, jos sitä ei muuten ole riittävästi työtehtävien perusteella valituilla osallistujilla.<br><br>*Toteutusesimerkkejä*<br><br>• Osallistujien auditointiosaamisen riittävyys on varmistettu.<br>• Tarvittaessa osallistujia on lisätty auditointiosaamisen täydentämiseksi. |

**4) Materiaalien kerääminen**

Auditointiaineiston suunnittelu ja kerääminen sekä sen toimittaminen auditoijalle etukäteen.

- Suunnitellaan, miten tarkasteltavat asiat esitetään auditoijalle ja mitä tietoa niiden todentamiseksi tarvitaan.
- Kerätään aineistosuunnittelun mukaiset materiaalit ja tiedot
- Varmistutaan auditointiaineiston muodostaman turvallisuuden hallintajärjestelmän kokonaiskuvauksen riittävyydestä
- Toimitetaan auditointiaineisto auditoijalle etukäteen.

Auditointimateriaalien keräämisessä on huomioitava turvallisuusjohtamisen laatu ja auditoinnin merkityksellisyys.

**Toimenpiteet auditoinnin sujuvuuden varmistamiseksi**

| | |
|---|---|
| Turvallisuusjohtamisen laatu | *Turvallisuusjohtamisen laatu*<br><br>Auditoitavat ymmärtävät turvallisuuden kokonaishallinnan periaatteet ja turvallisuuden toteutuksen omassa organisaatiossa.<br><br>• Mahdollistaa hallintajärjestelmän toiminnan kokonaisuuden kuvaamisen.<br>• Mahdollistaa oikeiden henkilöiden valinnan auditointiin<br>• Mahdollistaa oma-aloitteisen turvallisuuden hallinnan tilannekuvan esittämisen.<br><br>*Turvallisuusjohtamisen laatu materiaalien keräämisessä*<br><br>Jos turvallisuusjohtamisen laatu on korkea, auditoitava pystyy tunnistamaan helposti tarvittavat dokumentaatiot ja esittämään ne oma-aloitteisesti auditoijalle. Turvallisuuden hallintajärjestelmän eri elementit on sovitettu yhteen ja rajapinnat muihin johtamisen hallintajärjestelmiin on kuvattu. Jos turvallisuusjohtamisen laatu ole matala, voidaan joutua laatimaan erillinen kokonaiskuvaus auditoijaa varten.<br><br>Toteutusesimerkkejä<br><br>• Tarkasteltavien asioiden esittäminen on suunniteltu ja niiden todentamiseksi tarvittavat tiedot on tunnistettu.<br>• Kerätyn materiaalin kattavuudesta ja laadusta on varmistuttu. |
| Auditoinnin merkityksellisyys | *Auditoinnin merkityksellisyys*<br><br>Auditointiin osallistuva henkilöstö ymmärtää mihin turvallisuusauditoinnilla pyritään ja miksi se on tärkeä kohdeorganisaatiolle.<br><br>• Mahdollistaa auditoitavan organisaation tuen auditointiprosessille ja auditointitilaisuuden läpiviennille.<br>• Mahdollistaa todenmukaiseen tilannekuvaan perustuvan valmistautumisen ja auditoinnin.<br><br>*Auditoinnin merkityksellisyys materiaalien keräämisessä*<br><br>Jos auditoinnin tarkoitus on selvä, niin auditoitava pystyy tunnistamaan ja toimittamaan tarvittavat tiedot etukäteen. Auditoinnin tarkoitus on huomioitava tarvittavan materiaalin keräämisessä, jotta sen perusteella pystytään tekemään arviot auditoitavasta kohteesta.<br><br>*Toteutusesimerkkejä*<br><br>• Suunnitelman mukaiset ja auditoinnin tarkoitusta vastaavat materiaalit on toimitettu auditoijalle etukäteen. |