Korotetun suojaustason projektitilan suunnittelu ja toteutus tutkimusalan yrityksessä

Taina Pekko

2018 Laurea

Laurea-ammattikorkeakoulu

Korotetun suojaustason projektitilan suunnittelu ja toteutus tutkimusalan yrityksessä

Taina Pekko
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2018

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

Taina Pekko

Korotetun suojaustason projektitilan suunnittelu ja toteutus tutkimusalan yrityksessä

Vuosi 2018 Sivumäärä 41

Viranomaisilla on usein tarve käyttää yrityksiä palveluiden tuottajina ja kehityshankkeissa asiantuntijoina. Tällöin yrityksille saatetaan joutua luovuttamaan tai osa yritysten tuottamista tiedoista saattaa sisältää viranomaisen salassa pidettäviä dokumentteja. Lainsäädännössä määritellään sellaiset dokumentit ja tieto salassa pidettäviksi, joiden paljastumisella voi olla haitalliset seuraukset. Siksi viranomaisten on varmistuttava yhteistyökumppaneidensa kyvystä säilyttää salassa pidettävien dokumenttien luottamuksellisuus ja suojata niitä paljastumiselta. Tällaista tietoa käsittelevän yrityksen kannalta onnistuminen vaikuttaa yrityksen luotettavuuteen, imagoon sekä mahdollisesti liikevaihtoon hankkeiden määrän kautta.

Opinnäytetyön kohdeyritys osallistuu viranomaisen hankkeisiin tiedon ja tutkimustyön tuottajana. Tämän takia yrityksen on pystyttävä osoittamaan hankkeissa käytettävien tilojen täyttävän annetut vaatimukset ja kykynsä säilyttää viranomaisen salassa pidettävän tiedon luottamuksellisuus. Opinnäytetyö on toiminnallinen ja sen tavoitteena oli koostaa yhteen kohdeyritykselle korotetun suojaustason projektitilalle asetetut vaatimukset sekä dokumentoida projektitilan toteutuksen vaiheet. Tarkoituksena oli kuvata tällaisen projektitilan suunnittelu ja toteutus niin että toimivaltaiselle viranomaiselle voidaan auditoinnissa esittää luotettavasti käytetyt toteutusratkaisut.

Koska projektitilat auditoidaan Katakri 2015 auditointikriteeristön perusteella, on se tämän työn kannalta keskeisin dokumentti. Muu tietoperusta on koottu Katakrin perustana olevista laeista ja asetuksista sekä Katakrissa viitatuista standardeista ja ohjeista, joiden perusteella vaatimuksenmukaisuus voidaan toteuttaa. Rakennusteknisistä loppukuvista todennettiin olemassa olevat rakenteet ja tilaan suunnitellut rakenteelliset muutokset rakennustapaselosteesta. Kohdeyrityksellä on turvateknisistä toteutuksista yritystason periaatekuvaukset ja suunnittelu toteutettiin näiden linjausten mukaisesti. Koska tietoperustana käytetyt lait ja standardit sisältävät myös paljon projektille epäolennaista sääntelyä ja ohjeistusta, on rajaus tehty projektitilan fyysiseen turvallisuuteen. Menetelminä käytettiin kirjallisuuskatsausta, havainnointia, dokumenttianalyysia ja teemoittelua.

Keskeisenä tuloksena toteutettiin teemoiteltu vaatimusten kooste sekä kuvaus tilan fyysisen turvallisuuden ratkaisuista. Koska tilassa todettiin toteutusvaiheen aikana kosteusvaurio, ei opinnäytetyöprosessin puitteissa pystytty tuottamaan lopullista kuvausta toteutuksesta, käyttöönotosta ja viranomaisen auditoinnista. Vaatimusten kooste yhdessä suunnittelun kuvauksen kanssa on jo sinällään hyödyllinen dokumentti kohdeyritykselle. Toteutuksen kuvaamisen ja auditoinnin tulosten esittelyn sijasta on kuvattu vasta tulossa olevia vaiheita osana toteutusvaihetta kuvaavaa lukua. Toimivaltainen viranomainen on alustavasti hyväksynyt suunnitelmat ja prosessin kuvausta sekä pohdintaa hyödyntämällä kohdeyritys voi arvioida projektin kokonaistulosta, onnistumisia sekä kehityskohteita.

Asiasanat: Katakri 2015, Rakenteellinen suojaus, ST-luokitukset, Viranomaisen salassa pidettävä tieto

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

Taina Pekko

Designing and Building a High Security Level Project Space in a Research Company

2018 2018 Pages 41

Authorities need to use private research companies as subcontractors in development projects due to their expertise and resources. Development projects might require subcontractors to store, use, and produce authorities' documents, which according to the law must be kept secret. Finnish legislation defines confidentiality levels for authorities' documents based on how harmful revealing the documents would be. Authorities' need to make sure that the subcontractors are able to handle and produce documents in a way that maintains document confidentiality. Maintaining document confidentiality successfully can affect positively a subcontractor's image, reliability, and turnover through an increased number of confidential projects.

The commissioner company of this thesis is a research company, which participates in authorities' development projects as a producer of information and innovations. The company must ensure that it is capable of maintaining the confidentiality of authorities' documents. The objective of this thesis was to map requirements set by authorities and legislation to project spaces and document phases of the construction. The purpose was to describe the project space design and implementation so that the target company can credibly present it in the audit process to the authorities.

Audits of project spaces constructed for handling and storing classified documents follow the Katakri 2015 criteria and consequently it is a key document in this thesis. In addition, the theoretical framework of this thesis covers laws and regulations as well as standards and instructions referred to in Katakri 2015 as sources or implementation options. The existing structures of the project space were verified from constructional end-pictures and the planned modifications from the construction plan. The commissioner company also has company level processes and principle descriptions, which the planning and implementations are based on. The referred documents in the thesis include a range of regulations and instructions. As a result, the focus of the thesis has been restricted to the physical security aspects of the subject. The used research methods were literature review, observation, document analysis and thematising.

The outcome of this thesis is documentation describing requirements and the chosen solutions for physical security measures to fulfil the given requirements. A final report of the implementations and auditing of the space in this thesis scope were not feasible because some water damage was detected in the project space in the construction phase. The produced document comprising the requirements and describing the planned security solutions is still useful to the commissioner company. Instead of a construction phase description, this thesis includes a description of how the project should and will be finished. A competent authority has provisionally accepted the plans of the project space structures and security solution descriptions. The commissioner company can use this thesis in its evaluation of the project's outcome, success and in mapping development proposals.

Keywords: Katakri 2015, Structural protection, Confidentiality classification, Confidentiality obligation of authority documentation

Sisällys

1 Johdanto

Myös yritykset käsittelevät viranomaisen salassa pidettävää tietoa ja käsittelyä tapahtuu muuallakin kuin viranomaisen itsensä hallinnoimissa tiloissa. Viranomaisen on kuitenkin varmistuttava salassa pidettävän tiedon suojaamisen menettelyistä ja tiedon pysymisestä vain niiden henkilöiden saatavilla, joilla on tarve käsitellä kyseistä tietoa. Tämä opinnäytetyö käsittelee teknologia-alan yrityksen suojaustaso (ST) luokitellun materiaalin käsittelyyn tarkoitetun projektitilan rakennusprosessia. Kyseisessä yrityksessä tehdään hankkeita, joissa käsitellään ja tuotetaan viranomaisen salassa pidettävää tietoa. Tällaisiin hankkeisiin osallistuminen edellyttää asianmukaisten tilojen osoittamista hankkeen käyttöön. Projektitilan tarve yrityksessä on tunnistettu jo isomman toimitilamuutosten kokonaisuuden yhteydessä 2017, kun eri toimintoja suunniteltiin siirrettäväksi uusiin tiloihin. Tämän opinnäytetyön tekijä on osallistunut tilan toteutukseen suunnitteluvaiheesta lähtien ja opinnäytetyön kirjoittamisen alkaessa ollaan vaiheessa, jossa tilan rakenteelliset muutokset ovat alkamassa.

Koska toimeksi antavan viranomaisen on lakiperusteisesti varmistuttava yhteistyökumppaneiden kyvystä suojata viranomaisen salassa pidettävää tietoa, tarvitaan menettelyt tämän todentamiseksi. Keskeinen lainsäädännöllinen vaatimuslähde suojattavan tiedon käsittelylle on valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (A681/2010). Kansainväliset velvoitteet salassa pidettävälle tiedolle asettaa EU:n neuvoston turvallisuussäännöt. Näihin vaatimuksiin pohjautuen on laadittu viranomaisen auditointityökalu, Katakri 2015 jota käyttämällä kohdeorganisaatiot arvioidaan.

Käytännön tasolla laissa määritetty velvollisuus viranomaisen salassa pidettävän tiedon suojaamisesta edellyttää aina kyseiseen tarkoitukseen suunniteltuja ja rakennettuja tiloja, joiden vaatimuksenmukaisuuden toimivaltainen viranomainen käy tarkastamassa ennen tilojen käyttöön ottoa ja tiedon käsittelyn aloittamista tiloissa. Koska tiloille on normaaleista toimistotiloista poikkeavia vaatimuksia niin rakenteiden ja materiaalien murronkestossa kuin turvallisuusteknisessä valvonnassakin, on rakennusprojekti aina erillinen investointi yritykselle. Mikäli yrityksellä on käytössään hyvä prosessikuvaus vaatimuksista, suunnittelusta sekä toteutuksesta, voidaan tilan vaatimat investoinnit, tarvittavat taustaselvitykset, suunnittelun tarve ja rakentamiseen käytettävä aika arvioida etukäteen tarkemmin. Jos auditoitava tila ei täytä vaatimuksia, voi toimivaltainen viranomainen kieltää salassa pidettävän tiedon säilyttämisen ja käsittelyn esitetyissä tiloissa. Tällöin yritys ei voi myöskään osallistua viranomaisen hankkeeseen niiltä osin, kun hankkeen toteutus vaatii salassa pidettävän tiedon käsittelyä ja säilytystä yrityksen tiloissa.

2 Opinnäytetyön taustaa, tarkoitus ja keskeiset käsitteet

Tämän opinnäytetyön tavoitteena on koostaa viranomaisen salassa pidettävän ST-luokitellun tiedon säilyttämiseen ja käsittelyyn tarkoitettujen tilojen vaatimukset sekä dokumentoida suunnittelun ja toteutuksen vaiheet ja arvioida vaatimuksenmukaisuuden toteutumista. Työn tarkoituksena on tuottaa kuvaus, jossa käsitellään osa-alueiksi teemoitellen tilan turvallisuusratkaisuihin kohdistuvat vaatimukset sekä lähdeaineistojen esittämät toteutusratkaisut, projektin eri vaiheet sekä tavoitteiden saavuttaminen. Työ on tarkoitus liittää kohdeyrityksen toimitilaturvallisuuden prosessikuvaukseen ST-luokiteltujen tilojen perustamista kuvaavana liitteenä. Ajallisesti työn prosessi ei täydellisen seuraa projektin toteutumista, sillä alustava suunnittelu on aloitettu jo ennen opiskelijan mukaan tuloa ja toisaalta projekti on tarjouspyyntövaiheessa opinnäytetyön kirjoitusprosessin alkaessa.

Työ on toiminnallinen opinnäytetyö, jossa tarkastellaan projektina toteutettavaa tilahanketta sekä kuvataan sen eri vaiheet. Teoreettisena viitekehyksenä käytetään projektitilan päätarkoitukselle, suojata viranomaisen salassa pidettävää tietoa, vähimmäisvaatimukset antavaa lainsäädäntöä, standardeja joihin Katakri 2015 viittaa, rakennusmateriaaleja koskevaa kirjallisuutta sekä Finanssiala ry:n antamia murtosuojaluokitusdokumentteja.

Opinnäytetyön tutkimuskysymykset ovat seuraavat:

Mistä velvoitteet viranomaisen salassa pidettävien asiakirjojen käsittelyyn tulevat?

Mitä vaatimuksia on ST-luokitellun tiedon käsittelyyn tarkoitetun projektitilan fyysiselle turvallisuudelle?

Millaisilla ratkaisuilla viranomaisen salassa pidettävän tiedon säilyttämiseen tarkoitetun tilan vaatimuksenmukaisuus voidaan toteuttaa tutkimusalan yrityksessä?

Opinnäytetyö rajataan koskemaan yksittäisen projektitilan rakenteellisia ja turvateknisiä suojausratkaisuja. Kohdeyrityksen turvallisuusjohtamisen sekä fyysisen turvallisuuden yleisiä prosesseja käsitellään suhteessa niiden vaikutukseen projektitilan turvallisuusratkaisuihin ja vaatimuksenmukaisuuden toteutumiseen. Teknistä tietoturvallisuutta käsitellään vain siltä osin, kun se on tarpeellista projektitilaa suunniteltaessa ja rakennettaessa. Hankekohtaiset ratkaisut tietoteknisen turvallisuuden osalta on rajattu työn ulkopuolelle. Opinnäytetyön ulkopuolelle on rajattu myös hankintamenettelyt ja sitä koskeva sääntely. VAHTI-ohjeista on rajattu käsiteltäväksi vain VAHTI 2/2013, johon viitataan Katakri 2015 F-osiossa. T- ja I-osioissa viitataan myös muihin VAHTI-ohjeisiin, mutta näitä ei tässä työssä käsitellä.

2.1 Opinnäytetyön kohdeorganisaatio

Kohdeyritys on alallaan yksi Euroopan johtavista tietointensiivisen teknologia tutkimuslaitoksista, jolla on kansallista ja kansainvälistä toimintaa. Toiminnan keskiössä ovat kilpailukykyä lisäävät innovaatio- ja tutkimuspalvelut yksityiselle sekä julkiselle sektorille. Yrityksen asiantuntijat muun muassa kehittävät asiakkaille uusia älykkäitä teknologioita, joilla voidaan tähdätä muun muassa parempaan liiketulokseen, pienempiin tuotantokustannuksiin, raaka-ainehävikin pienentämiseen tai energian kulutuksen vähentämiseen. (Kohdeyritys 2018.)

Yksi kohdeyrityksen kilpailueduista on tutkimustyön vaatimat resurssit. Tällaisiksi resursseiksi voidaan lukea erikoistilat, uniikit tutkimuslaitteet ja eri toimialojen osaajat. Myös kansallinen ja kansainvälinen yhteistyö eri yritysten ja organisaatioiden kanssa on tärkeä voimavara. Taloudellisesta näkökulmasta mahdollisimman suuri käyttöaste on tärkeää, koska erikoistilat ja tutkimuslaitteet ovat usein kalliita ja vaativat isojakin investointeja. Toisaalta arvokkaita laitteita ja tiloja tulee suojata, mikä haastaa turvallisuusnäkökulmista. Lisäksi luottamuksellisuus on yksi kohdeyrityksen kulmakivistä. Haasteena onkin eri toimintojen ja kehittävän yhteistyön sovittaminen samoihin tiloihin niin, että kaikkien luottamuksellisuus pystytään takaamaan. Tämän vuoksi turvallisuusasioihin panostetaan ja niiden suunnittelussa pyritään pysymään kansallisesti ja kansainvälisesti kärkitasolla. (Kohdeyritys 2018.)

2.2 Keskeiset käsitteet

Katakri 2015 eli kansallinen turvallisuusauditointikriteeristö on viranomaisen auditointityökalu, jota voidaan käyttää arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista, kun yrityksessä käsitellään viranomaisen salassa pidettävää tietoa. Katakri on alun perin valmistunut osana hallituksen sisäisen turvallisuuden ohjelmaa vuonna 2009. Viimeisimmän version on sisäministeriön asettama neuvoa antava työryhmä päivittänyt 2015 ja sen on hyväksynyt NSA:n yhteistyöryhmä. Katakrin hallinnointiin ja tarvittaessa päivittämiseen osallistuvat toimivaltaiset viranomaiset sekä elinkeinoelämän edustajat. (Puolustusministeriö 2015.)

Rakenteellinen suojaus on tarkoituksenmukaisista rakenteista koostuva kokonaisuus, jolla suojataan rakenteiden sisäpuolelle jääviä asioita muun muassa rikoksilta, vahingoilta, luvattomalta pääsyltä sekä tahattomalta paljastumiselta tai leviämiseltä. Rakenteilla voidaan suojata myös niiden ulkopuolisia alueita esimerkiksi sisäpuolella säilytettäviltä myrkyllisiltä aineilta. Rakenteelliseen suojaukseen kuuluvat muun muassa kehäsuojaus, aluesuojaus, kuorisuojaus sekä kohdesuojaus. (Leppänen 2006, 333-345.)

Suojaustaso (ST) -luokitukset ovat salassa pidettävien asiakirjojen luottamuksellisuuden merkitsemiseen tarkoitettuja luokitteluja, jotka on määritetty valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa. Luokitukset ovat STI – STIV, STI:n ollessa erittäin salainen

ja STIV:n käytöltään rajoitettu. Luokitukset perustuvat siihen kuinka haitallista luokitellun asiakirjan oikeudeton käyttö voi olla. Luokitukset myös osoittavat millaisia tietoturvallisuusvaatimuksia tietojen käsittelyssä tulee noudattaa. (Aho 2010.)

Viranomaisen salassa pidettävä asiakirja sisältää lakiperusteisesti salassa pidettävää tietoa, joka paljastuessaan voi olla vahingollista yleiselle tai yksityiselle edulle. Salassapitovelvoitteet määrätään laissa viranomaisen toiminnan julkisuudesta (L621/1999) ja salassa pidettävän tiedon käsittelystä valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (A681/2010.)

3 Lainsäädäntö ja keskeiset standardit

Lainsäädännöllä tarkoitetaan laajana käsitteenä koko voimassa olevaa oikeutta ja oikeuskäytäntöjä, konkreettisemmin ajateltuna sillä tarkoitetaan lakeja ja säädöksiä joihin oikeuskäytännöt pohjautuvat. Kun yhdelle asiakokonaisuudelle tulee vaatimuksia useammasta säädöksestä, tulee säädöshierarkia ottaa huomioon. Alemman tason säädös ei saisi olla ylemmän tason säädöksen kanssa ristiriidassa, mutta tältä ei aina voida välttyä. Suomalaisessa pätemisjärjestyksessä perustuslaki on määräävin, sen jälkeen esitetyssä järjestyksessä tulevat tavalliset lait, tasavallan presidentin ja valtioneuvoston asetukset, ministeriöiden antamat asetukset ja muut alemman tasoiset säädökset. Koska Suomi kuuluu Euroopan unioniin, tulee sen noudattaa myös sen asettamaa yhteisölainsäädäntöä. Mikäli kansallinen- ja yhteisölainsäädäntö ovat ristiriidassa keskenään, tulisi oikeuskäytännöissä noudattaa yhteisölainsäädäntöä. (Eduskunta 2018.) Standardit taas ovat eri yhteisöjen ja toimielinten sopimia normeja, kuinka esimerkiksi lainsäädännön velvoitteet voidaan täyttää. Standardien tarkoitus on myös yhtenäistää käytäntöjä sekä taata laatu eri palveluille ja tuotteille. (Suomen Standardisointiliitto 2018.)

3.1 ST-luokituksia koskeva lainsäädäntö

Asiakirjan salassapidosta säädetään laissa viranomaisten toiminnan julkisuudesta (L621/1999) sekä valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (A681/2010). Karkeasti jaoteltuna laki viranomaisten toiminnan julkisuudesta edellyttää pykälässä 24 eritellyt asiakirjat salattaviksi ja määrää salassapito- ja luokitusmerkinnöistä, kun taas valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa määrittää salassa pidettävien asiakirjojen tietoturvavaatimukset sekä luokitusten perusteet. Valtioneuvoston asetus edellyttää muun muassa, että luvaton pääsy asiakirjoihin estetään, asiakirjoja käsittelevät vain käsittelyyn oikeutetut henkilöt ja heidät tunnistetaan. Tilat joissa asiakirjoja säilytetään ja käsitellään, tulee olla asianmukaisesti suojattu. Asetuksessa määritetään neljä suojaustasoa ja ne perustuvat asiakirjan sisältämän tiedon paljastumisen haitallisuuteen ja vahingollisuuteen. Mitä korkeamman suojaustason luokitus asiakirjalla on, sitä vaativammat ovat suojaustoimet.

Laki viranomaisen toiminnan julkisuudesta (jäljempänä julkisuuslaki) määrää julkisuusperiaatteesta, jonka mukaan viranomaisten asiakirjat ovat julkisia, ellei laissa toisin säädetä. Julkisuuslaki säätää jokaisen oikeudesta saada tieto viranomaisen julkisista asiakirjoista, viranomaisen vaitiolovelvollisuudesta, määrittää asiakirjojen salassapidosta ja tiedon saannin rajoituksista sekä viranomaisen velvoitteista näissä asioissa. Lain tarkoitus on lisätä viranomaistoiminnan läpinäkyvyyttä niin julkisen vallan kuin varojen käytössä. Salassa pidettäviä asiakirjoja ovat muun muassa sellaiset, joiden paljastuminen saattaa vaikuttaa taloudellisesti, poliittisesti tai toimintoja vaarantavasti valtioon tai viranomaiseen. Tällaisia asioita voivat olla esimerkiksi taktiset ja tekniset tiedot, rakennusten turvajärjestelyjä koskevat ja niihin vaikuttavat asiakirjat sekä poikkeusoloihin varautumisen suunnitelmat. Myös puolustusvoimien strategisia tietoja ja maanpuolustusta palvelevia keksintöjä koskevat asiakirjat ovat salassa pidettäviä. Asianosainen kenen oikeutta, etua tai velvollisuutta asiakirja koskee, on kuitenkin aina oikeutettu tiedon saantiin. Jos asiakirja on lain nojalla salassa pidettävä, tulee tästä olla merkintä. Luokitusmerkintä voidaan tehdä asiakirjaan sen osoittamiseksi, millaisia tietoturvallisuusvaatimuksia asiakirjan käsittelyssä on noudatettava. Asiakirjan salassapito lakkaa, kun laissa säädetty aika on kulunut tai salassapidon määrännyt viranomainen peruuttaa salassapidon määräyksen. Rakennusten turvallisuutta ja maanpuolustusta koskevat salaiset asiakirjat tulevat julkisiksi, kun rakennus tai laite ei ole enää käytössä, mikäli myös salassapidon perusteena olleita seurauksia ei enää voi aiheutua. Valtioneuvosto voi perustelluista syistä pidentää salassapidon aikaa 30 vuotta. (L621/1999.)

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (A681/2010) säätää viranomaisen asiakirjojen käsittelyä koskevista yleisistä tietoturvavelvoitteista, asiakirjojen luokittelusta sekä luokittelujen mukaisesta asiakirjojen tietoturvallisesta käsittelystä. Asetus määrittelee salassa pidettäväksi asiakirjan joka lainsäädännössä sellaiseksi määrätään. Valtionhallinnon viranomaisen on mitoitettava tietoturvallisuustoimenpiteet suhteessa asiakirjan sisältämiin tietoihin ja merkitykseen. Tietoturvallisuuden toteutumiseksi vaaditut toimenpiteet tulee perustua tiedon merkityksellisyyteen sekä riskiarvioon, missä tietoon kohdistuvat uhat on huomioitu suhteessa vaadittuihin suojaustoimiin. Muina yleisinä tietoturvavaatimuksina viranomaisen tulee varmistua muun muassa asiakirjoja käsittelevien henkilöiden tehtävien ja vastuiden määrittämisestä, tietoa käsittelevien henkilöiden työtehtäväperusteisesta tarpeesta käsitellä salassa pidettävää tietoa, käsittely- ja säilytystilojen riittävästä suojaamisesta sekä tietojen käsittelyyn liittyvien ohjeiden ja prosessien olemassaolosta.

Salassa pidettävät asiakirjat voidaan luokitella salassapitosäännöksessä tarkoitettujen etujen suojaamiseksi seuraavasti: Suojaustaso I – ERITTÄIN SALAINEN, asiakirjan paljastuminen tai oikeudeton käyttö voi aiheuttaa suurta vahinkoa yleiselle edulle. Suojaustaso II – SALAINEN, asiakirjan paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa yleiselle edulle. Suojaustaso III LUOTTAMUKSELLINEN, asiakirjan paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa yleiselle tai yksityiselle edulle. Suojaustaso IV – KÄYTTÖ RAJOITETTU, asiakirja

paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa yleiselle tai yksityiselle edulle. Asiakirjojen säilyttämiselle on määrätty viranomaisen huolenpitovelvoite, jossa edellytetään varmistumaan, että luokiteltuja asiakirjoja suojataan asianmukaisesti lukituksella, kulunvalvonnalla ja muilla toimenpiteillä. Tämän lisäksi suojaustason I-II asiakirjoja edellytetään säilytettäväksi kassakaapissa, holvissa tai muussa vastaavassa luvattoman pääsyn estävässä säilytysyksikössä. Henkilöt, joilla on pääsy käsittelytiloihin tai itse asiakirjoihin, tulee tunnistaa. Asiakirjojen käsittely viranomaisen tilojen ulkopuolella saa tapahtua vain viranomaisen luvalla, toimeksiannosta tai erikseen ohjeistettuna. Lisäksi asetus säätää asiakirjojen käsittelystä sekä tietojenkäsittely-ympäristöistä suojaustasojen mukaisesti. (A681/2010.)

3.2 Katakri 2015

Katakri 2015 on kansallinen viranomaisen turvallisuusauditointikriteeristö, jonka perusteella arvioidaan kykyä suojata viranomaisen salassa pidettävää tietoa. Kriteeristön avulla voidaan arvioida sisäisesti viranomaisen eri yksiköiden tietojärjestelmiä, mutta myös yritysten, yhteisöjen ja viranomaisten turvallisuustyötä ja sen kehittämistä. Useimmiten Katakria käytetään arvioimaan yrityksen turvallisuusjärjestelyjä yritysturvallisuusselvitystä tehtäessä (L726/2014.) Katakrin mukaan yrityksen turvallisuusjohtamisen, fyysisen turvallisuuden sekä teknisen tietoturvallisuuden tulee olla sillä tasolla, että yrityksen voidaan katsoa olevan kyvykäs suojaamaan viranomaisen salassa pidettävää tietoa oikeudettomalta paljastumiselta. (Puolustusministeriö 2015.)

Katakri 2015 ei aseta tietoturvallisuudelle ehdottomia vaatimuksia vaan sillä painotetaan uhkiin nähden hyväksyttävää turvallisuustasoa. Tämä tarkoittaa, että organisaatiolta odotetaan kykyä järjestelmälliseen riskienarviointiin, jonka pohjalta suojaustoimet toteutetaan. Toteutuksessa otetaan huomioon käyttäjien tarpeet ja tiedon käytön edellytykset, tiedon suojaamisen toteutusten kustannukset sekä turvallisuuteen kohdistuvat jäännösriskit niin että nämä ovat tasapainossa ja suojattaviin asioihin nähden järkevät. Katakri 2015 on toteutettu kolmena eri osa-alueena, joita kutakin voidaan arvioida erikseen tai kaikkia yhtäaikaisesti. Tehtäessä yritysturvallisuusselvitystä on aina arvioitava vähintään kohdeorganisaation turvallisuusjohtaminen. Katakria ei kuitenkaan ole tarkoitettu käytettäväksi julkisen hankinnan turvallisuusvaatimuksena, vaan vaatimusten tulee perustua salattavan tiedon käsittelyä ja säilytystä koskeviin lakivelvoitteisiin sekä kohdeorganisaation ja viranomaisen välisiin sopimuksiin. (Puolustusministeriö 2015.)

Katakrin osa-alue T käsittelee turvallisuusjohtamista. Yrityksen turvallisuusjohtamisen tasoa arvioitaessa on vähimmillään kohdennettava arviointi siihen organisaation osaa, jolla on suora tai epäsuora vaikutus salassa pidettävän tiedon käsittelyyn. Tämä osa-alue kattaa hallinnollisen turvallisuuden ja henkilöstöturvallisuuden, joten kriteereiden toteuttaminen koko organisaation toiminnassa vahvistaa yleistä turvallisuustyötä ja sen kehittämistä. Muista Katakrin osa-alueista poiketen turvallisuusjohtamisen vaatimukset eivät suoraan erittele eri suojaustasojen

vaikutusta turvallisuustoimien vaatimuksiin. Suojaustaso on kuitenkin otettava huomioon muun muassa ohjeissa, sillä esimerkiksi ST-II tason tiedon käsittely tulee ohjeistaa eri tavalla kuin mitä yleiset tietoturvaohjeet esittävät. Kohta T 04 käsittelee turvallisuusriskien hallintaa. Jo Katakrin johdanto nostaa riskien arvioinnin ja hallintakeinot keskeisiksi turvallisuusratkaisujen suunnittelussa. Toteutusesimerkkinä määritetään, että riskienhallinnan periaatteet tulee olla kuvattu, suojattavat kohteet tunnistettu, suojattaville kohteille on nimetty vastuuhenkilö, riskien arviointi ja tunnistus on toteutettu, suojausmenetelmät toteutetaan suhteessa tunnistettuihin riskeihin, riskienhallintaprosessissa käytetään järjestelmällistä menetelmää ja riskienhallintaprosessin perusteella tehdyt johtopäätökset on huomioitu turvallisuusdokumentaatiossa. (Puolustusministeriö 2015, 5.)

Yritystä, joka sopimusperusteisesti tekee viranomaisen kanssa yhteistyötä hankkeessa jossa käsitellään salassa pidettävää tietoa, arvioidaan pääsääntöisesti vain niiden tilojen osalta joissa tiedon luonti, vastaanottaminen, käsittely sekä tuhoaminen tapahtuvat. Katakrin osassa F kuvataan fyysiselle turvallisuudelle annettuja vaatimuksia. Tilojen arviointi suoritetaan siellä käsiteltävän korkeimman suojaustason materiaalin vaatimusten mukaisesti. Tilojen suunnittelussa ja rakentamisessa Katakri 2015 esittää huomiotavaksi seuraavat asiat: Missä tiloissa suojattavia tietoja käsitellään ja minkä suojaustason tiedoista on kyse? Missä ympäristössä ja rakennuksen osassa suojattavia tietoja käsitellään? Millaiset ovat rakennuksen tai tilan turvajärjestelyt ja rakenteet? Miten toteutetaan salassa pidettävien tietojen suojaaminen tilassa (luominen, vastaanottaminen, käyttäminen, säilyttäminen ja hävittäminen)? Millä tietojenkäsittelyvälineillä ja järjestelmillä tietoja tilassa käsitellään? Huomioon on otettava myös kuinka paljon tietoa tiloissa säilytetään; suojattavien tietojen kasautuminen saattaa edellyttää tiukempien turvallisuusvaatimusten soveltamista. Esimerkiksi suuri määrä suojaustason IV tietoa saattaa muodostaa suojaustason III kokonaisuuden. (Puolustusministeriö 2015, 16.)

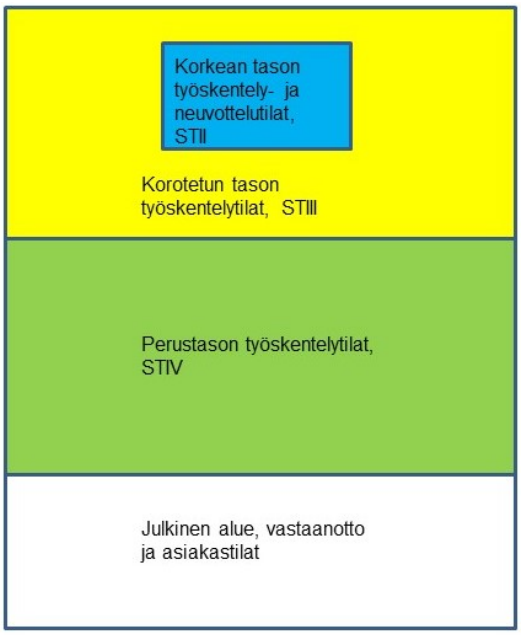
Katakrin käsittelemät fyysisen turvallisuuden osa-alueet ovat tiloja ja alueita koskevat vaatimukset, turvallisuusjärjestelmät ja laitteet, luvattoman pääsyn estäminen, tiedon suojaaminen salakatselulta ja salakuuntelulta sekä toiminnan jatkuvuuden varmistaminen. Koska suojaustasomerkinnät ovat riippuvaisia tiedon paljastumisen ja oikeudettoman käytön haitallisuudesta, myös suojaamisratkaisujen vaatimukset kiristyvät mitä korkeamman luokituksen tietojen käsittelyyn ja säilytykseen tarkoitetusta tilasta on kyse. Fyysisissä ratkaisuissa tämä on toteutettavissa korottamalla rakenteiden ja laitteiden murronkestoa sekä lisäämällä kehäsuojauksen mukaisia kerroksia suojattavan asian ympärille. Lisäksi tiedon käyttäjien ohjeet ja toimintamallit korostuvat, jotteivat he tahattomasti toiminnallaan heikennä suunniteltujen suojausten toimivuutta. Valvonnalla ja todentamisella pienennetään riskiä tahallisiin väärinkäytöksiin ja toisaalta edesautetaan poikkeamien selvittämistä. (Puolustusministeriö 2015, 17-28.)

I-alueessa kuvataan vaatimukset, joilla pyritään varmistamaan viranomaisen salassa pidettävän sähköisen tiedon eheys, käytettävyys ja saatavuus. Teknisen tietoturvallisuuden ratkaisuilla suojataan tietoja paljastumasta sellaisille henkilöille, joilla ei ole oikeutta niitä käsitellä. Vaatimukset on jaettu tietoliikennettä-, tietojärjestelmiä-, tietoaineistoa- ja käyttöturvallisuutta käsitteleviin osioihin. Näissä osa-alueissa käsitellään muun muassa sähköisiä hallintayhteyksiä, langattomia verkkoja, etäkäyttöä ja varmuuskopiointia. Myös tietoteknisten ympäristöjen osalta edellytetään tehtäväksi riskiarviointi, jonka pohjalta suojaukset tulee suunnitella ja vaatimuksia tulkita. Yksi osa tarkoituksenmukaisten suojausten suunnittelua ja toteutusta on tietoaineiston oikea luokittelu, jottei dokumentteja edellytetä suojattavaksi aineiston sisältöön nähden liian suurin vaatimuksin. Tietojenkäsittely-ympäristöä tulee käsitellä kokonaisuutena ja arvioida vaatimuksenmukaisuus vain soveltuvilta osin. Tällä tarkoitetaan esimerkiksi sitä, että mikäli tilassa ei käsitellä paperimateriaalia, arvioidaan vain sähköisten järjestelmien ja siihen kuuluvien laitteiden turvallisuus ja suojaus. Yleensä vaatimuksenmukaisuuden pääasiallisena toteuttajana ja arvioijana toimii viestintävirasto, kun puhutaan viranomaisen salassa pidettävästä tiedosta sähköisessä muodossa. (Puolustusministeriö 2015, 29.)

3.3 VAHTI-ohjeet

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, VAHTI, on valtionvarainministeriön asettama elin, jonka tehtävänä on olla julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu ja koordinointielin. Tämä elin myös valmistelee ja ohjaa VAHTI-ohjeiden toteuttamisen. Näiden ohjeiden tarkoituksena on tukea tietoturvallisuuden toteutumista valtionhallinnossa sekä auttaa organisaatioita toteuttamaan salassa pidettävän tiedon käsittelyä ja säilytystä säädösten ja linjausten mukaista. (Valtiovarainministeriö 2018.) Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa sekä laki kansainvälisistä tietoturvallisuusvelvoitteista antavat lakivaatimukset tietoturvallisuuden toteuttamisesta sekä sellaisten tilojen valvonnasta ja suojaamisesta, missä käsitellään salassa pidettäviä asiakirjoja. VAHTI-ohjeet ovat VAHTI-asiantuntijajaoston ja sen alaisuudessa toimivien asiantuntiaryhmien tuottamia käytännön ohjeita digitaalisen turvallisuuden kehittämiseen. Katakri viittaakin VAHTI-ohjeisiin useassa vaatimuskohdassa, lisätietoviitteenä ja toteutusesimerkkinä. Mikäli VAHTI-ohje ja Katakri ovat ristiriidassa keskenään, on toteutusratkaisuja rakentavan organisaation käännyttävä toimivaltaisen viranomaisen puoleen ja pyydettävä heiltä kannanottoa kyseiseen toteutukseen hyväksytystä ratkaisusta. VAHTI-ohjeet on kattava ohjeistokokonaisuus tietoturvallisuuden hallintaan niin turvallisuusjohtamisen, fyysisen turvallisuuden kuin teknisen tietoturvallisuudenkin osa-alueilla. VAHTI 2/2013 keskittyy fyysiseen turvallisuuteen. Ohje käsittelee lainsäädännön sekä muun viitekehyksen, turvallisuusvyöhykkeet, rakenteelliset turvallisuusvaatimukset sekä turvallisuusvalvonnan. Liitteissä on kuvattu eri toteutusesimerkkejä, esitetään suosituksia sekä viitataan tarkemmin kyseisessä ohjeessa mainittuihin dokumentteihin. Kyseinen VAHTI-ohje käsittelee kaikkia osa-alueita dokumentin nimen mukaisesti toimitilojen näkökulmasta. (Valtiovarainministeriö 2013.)

Turvallisuusvyöhykkeet – luvussa käsitellään toisiaan seuraavia rakenteellisia suojauksia. Eri vyöhykkeet perustuvat suojaustasoihin, jotka on määritelty lainsäädännössä. Mitä korkeampi suojaustaso on, sitä vahingollisempaa kyseisen tiedon paljastuminen on ja sitä paremmat suojaukset kyseinen tieto vaatii. Eri turvallisuusvyöhykkeiden yleisten vaatimusten lisäksi luvussa käsitellään normaaleista käsittelytiloista poikkeavia tietojenkäsittely-ympäristöjä, kuten organisaation normaalien toimitilojen ulkopuolella tehtävää etätyötä sekä sellaista työtä, joka vaatii liikkumista. Molemmissa tapauksissa tietojen suojaaminen voidaan mitoittaa satunnaisen käsittelyn periaatteiden mukaisesti, kunhan riskikartoitukset on tehty ja jäännösriski hyväksytty tapauskohtaisesti. Kuviossa 1 on kuvattu VAHTI 2/2013 mukainen turvallisuusvyöhykkeiden esimerkki. (Valtiovarainministeriö 2013.)



Kuvio 1: Turvallisuusvyöhykkeet (Valtiovarainministeriö 2013, 19-24)

Turvallisuusvyöhykejaossa korkeamman suojaustason tilat seuraavat matalamman suojaustason tiloja. Korkean suojaustason, STII, tilat on esitetty sijoitettavaksi niin että niitä ympäröi korotetun tason työskentelytilat. Tällä ratkaisulla korkean tason tilan omat suojausratkaisut ympäröidään myös korotetun tason suojauksilla, mikä lisää murronkestoa ja hidastaa merkittävästi tiloihin tunkeutumista. Lisäksi salakatselu ja –kuuntelu vaikeutuu merkittävästi, jos tilat eivät ole rakennuksen kuoressa kiinni eikä ikkunoita ole. Keskeisiä elementtejä vyöhykkeiden välillä ovat kulunvalvonta ja sen osana lukitus sekä kiinteät rakenteet. Rakentamisen ja rakennusmateriaalien lähteeksi VAHTI 2/2013 esittää ympäristöministeriön ylläpitämän Suomen rakennusmääräyskokoelman. (Valtiovarainministeriö 2013, 19-24.)

Rakenteellisten vaatimusten osiossa käsitellään alue, ulkopinnat, katto-, seinä-, lattia-, ovi- ja ikkunarakenteet. Turvallisuusvalvontana käsitellään vyöhykkeitä ja rakenteellisia ratkaisuja tukevat turvallisuustekniset ratkaisut sekä valvontatoimet. Keskeisiä käsitteitä ovat kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmät sekä vartiointi vasteaikoineen. Rakenteiden toteutuksessa korostuu murron kesto sekä salakatselun ja –kuuntelun estäminen. Näitä ominaisuuksia saadaan parannettua vahvistamalla rakenteita esimerkiksi paksuuden lisäämisellä tai pellityksellä. Äänen kulkemisen estämisessä voidaan toteutuksena käyttää ilmastointikanavissa ääniloukkuja ja muiden läpivientien villoittamista tai massaamista. Useille materiaaleille on olemassa valmistajan ilmoittamat äänieristävyydet, joilla voidaan laskea ääniaallon vaimenemista eri materiaaleja käytettäessä. Ikkunoita ja lasipintoja lukuun ottamatta kiinteät esteet ovat itsessään näköesteitä, jotka estävät salakatselun. Ikkunat voidaan suojata esimerkiksi sälekaihtimin ja lisäsuojaa antavat näyttöjen tietosuojakalvot. Lukituksen osalta VAHTI 2/2013 viittaa Finanssiala ry:n ohjeiden mukaisiin lukituksiin. Eri lukkovalmistajien lukkomallit on näissä materiaaleissa listattu ja niille on annettu murtosuojaluokitus. Lukkomalliksi on syytä valita sellainen tuote, jonka patenttisuoja on voimassa ja luvaton avainten kopioiminen tällä tavoin estetty. Jos avaimia säilytetään putkilukoissa esimerkiksi pelastusviranomaisia varten, on näiden putkien oltava valvottuja. Kiinteistön ulkokuoressa olevissa putkilukoissa ei saa säilyttää suojattuihin tiloihin käyviä avaimia, vaan tällaiset avaimet tulee säilyttää kuoren sisäpuolelle sijoitetussa putkessa ja ulkopuolella olevassa vain reittiavainta sisäputkelle. (Valtiovarainministeriö 2013.)

3.4 Pelastuslaki

Pelastuslain tarkoitus on parantaa ihmisten turvallisuutta ja vähentää onnettomuuksia, mutta myös onnettomuustilanteissa tai sellaisen uhatessa taata ihmisten pelastaminen, tärkeiden toimintojen turvaaminen sekä seurausten tehokas rajoittaminen. Laki käsittelee palo- ja pelastusturvallisuuden yleisiä velvoitteita, kiinteistön tai rakennuksen rakentajan, omistajan ja haltijan velvoitteita sekä pelastusviranomaisten velvollisuksia, oikeuksia ja tehtäviä. Kiinteistöjen rakenteille asetetaan vaatimuksia samoin kuin paloilmoitinlaitteistoille ja poistumisturvallisuudelle. Myös tässä laissa painotetaan riskiarviointia ja omatoimista varautumista. (L379/2011.)

Poistumisteille sekä niiden esteettömyydelle asetetaan suuria vaatimuksia niiden vaikuttaessa merkittävästi rakennusten pelastusturvallisuuteen. Rakennuksen omistaja, haltija sekä toiminnan harjoittaja ovat kaikki osaltaan vastuussa siitä, että uloskäytävät ovat esteettömiä ja kulkukelpoisia niin että rakennuksessa olevat henkilöt voivat tulipalo- tai onnettomuustilanteessa poistua turvallisesti ja tehokkaasti. Uloskäytävillä ei saa säilyttää tavaroita ja ne on valaistava asianmukaisesti. Käytännössä nämä velvoitteet tarkoittavat sitä, että lukitukset eivät saa estää poistumista edes sellaisessa tilanteessa, että poistuvalla henkilöllä ei ole tarvittavia avaimia reitille. (L379/2011.)

Laki sisältää myös väestönsuojien rakentamisen velvoitteen. Väestönsuojille on asetettu erilaisia koko, rakenne ja käyttötarkoitusmääräyksiä. Lain rikkomisesta on määrätty rangaistussäädökset ja lain toteutumista valvovat muun muassa paloviranomaiset. Viranomaiset voivat myös antaa korjausmääräyksen, mikäli toteutukset eivät täytä vaatimuksia. Väestönsuoja on rakennettava kiinteistöön, jossa on enemmän kuin 1200 kerrosneliötä ja rakennuksessa asutaan tai työskennellään pysyvästi. Vaatimus voidaan täyttää myös rakennuskokonaisuuden yhteisellä väestönsuojalla, jonka suojapaikat täyttävät vaatimukset kokonaisuuden kokoon ja henkilömäärään nähden. Rakenteellisesti väestönsuojan tulee suojata siellä oleskelevia ihmisiä asevaikutuksilta, rakennuksen sortumiselta, ionisoivilta ja myrkyllisiltä aineilta. Teknisistä yksityiskohdista on säädetty tarkemmin sisäasianministeriön asetuksella. Normaaliolojen aikana väestösuojaa voidaan käyttää muuhun tarkoitukseen, sillä edellytyksellä, että sen välineet ja laitteet ylläpidetään asianmukaisesti muusta käytöstä huolimatta ja se on otettavissa väestösuojakäyttöön 72 tunnissa. (L379/2011.)

3.5 Rakentamista koskeva sääntely

Maankäyttö- ja rakennuslaki (L132/1999) antaa yleiset edellytykset ja suuntaviivat alueiden ja rakennusten suunnittelulle, rakentamiselle ja käytölle niin että edistetään ekologista, taloudellista, sosiaalista ja kulttuurista kestävää kehitystä. Ympäristöministeriö ylläpitää Suomen rakennusmääräyskokoelmaa, joka täydentää maankäyttö- ja rakennuslakia ohjein ja määräyksi. Uudisrakentamisessa määräykset ovat velvoittavia. Korjausrakentamisen osalta määräyksiä tulee noudattaa soveltuvilta osin. Viimekädessä korjausurakoissa määräyksen velvoittavuudesta ja toteutustavasta päättää kunnan rakennusvalvontaviranomainen. (Ympäristöministeriö 2018a.)

Rakentamismääräyskokoelma sisältää alakohtina suunnittelun ja valvonnan, rakenteiden lujuuden ja vakauden, paloturvallisuuden, terveellisyyden, käyttöturvallisuuden, esteettömyyden, meluntorjunnan ja ääniolosuhteet, energiatehokkuuden, rakennuksen käyttö- ja huolto-ohjeen sekä asuntosuunnittelun. Rakenteiden lujuuden ja vakauden osalta määrätään, että rakennuttajan, suunnittelijoiden ja urakoitsijoiden on varmistuttava kaikessa rakentamisessa siitä, että käytetyt rakennusmateriaalit ovat kantavuudeltaan riittävät niiden varaan tulevaan kuormaan nähden. Materiaalien kantavuudet tulee olla luotettavasti todennettu esimerkiksi lujuuskokein. Rakentamisen tai käytön aikana ei saa tulla tilannetta, jossa rakennelma olisi vaarassa sortua. Myös rakenteisiin kohdistuvat ulkoiset kuormat tulee ottaa huomioon niin, ettei näiden vaikutuksesta tapahdu suhteettoman suuria vahinkoja. (Ympäristöministeriö 2018a.)

Ympäristöministeriön asetus rakennusten paloturvallisuudesta edellyttää, että paloturvallisuus tulee ottaa huomioon kaikessa suunnitteluun liittyvässä toiminnassa. Yleisesti palon kehittymistä ja savun leviämistä on pystyttävä rajoittamaan niin rakennuksen sisällä kuin sen ympäristössäkin. Palon sattuessa reitit tulee olla sellaisia, että sisällä olevat pystyvät pelastautu-

maan esteettä. Rakennuksen käyttötarkoitus ja sinne sijoitetut toiminnot määrittävät rakennukselle paloluokan joka taas määrittää useita rakentamiseen vaikuttavia asioita kuten paloosastoinnin toteutuksen sekä käytettävien materiaalien palonkestovaatimukset. Paloluokkaan liittyy tietyissä tapauksissa maksimihenkilömäärään, rakennuksen kokoon ja käyttötarkoitukseen liittyviä rajoituksia. Asetuksessa esitetään myös käyttötarkoituksen ja paloluokan mukaan sellaiset rakennukset, joihin on asennettava hätäkeskukseen kytketty automaattinen paloilmoitinlaitteisto. (Ympäristöministeriö 2018b.)

3.6 Tietoturvallisuuden hallintakeinot

Standardi on vaatimuksia antava dokumentti, jonka tarkoituksena on standardisoimalla taata tuotteiden tai järjestelmien tasalaatuisuus, yhteensopivuus, turvallisuus ja vaatimuksenmukaisuus. Vaatimukset standardeissa on yleensä johdettu kansallisesta lainsäädännöstä tai EU-säädöksistä. Standardisoinnilla tarkoitetaan yhteisten toimintamallien luomista ja standardien tarkoitus on yhtenäistää toimintamalleja ja näin viranomaisten, elinkeinoelämän ja kuluttajien toimimista yhdenmukaisesti. Standardin mukaisella sertifioinnilla organisaatio voi osoittaa oman tuotteensa, toimintamallinsa tai palvelunsa yhdenmukaisuuden vaatimuksiin nähden. Vaikka standardeilla ei ole suoraa laillista asemaa, on niillä yleensä kiinteä yhteys EU-säädöksiin tai kansalliseen lainsäädäntöön. Aikaisemmin EU-säädöksissä ja direktiiveissä oli hyvin yksityiskohtaisia teknisiä vaatimuksia tuotteelle tai palvelulle. Näistä vaatimuksista johdettiin EU-standardit, jotka velvoitettiin sopimusperusteisesti vahvistamaan myös kansallisissa standardointielimissä. Nykyisin pyritään virallisissa säädöksissä määrittämään vaadittu taso ilman tarkkoja teknisiä kuvauksia. Kansalliset tai kansainväliset standardisointielimet yhdessä eri toimialaelinten kanssa luovat vaatimusten pohjalta standardit, jotka vastaavat vaadittuja tasoja. Euroopan standardisointijärjestö CEN edellyttää jäsenmaitaan vahvistamaan kaikki eurooppalaiset standardit kansallisesti. SFS:n standardisointiryhmät osallistuvat CEN:in standardisointitoimintaan Suomea edustavana toimijana. (Suomen standardisoimisliitto 2018.)

Standardi ISO/IEC 27002:2017 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohje (jäljempänä ISO 27002) on kansainvälinen ohje, joka on tarkoitettu organisaatioille tietoturvallisuuden hallintakeinojen toteuttamiseen sekä tietoturvallisuuden hallintajärjestelmän toteuttamisprosessin perustamiseen. Standardi ohjeistaa luomaan ja ylläpitämään tietoturvallisuuden hallintaa koskevat politiikat, prosessit, menettelytavat, organisaatiorakenteen sekä ohjelmisto- ja laitteistotoimintojen dokumentoinnin. Hallintakeinojen suunnittelu ja luominen tulee aloittaa sähköisen, fyysisen ja suullisen tietopääoman kartoittamisella ja jatkaa kuvaamalla tavat sekä kanavat, miten ja missä tieto liikkuu. Organisaation tulee myös tunnistaa siihen kohdistuvat turvallisuusvaatimukset, jotka pääasiallisesti tulevat organisaation itsensä toteuttamasta riskien arvioinnista, lakien ja asetusten asettamista vaatimuksista sekä organisaation omista tavoitteista ja liiketoimintavaatimuksista, jotka koskevat

tiedon käsittelyä, tallentamista, viestimistä ja arkistointia. Vasta tämän jälkeen voidaan aloittaa suojaamisen ja hallinnan keinojen suunnittelu. (Suomen Standardisoimisliitto 2017.)

Luku 11 käsittelee fyysistä turvallisuutta ja ympäristön turvallisuutta. Fyysisten hallintakeinojen tarkoitus on estää luvaton tunkeutuminen tietoaineistoihin ja tietojenkäsittelypalveluihin sekä turvata toiminnan häiriöttömyys ja tietoaineistojen vahingoittumattomuus. Hallintakeinoina esitetään selkeiden fyysisten turva-alueiden olemassaolo, kulunvalvonta, toimistojen, tilojen ja laitteistojen suojaus sekä niiden suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan, kaapelointien turvallisuus, tietoaineistojen sekä niitä sisältävien laitteiden turvallinen käytöstä poistaminen sekä tietoaineistojen turvallinen käsittely ja säilyttäminen. Turva-alueet tulee standardin mukaan olla selkeästi määriteltyjä ja sillä tavalla rakenteellisesti suojattuja, että murtautuminen näihin tiloihin on hankalaa. Asianmukaiset murtohälytinjärjestelmät tulisi asentaa alueellisesti ja tilojen ollessa tyhjillään tulee hälytysten olla päällä. Palo-ovet ja pelastusreitit tulee varustaa rikosilmoitinjärjestelmän ilmaisimilla. Kulunvalvontaa käytetään, jotta vain luvan saaneet henkilöt pääsevät alueelle. Pääsyoikeudet turva-alueille tulee katselmoida säännöllisesti ja tarpeettomat oikeudet poistaa. Alueella käytössä olevat laitteet tulee suojata asian mukaisesti ja muun muassa sähkökatkoilta. (Suomen Standardisoimisliitto 2017.)

4 Opinnäytetyössä käytetyt menetelmät

Toiminnallinen opinnäytetyö on usein työelämän tarpeisiin toteutettu projekti, jolla kehitetään tai tutkitaan toimeksi antaneen organisaation osoittamaan aihetta, tarkoituksena tuottaa konkreettisesti kehittävä, analysoiva tai muutoin toimeksiantajan toimintaa hyödyttävä työ. Yleisiä tiedonkeruumenetelmiä ovat muun muassa kirjallisuuskatsaus, dokumenttianalyysi, havainnointi, haastattelut sekä kyselyt. (Vilkka & Airaksinen 2003.)

Kirjallisuuskatsaus tiedonkeruumenetelmänä kartoittaa työn aiheen kannalta olennaiset olemassa olevat kirjalliset materiaalit sekä kokoaa ne teoreettiseksi viitekehykseksi, jonka avulla kokonaisuus hahmotetaan. Havainnointi on tietoa tutkimuskohteesta keräävä menetelmä, jota voidaan käyttää todellisessa ympäristössä tai laboratorio-olosuhteissa. Havainnointia tehdessä tutkija tekee tietoista tarkkailua kerätäkseen tutkimuskohteestaan tietoa, todentaakseen tapahtumia ja ilmiöitä. Menetelmää voidaan käyttää ennalta jäsennellysti tai vapaasti ja tutkimuskohteen mukana mukautuen. (Vilkka 2014.)

Tiedon analysointimenetelmänä dokumenttianalyysissa käsitellään kirjallisuuskatsauksen avulla tutkimuksen kannalta olennaisiksi tunnistettuja dokumentteja. Menetelmällä on tarkoitus analysoida jo julkaistua tietoa tutkimusaiheesta, järjestelmällisesti käsitellä niiden sisältöä sekä kartoittaa tutkimuksen kannalta merkittävät asiat. Prosessi etenee aineiston etsimisen, valinnan ja valmistelun kautta aineiston analyysiin, jonka jälkeen kerätty tieto pelkistetään ja siitä tehdään tulkinnat ja johtopäätökset. Teemoitetussa dokumenttianalyysissa tutkimusaiheen

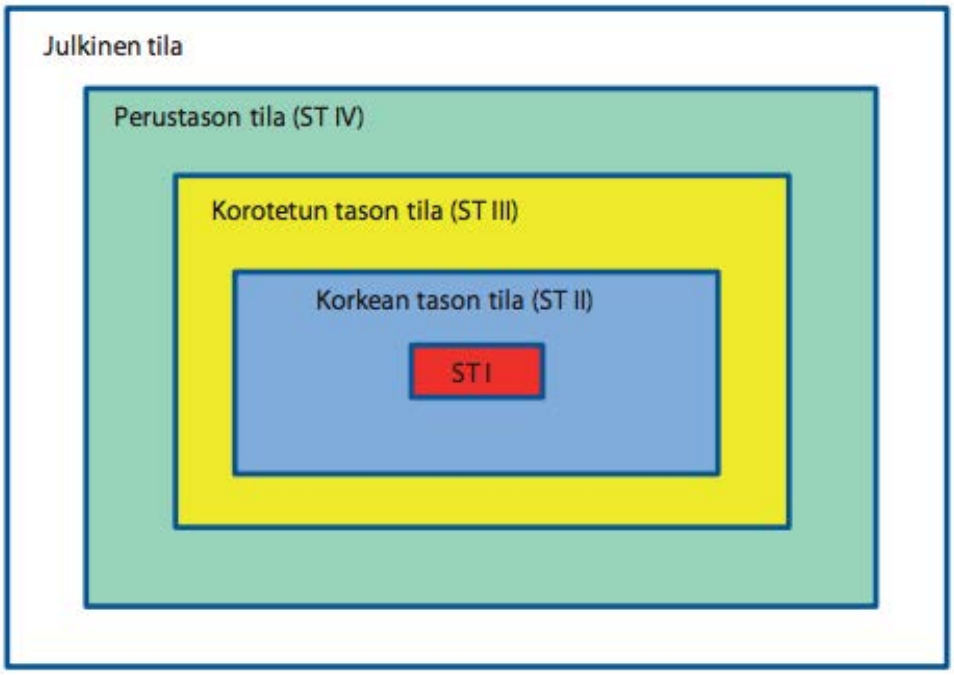
kannalta olennaiset asiat ryhmitellään ja järjestellään aihepiirien mukaisesti selkeiksi kokonaisuuksiksi. Menetelmää käytetään usein ongelmien ratkaisussa, kun analysoitavia dokumentteja on useita ja niissä käsitellään samoja aihepiirejä. (Vilkka 2014.)

5 Projektitilan fyysisen turvallisuuden vaatimukset

Yrityksen käsitellessä viranomaisen salassa pidettävää tietoa, tehdään se yleensä yrityksen muista, normaaleista toimistotiloista erillisissä ja suojatummissa tiloissa. Tällöin normaalin tuotannon tiloja, jotka eivät liity lakivelvoitteisesti suojattavan tiedon käsittelyyn, ei tarvitse hyväksyttää toimivaltaisella viranomaisella. Yrityksille on tarjolla useita eri ohjeita ja työkaluja joiden perusteella suojaustoimet voidaan toteuttaa. Viranomainen arvio toteutuksia kulloinkin voimassa olevaa Katakria käyttäen. Katakri 2015 viittaa monissa kohdin ISO 27002 hallintakeinoihin sekä niiden toteutusohjeisiin vaatimuksen mukaisena toteutusvaihtoehtona. Toinen lähde toteutusvaihtoehdoille on VAHTI 2/2013. (Puolustusministeriö 2015.)

5.1 Monitasoisen suojaamisen periaatteet

Yksi fyysisen turvallisuuden perusperiaatteista on monitasoinen suojaaminen. Sillä tarkoitetaan joukkoa toisiaan täydentäviä turvatoimia, joilla varmistetaan hyväksyttävä suojaustaso. (Puolustusministeriö 2015.) Katakri esittää vaatimuksena monitasoisen suojaamisen tiloille, joissa käsitellään ST-luokiteltua tietoa. Tilojen tulisi muodostua keskenään sisäkkäin olevista vyöhykkeistä, joiden välillä liikkuminen on hallittua ja tunnistettua. Korkeimman suojauksen tilojen tulee olla aina sisimpänä. Lisäksi huomioon tulee ottaa eri vyöhykkeiden toisiaan täydentävät rakenteet sekä suojattavaan tietoon kohdistuvat riskienarvioinnissa tunnistetut uhat. Vaatimus ohjaa paljolti ST-luokiteltujen tilojen sijoittelua sekä rakenteellista toteuttamista. Tietoa suojattaessa monitasoisen suojauksen muodostavat muun muassa käsittelytilan rakenteet, käsittelytilaa ympäröivien tilojen rakenteet, eri turvatekniset järjestelmät kuten rikosilmoitin- ja kulunvalvontajärjestelmät sekä vartiointipalvelut. VAHTI 2/2013 mallintaa turvallisuusvyöhykkeet kerroksittain niin että uloimpana on julkinen vyöhyke, jota seuraavat perustason tilat, korotetun tason tila, korkean tason tila ja sisimpänä korkean tason STI tila, kuten kuviossa 2 on esitetty. (Valtiovarainministeriö 2013.)



Kuvio 2: Turvallisuusvyöhykkeet (Valtiovarainministeriö 2013)

Standardi ISO 27002:2017 ohjeistaa toteuttamaan avaintilat niin, ettei niihin ole julkista pääsyä eikä rakennuksen tai tilan ulkopuolella ole merkkejä osoittamassa luottamuksellisten materiaalin käsittelyä ja säilyttämiseen liittyvien tilojen sijaintia. Tämä voidaan toteuttaa esimerkiksi VAHTI 2/2013 mallin mukaisesti. Luottamuksellinen materiaali tai puhe ei saa olla kuultavissa tilan ulkopuolelle ja sähkömagneettisen suojauksen toteuttamista tulisi harkita, riippuen mitä tietoa tiloissa säilytetään ja kuinka sitä käsitellään. VAHTI 2/2013-ohjeessa käsitellään turvallisuusvyöhykkeiden lisäksi vyöhykkeillä käsiteltävän salassa pidettävän materiaalin luokituksia. Ohje jakaa tilat julkiseen, perustason, korotetun tason sekä korkean tason työskentelytiloihin, jolloin julkiseksi tilaksi luokitellaan tilat ja parkkipaikat, joihin ainakin osan aikaa päivästä on vapaa kulku, kuten aulatilat. Perustason tiloilla tarkoitetaan normaaleja toimistotiloja, joissa voidaan tietyin edellytyksin käsitellä ja säilyttää STIV-luokan tietoa. Korotetun ja korkean tason työskentelytiloilla tarkoitetaan erityissuojaamista vaativia tiloja ja niissä käsitellään STII-III luokan tietoa. (Suomen Standardisoimisliitto 2017; Valtiovarainministeriö 2013.)

5.2 Alueita koskevat vaatimukset

Organisaation tulee määritellä alueet joilla voidaan käsitellä ja säilytetään salassa pidettävää materiaalia. Katakrin jaottelun mukaan ne ovat hallinnollinen alue, turva-alue ja tekninen turva-alue. Mitä korkeampi luokitus tiedolla on, joita tiloissa säilytetään ja käsitellään, sitä kovemmat ovat tilan suojausvaatimukset. Alueet tulee olla selkeästi rajattu, kulunvalvottu sekä tason mukaisesti muutoin fyysisesti suojattu, kuten rakenteilla ja murtohälytinjärjestelmin. Käytännössä hallinnollisella alueella tarkoitetaan normaaleista toimistorakenteista koostuvaa

rajattua aluetta, jossa voidaan käsitellä ja tietyin edellytyksin myös säilyttää STIV-luokan tietoa. Mikäli hallinnollisella alueella käsitellään salassa pidettävää tietoa, tulee tälle tiedolle olla luokituksen mukainen säilytysyksikkö ja tila tulisi olla lukittavissa lukolla, jonka avainten kopioiminen on estetty patenttisuojalla. Turva-alueen rakenteellisen suojauksen taso riippuu tilassa käsiteltävän ja säilytettävän tiedon luokituksesta sekä siitä, onko tilassa suojattavan aineiston säilyttämiseen vaatimukset täyttävä säilytysyksikkö. Tekniselle turva-alueelle Katakri määrittää turva-aluetta koskevien vaatimusten lisäksi tarkemmat valvonnan ja teknisen suojauksen velvoitteet. Yksi merkittävimmistä eroista turva-alueeseen nähden on luvattomien tietoliikenneyhteyksien ja laitteiden kielto sekä velvoite tarkastaa tila säännöllisesti luvattomien tietoliikenneyhteyksien ja elektronisten laitteiden havaitsemiseksi. Käytännössä tämä tarkoittaa sitä, että tilassa saa olla vain siellä käsiteltävälle tiedolle tarkoitettuja ja hyväksyttyjä laitteita ja yhteyksiä, ei esimerkiksi henkilökohtaisia matkapuhelimia tai muuhun käyttöön tarkoitettuja työasemia. (Puolustusministeriö 2015.) VAHTI 2/2013 mukaan STIV luokan tiloille ei ole määritelty erityisiä murtosuojavaatimuksia, mutta materiaalin säilytys tulee tapahtua lukitussa kaapissa ja tiloihin pääsyn tulee olla valvottua. Korotetun tason työtiloissa voidaan käsitellä ja säilyttää STIII-luokan materiaalia. Tilojen rakennusmateriaaleille, tiedon säilytysyksiköille sekä tilojen valvonnalle on asetettu korotettuja vaatimuksia. Korkean tason tilojen tulee olla korotetun tason tilojen sisäpuolella ja siellä voidaan käsitellä STII-luokan tietoa. Verrattuna korotetun tason tiloihin, korkean tason tiloille asetetaan korkeammat vaatimukset niin murtosuojauksessa, säilytysyksiköissä kuin salakatselun, salakuuntelun ja hajasäteilysuojauksen osalta. (Valtiovarainministeriö 2013.)

Pelastuslaissa ja Suomen rakennusmääräyskokoelmassa määritettyjä vähimmäisvaatimuksia ei voi ohittaa silloinkaan, kun tilaa rakennetaan suojaamaan viranomaisen salassa pidettävää tietoa. Lujuutta ja vakautta koskevat säännökset palvelevat myös tiedon suojaamisen tarpeita, mutta käyttöturvallisuus, paloturvallisuus ja esteettömyys voivat olla sellaisia asioita, jotka tulee ratkaista niin että nämä velvoitteet saadaan toteutettua mutta tieto suojattua.

Suojattavan tiedon käsittelyalueille tullee olla rajoitetut ja hallinnoidut kulkuoikeudet, jotka perustuvat tarpeeseen käsitellä tietoa. Oikeudet myönnetään nimetyn henkilön toimesta vain asianmukaisesti turvallisuusselvitetyille henkilöille. Kulkuoikeuksien hallinnointi tulee olla dokumentoitu ja ohjeistettu. Mikäli vierailut ovat tiloissa tarpeen, tulee vieraat aina kirjata ja olla saatettuna, korkeamman suojaustason tiloissa lisäksi asianmukaiselle tasolle turvallisuusselvitetty. Osana pääsyn hallintaa ja tiloissa liikkuvien henkilöiden tunnistamista tulee käyttää henkilökortteja tai muita vastaavia, näkyviä tunnisteita. Myös huoltohenkilöstö tulee huomioida ja heidän kulkuoikeutensa pitää perustua tarpeeseen huoltaa tiloja tai tiloissa olevia laitteita. Heidän hyväksyntänsä ja turvallisuusselvityksensä tulee olla samalla tasolla kuin tilan muiden käyttäjien. Tarvittaessa tilapäiset huollot voidaan suorittaa hyväksytyn tilan käyttäjän saattamana. Henkilöstömuutokset tilojen käyttäjissä ja huoltohenkilöstössä tulee huomioida heti kun

muutos tapahtuu. Tämä tarkoittaa kulkuoikeuksien päättämistä ja avainten takaisin kuittaamista. Mikäli avaimia ei saada takaisin, tulee lukot uudelleen sarjoittaa. (Puolustusministeriö 2015; Valtiovarainministeriö 2013.)

5.3 Turvallisuusjärjestelmät ja laitteet

Suojaustaso määrittää turvajärjestelmille, teknisille laitteistoille, lukituksille sekä säilytysyksiköille vaatimukset. Säilytysyksiköillä tarkoitetaan lukittuja kaappeja, kassakaappeja, elementtiholveja sekä turvakaappeja. Katakri 2015 esittää vaatimuksena SFS-EN 1143-1 tai SFS-EN-14450 standardit täyttävän tai vastaavan säilytysyksikön käyttöä suojaustasoille III ja II, tilan rakenteellisten vaatimusten täyttyessä suojaustasolla IV riittää lukittu kaappi. Säilytysyksiköiden osalta VAHTI 2/2013 viittaa Katakriin. ISO 27002 ei viittaa säilytysyksiköiden standardeihin, vaan edellyttää riskiarviointiin perustuvaa monitasoista suojaamista, jonka yksi muodoista säilytysyksiköt ovat. Useammalla esteellä asetetaan hitaampi ja vaikeampi pääsy käsiksi suojattaviin materiaaleihin. Hälytys-, kulunvalvonta- ja kameravalvontajärjestelmille Katakri 2015 vaatimuksena on järjestelmäasennusten ja tiedonsiirron toteuttaminen kuten lisätietona tai lähteenä mainitut standardit esittävät tai vastaavalla tavalla. Kameravalvontajärjestelmän suunnittelu, käyttöönotto sekä luovutustarkastus voidaan esimerkiksi tehdä kuten Finanssiala ry:n K-menetelmä ohjeistaa. VAHTI 2/2013-ohjeessa teknisiä turvallisuusjärjestelmiä edellytetään, mikäli tiloissa käsitellään STIII- tai korkeamman luokan tietoa. Valvontajärjestelmiksi edellytetään kameravalvonta-, kulunvalvonta- sekä rikosilmoitinjärjestelmää. Korkean tason tiloihin pääsy tulee todentaa kaksiosaisella tunnistuksella, esimerkiksi yhdistämällä kulkutunniste henkilökohtaiseen koodiin. Rikosilmoitinjärjestelmä voi perustason tiloissa olla Finanssiala ry:n murtosuojaluokan 2 vaatimukset täyttävä ja langaton, korotetun tason sekä korkean tason tiloissa vaaditaan luokka 3 eikä langattomia järjestelmiä hyväksytä. (Puolustusministeriö 2015; Valtiovarainministeriö 2013.)

Koska tiloihin, joissa säilytetään salassa pidettävää tietoa, edellytetään kulunvalvontajärjestelmää. Kulkuoikeudet tulee Katakrin mukaan kontrolloida ja pääsyoikeudet perustua tarpeeseen. Kulkuoikeuksia hallioiva henkilö tulee olla nimetty ja menettelytapojen ohjeistettu sekä dokumentoitu. Kaikki pääsyoikeudet avaimiin, numeroyhdistelmiin, säilytysyksiköihin ja tiloihin tulee dokumentoida ja ylläpitää vastuuhenkilön toimesta. Pääsyoikeuden saajan tulee olla turvallisuusselvitetty ja hänellä tulee olla tarve saada pääsy tiloihin tai tietoihin. Pääsyoikeudet katselmoidaan säännöllisin väliajoin. Turva-alueelle kulkuoikeudet voidaan myöntää vain tilaan oikeutetuille henkilöille ja kaikki kulkutapahtumat tulee olla jälkikäteen todennettavissa. Mikäli tilassa käsitellään STII-luokan tietoa, tulee edellä olevan lisäksi kulkutapahtumien todentaminen olla mahdollista niin sisään kuin ulos tilasta. Huoltotoimet alueilla, joissa käsitellään ST-luokiteltua tietoa, tulee tapahtua nimettyjen huoltohenkilöiden toimesta ja jos kyseessä on STIII-luokan tila tai korkeampi, lisäksi tilan kulkuoikeudet omaavan henkilön valvonnassa. ST-

luokitellun tiedon käsittely on kaikissa tiloissa kielletty huolto-, asennus- ja siivoustoimien aikana. (Puolustusministeriö 2015.) ISO 27002 toimintaohjeet ovat hyvin saman sisältöiset Katakrin kanssa, mutta standardi esittää, että vieraiden saapuminen sekä poistuminen tulisi kirjata ylös (Suomen Standardisoimisliitto 2017). VAHTI 2/2013 asettaa vieraiden hallinnalle yksityiskohtaisimmat ohjeet. Kaikkiin ST-luokiteltuihin tiloihin kohdistuvien vierailujen osalta edellytetään vieraiden tunnistamista, kirjaamista sekä vierailijatunnisteella varustamista. STIII-II luokituksen tiloissa on lisäksi huolehdittava, ettei vieraalla ole mahdollisuutta nähdä tiloissa käsiteltävää tietoa. STII-luokituksen tiloihin pääsyn ennalta ilmoitetulle vieraalle voi myöntää vain tilan turvallisuusvastaava. (Valtiovarainministeriö 2013.)

Avaimet ja kulkutunnisteet muodostavat tärkeän osan kulunhallinnasta ja Katakrin mukaan ne tulee ST-luokiteltuihin tiloihin hallinnoida nimetyn ja hyväksytyn henkilön toimesta. Avainhallinnan ja kulunvalvonnan prosessit tulee olla kuvattu ja ohjeistettu sekä kaikki avainten luovutukset ja palautukset kirjattu asianmukaisesti. Lisäksi muut kiinteistön avaimet eivät saa käydä ST-luokiteltuihin tiloihin, vaan niihin tulee olla omat avaimensa. Avainhallinnan luotettavuuden kannalta on lukostomallin hyvä olla sellainen, että se on edelleen patentin suojaama, vaikka tätä ei suoraan vaatimuksissa esitetäkään. Tällöin lisäavainten teettäminen on kontrolloitua ja avainmäärät tiedetään. (Kohdeyritys 2018a.) Mikäli turva-alueelle on vartiointi- ja huoltohenkilöstölle tarkoitettuja avaimia, ne tulee säilyttää sinetöidysti ja vartiointi- tai huoltokäynnillä tulee olla aina kaksi henkilöä paikalla. Salassa pidettävän aineiston säilytysyksiköihin ei myönnetä pääsyoikeuksia tiedonsaantitarpeen ulkopuolisille henkilöille. ISO 27002 ei ota avainhallintaan kantaa, vaan esittää että turva-alueelle pääsy tulee olla rajoitettua, tunnistettua ja todennettavissa. VAHTI 2/2013-ohje antaa yksityiskohtaisempia ohjeita lukituksesta ja avainhallinnasta viitaten Finanssiala ry:n murtosuojaohjeisiin. Vyöhykkeen ulkorajat tulee olla turvalukoin lukittu, avainten ja kulkuoikeuksien hallintajärjestelyt valvottu ja dokumentoitu. Jakamattomia avaimia tulee säilyttää kassakaapissa tai holvissa. Kaikki avaimet tulee olla yksilöllisesti merkitty ja niiden jako dokumentoitu. Pelastuslaitokselle tulee mahdollistaa pääsy myös korotetun ja korkean tason tiloihin, mutta avaimet tulee säilyttää valvotussa putkessa eikä kiinteistön ulkokuoressa saa olla putkea joka sisältää avaimen näihin suojattuihin tiloihin. Ulkoputkessa tulee olla vain reittiavain, jolla päästään kiinteistön kuoren sisäpuolella olevalle putkelle. Tiedon suojaamisen kannalta tämä vaatii turvallisuusteknistä valvontaa, eli avainputkien liittämistä rikosilmoitinjärjestelmään, jolloin saadaan ilmoitus, kun sylinteri irrotetaan putkesta. Suojattavien tilojen ohjeissa sekä pelastussuunnitelmassa tulisi ottaa huomioon pelastusviranomaisten pääsyn mahdollistaminen suojattaviin tiloihin mahdollisuuksien mukaan, huomioiden toteutusratkaisut sekä suojattava tieto. (Finanssiala 2017c; Valtiovarainministeriö 2013.)

5.4 Salakatselulta ja salakuuntelulta suojaaminen

Kestävät rakenteet ja oikein hallinnoidut pääsyoikeudet antavat jo kattavan suojan salakatselulta, mutta Katakri 2015 edellyttää tämän lisäksi ottamaan huomioon kaikki sellaiset seikat, mitkä voivat vaikuttaa tiedon näkymiseen asiattomille. Kannettavissa tietokoneissa tulee olla sivusta katselun estävät näytönsuojat ja työhuoneiden ikkunat tulee varustaa esimerkiksi sälekaihtimilla. (Puolustusministeriö 2015.) ISO 27002 esittää tilat toteutettavaksi siten, että luottamukselliset tiedot eivät ole nähtävissä tai kuultavissa ulkopuolisten toimesta. (Suomen Standardisoimisliitto 2017). Edellä mainittujen asioiden lisäksi VAHTI 2/2013-ohje ohjeistaa asettamaan näytöt sellaiseen työskentelyasentoon, ettei käsiteltävä informaatio näy ulos ikkunoista (Valtiovarainministeriö 2013.)

Salakuuntelusta Katakri edellyttää varmistumaan, ettei tilassa puhuttu tieto välity viereisiin tiloihin sellaisille henkilöille, joilla ei ole oikeutta tietoon. VAHTI 2/2013 ohje antaa myös salakuuntelun estämisestä yksityiskohtaiset, tilan suojaustason mukaan kovenevat vaatimukset. STIII ja STII luokitellun materiaalin käsittelyyn tarkoitetuissa tiloissa äänieristyksen tulee olla sellainen, että se estää asiattomia kuulemasta tilassa käytyjä keskusteluja. Tilojen ja tiedon käyttäjät tulee kouluttaa siihen, ettei salassa pidettäviä keskusteluja saa käydä esimerkiksi rakennuksen taukopaikoilla sekä siihen että huoneiden ovet ja ikkunat tulee pitää kiinni, kun keskustellaan salassa pidettävistä asioista. Työskenneltäessä monimuotoympäristöissä tulee salassa pidettävät keskustelut käydä aina niiden vaatiman äänieristävyyden täyttävissä suljetuissa huoneissa. (Puolustusministeriö 2015; Valtiovarainministeriö 2013.)

5.5 Toiminnan jatkuvuuden varmistaminen

Katakrin sisältämät vaatimukset toiminnan jatkuvuuden varmistamisesta ovat monilta osin hallinnollisia toimia. Se sisältää kuitenkin velvoitteen ennalta ehkäistä ja minimoida toimintahäiriöiden ja poikkeuksellisten tapahtumien vaikutusta salassa pidettävän tiedon käsittelyyn ja sen säilytykseen. Tilojen sisältäessä tietojärjestelmiä ja palvelimia, tarkoittaa tämä kiinteistöteknisestä näkökulmasta tunnistettuihin riskeihin varautumista eri teknisin ja mekaanisin järjestelmin. Myös LVIS-laitteiden ja niitä kontrolloivien laitteistojen vikaantuminen tulee ennakoida. LVI-automaation etähallinta tulee kuitenkin kriittisiksi tunnistettujen palvelin- ja laitetilojen osalta olla estetty. Näissä tiloissa tulee olla lisäsuojana myös olosuhdesensoreita. (Puolustusministeriö 2015.) ISO 27002 käsittelee laitteistojen sijoittelua ja suojausta siten, että ympäristöuhat ja luvaton tunkeutuminen on huomioitu ja mahdollisuuksien mukaan estetty. Lisäksi sähkön saanti ja muut peruspalvelut tulisi olla turvattu. (Suomen Standardisoimisliitto 2017). VAHTI 2/2013 käsittelee jatkuvuuden varmistamista sinänsä hyvin lyhyesti. Jatkuvuuden varmistamiseen on oltava tarvittavat suunnitelmat joiden mukaisesti toimimalla organisaation toiminta voi jatkua esimerkiksi eri toimipisteessä ja tarvittaessa rajoitetummassa mittakaavassa. (Valtiovarainministeriö 2013).

6 Projektitilan suunnittelu

Kohdeyrityksessä projektitilojen rakentaminen perustui tunnistettuun liiketoiminnalliseen tarpeeseen. Toimitilaprojektissa saneerattiin uudet toimitilat ja vanhoista luovuttiin. Yrityksen rakentaessa ST-luokitellun tiedon tuottamiseen ja säilytykseen tarkoitettua tilaa, tulevat tilan vaatimukset kansallisesta lainsäädännöstä. Sopimuksilla, ohjeilla, tilojen rakenteilla sekä teknisillä turvaratkaisuilla suojataan viranomaisen salassa pidettävää tietoa (Puolustusministeriö 2015.) Lähtökohtaisesti viranomaisen asiakirjat ovat julkisuusperiaatteen mukaisesti julkisia, ellei laissa toisin määritellä. Viranomaisen toimeksi antamassa hankkeessa viranomainen määrittää yritykselle luovuttamansa sekä hankkeessa tuotettavan tiedon luokituksen. Oikeutukset ja vaatimukset tiedon salaamiselle tulevat laista viranomaisen toiminnan julkisuudesta (L621/1999) sekä valtioneuvoston asetuksesta tietoturvallisuudesta valtionhallinnossa (A681/2010). Tarvekartoituksen perusteella kohdeyrityksen uusissakin tiloissa tarvittiin STIII tiedon käsittelyyn ja säilytykseen hyväksytty projektitila, olemassa olevien ja mahdollisten uusien projektien tarpeisiin.

6.1 Riskien arviointi

Toimitilahankkeen alussa toteutettiin riskien arviointi, jossa otettiin huomioon myös projektitilaan kohdistuvat mahdolliset riskit. Riskiarviointityöpajoja toteutettiin kaksi, tukitoimintojen henkilöstön kanssa omansa ja tuotannon yksiköiden kanssa omansa. Riskikartoitukset toteutettiin etukäteen valmisteltuja lomakkeita käyttämällä. Lomakkeiden kysymykset ja sisältö pohjautuivat yrityksessä sisäisesti tunnistettuihin liiketoimintaan kohdistuviin riskeihin, uusien toimitilojen katselmukseen, uusien toimitilojen sijaintiin ja erityispiirteisiin sekä suojattaviksi tunnistettuihin arvoihin. Arviointityöpajan vetäjä toimi fasilitaattorina, jonka tehtävä oli pitää työpajaan osallistuvat henkilöt oikeilla raiteilla ja ylläpitää keskustelua ennalta suunnitelluilla aihealueisiin liittyvillä esimerkeillä ja keskustelunohjauksilla. (Kohdeyritys 2017.)

Toimitila- ja tuotantopuolen edustajat tunnistivat hyvin saman tapaisia riskejä korkeiksi, keskitasoisiksi sekä merkityksettömiksi. Erot tulivat painotuksissa loogisesti niin että toimitilojen edustajat painottivat tiloja, ympäröiviä asioita, kiinteistössä ja kiinteistöteknisissä laitteissa tapahtuvia vikaantumisia, kun taas tuotannon edustajat painottivat tuotantoon vaikuttavia tekijöitä. Korkeiksi riskeiksi tunnistettiin vieraiden, ulkopuolisen henkilökunnan, asiakkaiden ja kiinteistön muiden käyttäjien aiheuttama tietovuoto, tulipalo sekä monitilatyöskentelyssä materiaalien käsittely. Tuotannon edustajat nostivat tärinän tuotannolle aiheuttamat riskit merkittäväksi. Keskitason riskeiksi tunnistettiin oman henkilökunnan aiheuttama tietovuoto, varkaus tai murto, vesivahinko, sähkö- tai tietoliikennekatkokset sekä ympäristöstä ja liikenteestä aiheutuvat asiat. Näissä toimitilapuoli painotti vikaantumisista johtuvia riskejä. Tuotannon edustajat eivät kokeneet oman henkilökunnan aiheuttamia tietovuotoja juurikaan merkityksellisenä. Suurin osa tunnistetuista riskeistä ovat sellaisia, että kohdeyrityksen toimitilahankkeissa

ne otetaan huomioon ja niiden vähentämiseksi on hyvät, olemassa olevat prosessit. Monitilatyöskentelyä ollaan nyt vasta lisäämässä, joten etenkin turvateknisillä ratkaisuilla sekä toimintojen sijoittelulla pyrittiin vaikuttamaan tähän riskiin. (Kohdeyritys 2017.)

6.2 Rakenteellinen suojaus

Projektitilan suunnittelussa otettiin huomioon kokonaistoimitilahankkeen alussa tehty riskikartoitus, jossa käsiteltiin myös korotetun suojaustason projektitilaan kohdistuvat riski. Suurimmiksi riskeiksi kartoituksessa nostettiin tulipaloriski, tietoon liittyvät riskit kuten materiaalitulostukset monitoimitilaympäristössä, aineistojen tuhoamisen prosessit sekä oman henkilökunnan ja ulkopuolisten aiheuttamat tietovuotoriskit. Projektitilan osalta todettiin, että edellä esitetyt riskit eivät ole merkittäviä tai vaadi lisätoimenpiteitä, mikäli tila ja sen toiminnot suunnitellaan ja toteutetaan olemassa olevan prosessin mukaisesti sekä Katakri 2015 vaatimukset täyttäen. (Kohdeyritys 2017.) Riskikartoituksen jälkeen tehtiin selvitys mahdollisista tiloista projektitilalle. Selvityksessä otettiin huomioon tilojen sijoittuminen kiinteistön sisällä, tilavaihtoehdon välittömään läheisyyteen sijoittuvat toiminnot, olemassa olevat rakennusmateriaalit ja niiden perusteella rakenteiden vahvistamisen tarve halutun suojaustason saavuttamiseksi sekä muutostöiden kustannusennusteet.

Alustavien suunnitelmien teon aikana tuli projektitilalle valitun kiinteistön omistajalta tieto, että tilan lattiarakenne ei mahdollisesti olekaan kantavuudeltaan riittävä tilaan sijoitettaville kassakaapeille. Lisäksi tilaa vahvistavien pellitysten toteuttaminen olisi ollut haasteellista, sillä ikkunoiden kohdalla olisi ratkaisu saattanut aiheuttaa kosteuden kerääntymistä rakenteiden väliin. Tämän vuoksi tilan sijoittamisen selvitys käynnistettiin uudelleen samoin kuin muu suunnittelu. Vuokrasopimustarkastelussa myös huomattiin, että uudesta kiinteistöstä on vuokrattu tila, jolle ei ollut osoitettu vielä käyttöä. Kyseinen tila vaihdettiin neuvotteluissa kohdeyrityksen jo vuokraamien tilojen vieressä sijaitsemaan tilaan, joka soveltui parhaiten projektitilakäyttöön.

Suunnitelmat toteutti kohdeyritykselle turvasuunnittelukonsultti viranomaisvaatimusten mukaisesti ja kohdeyrityksen linjauksia noudattaen. Tämän jälkeen kohdeyrityksen edustajat tarkistivat suunnitelmat ja hyväksyivät ne. Alustavat suunnitelmat toimitetiin suunnittelutoimistolle, joka toteutti lopulliset rakenne, paloilmoitin ja sprinklaus sekä LVIS suunnitelmat, jotka sisälsivät rakennustapaselosteen, huonekortit, huoneselosteet, pohjapiirroksen sekä sisäovikortit. Tarjoukset pyydettiin suunnitelmien pohjalta. Turvateknisten järjestelmien rakentamisesta tarjoukset pyydetiin kohdeyrityksen sopimustoimittajilta, joiden henkilöstössä on tarvittava määrä valmiiksi kohdeyrityksen toimeksiantoon turvallisuusselvitettyjä asentajia ja projektinjohtoa.

Olemassa olevien rakenteiden kartoitus on ohjaava vaihe rakenteiden suunnittelua. Kartoittamalla olemassa olevien rakenteiden murtolujuus sekä äänieristävyys voidaan tarvittaessa toteuttaa rakenteiden vahvistamisen suunnittelu sekä äänieristävyyden parantaminen. Tila joka vuokrattiin projektitilakäyttöön, sijaitsee kohdeyrityksen jo vuokraamien tilojen sisällä niin, että lisäämällä tilan ulkopuolella olevalle käytävälle ovi saadaan rajaava vyöhyke projektitilan ulkopuolelle. Tila sijoittuu kiinteistössä siten, että sinne kuljetaan kohdeyrityksen tilojen läpi, sen takaosa rajautuu kallioon ja viereinen tila on kohdeyrityksen käytössä oleva toinen vastaava tila. Käytävän varrella on kohdeyrityksen käytössä olevia muita tiloja. Käytävällä liikkuu jatkossa vain kohdeyrityksen kulkulupaprosessin mukaisesti hyväksyttyjä henkilöitä, kun käytävän väliovi on toteutettu. Projektitilan seinärakenteet ovat betoniharkkoja, joiden paksuus antaa riittävän murto- ja palosuojan tilalle. Koska tila sijaitsee kellarikerroksessa, on lattia maan varainen. Tämä takaa riittävän kantavuuden säilytysyksiköille sekä hyvän murtosuojan. Katto on teräsbetonilaattaa, jonka kantavuus on rakennuksen välipohjarakenteena rakennusmääräykset täyttävä. Olemassa olevissa läpivienneissä ei ole eristyksiä, jotka estäisivät ensisijaisesti palotilanteessa savun kulkeutumisen tilasta toiseen mutta oikein toteutettuna eristävät myös ääntä. Nämä läpiviennit massataan tai villoitetaan. Projektitilaan rakennetaan työhuoneita, jotka saattavat olla eri hankkeiden käytössä yhtä aikaa. Tästä syystä myös työhuoneiden väliseinäratkaisujen tulee olla äänieristäviä. Riittävä äänieristävyys saadaan toteuttamalla työhuoneiden seinät molemminpuolisilla kipsilevyillä, joiden välissä on teräsranka sekä villakerros. Työhuoneiden ovet toteutetaan puisina ääneneristysovina joiden äänieristävyys on 42 dB. (Insinööritoimisto 2018; Rakennusliike 1992; Ympäristöministeriö 2018a.)

Koska tilan olemassa olevat rakenteet antavat riittävän murtosuojan, tarvitaan vahvistavia rakenteita vain sellaisiin tilan kuoren osiin, jossa on kevytseinärakenteita. Kartoituskäynnillä todettiin, että ainoa tällainen kohta on tilan oviaukon yläpuolella. Kyseinen kohta suunnitellaan toteutettavaksi niin että molemmin puolin seinää on tuplakipsilevyt, sinkittyä teräslevyä ja näiden välissä teräsranka sekä palovilla. Läpiviennit tarkistetaan vielä rakennusvaiheessa, mutta kaikissa on oltava asianmukaiset palokatkomassaukset, jotka toimivat myös äänieristeinä. Ilmastointikanaviin suunniteltiin ääniloukut. Tilan sisäpuolella olevat kevytseinät puretaan. Tilan rajalle murtosuojaluokan 3 turvaovi. Ovella on standardin EN-1627 mukaisesti sertifiointi ja se täyttää Katakrin murtosuoja- ja äänieristävyysvaatimukset. (Insinööritoimisto 2018.)

6.3 Tekninen suojaus

Tekninen valvonta on yksi osa monitasoisessa suojaamisessa, jolla täydennetään rakenteellista turvallisuutta ja prosessein sekä toimintaohjein toteutettuja suojauksia. Kulunvalvontaa edellytetään käytännössä kaikissa ST-luokituksia käsittelevissä ohjeissa ja standardeissa, mutta mallikohtaisia suosituksia tai kovin syvälle toteutukseen meneviä vaatimuksia ei ole asetettu.

Rikosilmoitinjärjestelmä edellytetään vähintään tekniselle turva-alueelle, mutta se on suositeltava koko kiinteistöön. Kameravalvontajärjestelmä on ehdollinen kaikilla alueilla, mutta sillä voidaan tietyin edellytyksin korvata vartijakäyntejä. Vaikka mallikohtaisia vaatimuksia ei ole esitetty, Katakri 2015 velvoittaa käsittelemään langattomien verkkojen rajapintoja kuten julkisia verkkoja, jolloin langattomien verkkojen kautta kulkeva tieto edellytetään suojattavaksi viranomaisen kyseiselle suojaustasolle hyväksymällä salausratkaisulla. Teknisten turvajärjestelmien kohdalla langattomat ratkaisut ovat vielä harvinaisia tiedonsiirrossa, eivätkä järjestelmät välttämättä tue hyväksyttyjä salausratkaisuja. Tämän vuoksi turvatekniset ratkaisut edelleen toteutetaan pääasiassa kaapeloimalla, ST-luokitelluissa tiloissa tämä erityisesti on luotettavin ja yksinkertaisin tapa toteuttaa tiedon siirto. (Puolustusministeriö 2015.)

Kohdeyrityksellä on kuvatut yleiset periaatteet kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmien toteuttamisesta yrityksen hallinnoimissa tiloissa (Kohdeyritys 2018b). Periaatteiden luonnissa on käytetty lähdetietona muun muassa Finanssiala ry:n (jäljempänä FK) rakenteellisen murtosuojauksen ohjeita soveltuvan tason mukaisesti sekä kameravalvonnan suunnittelun ohjetta, K-menetelmää. Rikosilmoitinlaitteiston keskus sekä ilmaisimet valitaan FK:n laitelistausten mukaisesti. (Finanssiala 2017a; Finanssiala 2018b.) Myös ST-luokitellun materiaalin käsittelyyn ja säilyttämiseen tarkoitettuja tiloja toteutettaessa noudatetaan edellä mainittuja periaatteita, viranomaisvaatimukset huomioiden. Kamera- ja kulunvalvonta liitetään kiinteistön olemassa olevaan järjestelmään, mutta rikosilmoitinlaitteisto toteutetaan omalla itsenäisellä keskuksella. Kaikki kulunvalvonta tilaan ja tilasta ulos toteutetaan kaksipuolisilla kulunvalvontalukijoilla. Virastotyöaikojen ulkopuolella järjestelmä vaatii kaksiosaisen tunnistautumisen. Kameravalvonnalla katetaan liikenne tilaan sisään sekä mahdolliset hätäpoistumistiet, mutta tilassa tehtävää työtä ei valvota. Rikosilmoitinlaitteiston ilmaisimina käytetään liiketunnistimia, magneettikoskettimia, runkoääni-ilmaisimia sekä vartijakutsupainikkeita. Lasirikkoilmaisimia tilaan ei tarvita, koska se on ikkunaton. Rikosilmoitinlaitteistoon voidaan tarvittaessa liittää myös lämpötila-, kosteus- ja paloilmaisimia. Tässä projektitilassa on olemassa oleva, kiinteistön järjestelmään kytketty paloilmoitinlaitteisto sekä sprinklaus, joten erillisiä rikosilmoitinjärjestelmään kytkettyjä paloilmaisimia ei tarvita.

Vaatimuksenmukaisesti toteutettaessa valitulla lukituksella on voimassa oleva patenttisuoja ja lukkorungot sekä avainpesät valitaan FK:n Lukot – listauksesta. FK:n listaamat tuotteet täyttävät standardien SFS 7020 ja SFS 5970 vaatimukset. Kun tilan uloimpaan oveen lisätään murtosuojaluokan 3 turvalukko, voidaan käyttölukkona käyttää luokan 1 lukkorunkoa. Murtosuojaoven lukkorungot ovat FK:n hyväksymät ja standardin SFS-EN 12209 täyttävät. Käyttölukitus toteutetaan sähkölukkorungolla ja varmuuslukitus mekaanisella lukkorungolla, joka itsessään sisältää avainpesän. Avainpesien malliksi valitaan sellainen, jolla on voimassa oleva patenttisuoja. Murtosuojaoven käyttölukon avainpesä kuitenkin vaihdetaan tälle tilalle luotavan uuden lukoston pesään. Työhuoneiden oviin tulee mekaaniset lukkorungot ja tilan oman lukoston lukkopesät niin, että jokaiselle huoneelle on oma avaimensa. (Finanssiala 2018a.) Valmiisiin huoneisiin

tuodaan kassakaapit. Kohdeyrityksen käyttämät kassakaapit ovat Katakrin vaatimukset täyttävät ja hankitaan lukittavilla sisälokeroilla varustettuina. Käytetty kassakaappityyppi on murtotestattu ja tyyppihyväksytty eurostandardin EN 1143-1 mukaisesti murtosuojaluokkaan EURO II ja ne ovat FK:n kassakaappiohjeen mukaiset. (Finanssiala 2017b.)

ST-luokiteltujen projektien tietojenkäsittely-ympäristöt toteutetaan linjausten ja kuvausten mukaisesti lähtökohtaisesti niin sanottuina kylminä ympäristöinä. Tällä tarkoitetaan sitä, että hanketietoja käsittelevien laitteiden liittäminen tietoverkkoihin on estetty. Pääsääntöisesti laitteet ovat kannettavia työasemia, jotka asennetaan hankkeen ja toimeksiantajan tarpeiden sekä vaatimusten mukaisesti ja työskentelyaikojen ulkopuolella niitä säilytetään säilytys-yksiköissä, mikäli tilalla on muita käyttäjiä kuin kyseiseen hankkeeseen osallistuvat. Tarvittaessa projektitilaan voidaan rakentaa oma suljettu tietojenkäsittely-ympäristö hankkeen tarpeiden mukaisesti ja toimeksiantajan vaatimukset huomioiden. Lisäksi tietoja suojataan kohdeyrityksen sisäisten linjausten mukaisella kulkuoikeuksien rajaamisella. (Kohdeyritys 2016.)

7 Projektitilan toteutus

Suunnitelmien valmistuttua pyydettiin tarjoukset. Koska kyseessä on ST-luokitellun materiaalin käsittelyyn tarkoitettu tila, tulee ottaa huomioon luottamuksellisuus- ja turvallisuusselvitysnäkökulmat myös tarjouspyyntömateriaaleja jaettaessa. Kaikkien tarjoajien kanssa noudatettiin salassapitositoumusmenettelyä kohdeyrityksen periaatteiden mukaisesti. Turvallisuusteknisten ratkaisujen tarjoukset pyydettiin valmiiksi turvallisuusselvitysmenettelyn mukaisesti hyväksytyiltä sopimustoimittajilta. Kun tarjoukset oli saatu ja vertailu tehty, tehtiin tilaukset sekä sopimukset. Kaikille projektitilan toteuttamiseen osallistuville henkilöille teetettiin henkilöturvallisuusselvitys. (Kohdeyritys 2018c.)

Valittujen urakoitsijoiden kanssa aloitettiin pitämällä aloituspalaveri. Palaverissa käsiteltiin sopimusasioiden tilanne, vakuutusasiat sisältäen pääurakoitsijan vakuutuksen suuruus sekä kattavuus, turvallisuusasiat sekä niihin liittyvät asiakirjat sekä vastuut, projektiin osallistuvien henkilöiden roolit sekä vastuut, käytettävät aliurakoitsijat, suunnitelmien tilanne, dokumenttien käsittely, jako sekä turvallisuusselvitysmenettelyt, työmaan käytännön asiat sekä aikataulut. Palaverin päätteeksi tehtiin katselmointi urakka-alueella. Aikatauluja sovittaessa sovittiin seurantapalaverien tarpeesta, vastaanottotarkastuksen päivämäärä sekä mahdolliset sanktiot urakan viivästymisestä. Rooleista sovittaessa käsiteltiin päätoteuttaja ja tilaajavastuut sekä vastuuhenkilöt jotka huolehtivat vastuiden täyttymisestä roolinsa mukaisesti. Lähtökohtaisesti pääurakoitsija vastaa työmaan turvallisuudesta, rajaamisesta, valvonnasta ja vartioinnista sekä päätoteuttajavelvoitteiden huolehtimisesta kuten työntekijätietojen keräämisestä ja ilmoittamisesta verottajalle. Kohdeyrityksen nimetyn edustajan vastuulla on huolehtia tilaajan velvoitteista ilmoitusmenettelyineen. Koska tilan rakenteellinen toteutus tulee dokumentoida, sovittiin aikataulujen mukaiset katselmukset urakan edistymiselle, jolloin kohdeyrityksen edustaja

käy kuvaamalla dokumentoimassa eri rakenteiden toteutuksen ennen kuin ne peitetään seuraavilla materiaaleilla. Välitarkastuspöytäkirjaesimerkki on liitteenä 1. Käytetyt materiaalit urakoitsijat voivat dokumentoida esimerkiksi materiaaliluetteloita käyttämällä. Turvateknisistä asennuksista, kuten turvaovesta, rikosilmoitin-, kameravalvonta- ja kulunvalvontajärjestelmistä tuotetaan asennuspöytäkirjat. Pääurakoitsija vastaa eri urakoitsijoiden tiedottamisesta urakan etenemisestä sekä kokonaisaikataulussa pysymisestä.

Kun toteutusvaihe saadaan käynnistettyä, tulee rakennusaikana tehdä todennukset sellaisille ratkaisuille, jotka rakentamisen edetessä peitetään pintamateriaaleilla. Tällaisia ovat muun muassa rakenteita vahvistavat pellitykset, läpivientien tiivistäminen, ääniloukut sekä kaapeloinnit, jotka jäävät valmiissa tilassa pintarakenteiden alle piiloon. Liitteenä yksi on välitarkastuspöytäkirjapohja, johon on hahmoteltu rakennusaikana tehtävien tarkastusten alakohdat. Pöytäkirjan sekä sen liitteiden tarkoitus on todentaa myöhemmässä vaiheessa piiloon jäävien rakenteiden toteutus. Tarkastuspöytäkirjaa tukemaan on hyvä valokuvata eri vaiheet ja liittää kuvat liitteinä pöytäkirjaan. Mikäli toteutuksessa havaitaan puutteita tai korjattavaa, on tehtävä myös tarkastus, kun korjaavat toimenpiteet on suoritettu.

Rakennustöiden valmistuttua pidetään rakennusurakan vastaanottotarkastus ja turvaurakoiden käyttöönottotarkastus. Käyttöönottotarkastuksen ja vastaanottotarkastuksen mallipohjapöytäkirjat ovat liitteinä 2 ja 3. Turvaurakoitsijoiden kanssa kohdeyrityksellä on sopimukset, joissa on määritelty käyttöönottoaika, joka urakan koosta riippuen on kahdesta viikosta kolmeen kuukauteen. Tarkastuksessa käydään läpi toteutusaikana suunnitelmiin tehdyt muutokset sekä niiden toteutus, testataan laitteistojen tekninen toimivuus, käydään läpi mahdolliset lisätöinä tehdyt asiat, sovitaan käyttäjille ja turvallisuusorganisaatiolle tarvittavista käytönopastuksista, tarkastetaan luovutusdokumentit, listataan puutteet sekä sovitaan puutteiden korjaamisesta ja koekäyttöajan pituudesta. Teknisten tarkastusten ja havainnoinnin lisäksi tärkeää on tarkastaa dokumentaation paikkansa pitävyys. Rakenteiden osalta tulee olla olemassa materiaaliluettelot sisältäen materiaalien ja laitteiden tekniset tiedot sekä asennuspöytäkirjat tai selosteet. Turvateknisten asennusten osalta tulee olla dokumentoituna järjestelmäkaaviot, järjestelmän kuvaus, ristikytkentätiedot, testauspöytäkirjat sekä pistesijoituskuvat joista muodostuu järjestelmän loppukuvat. Tarkastuksessa katselmoidaan paikan päällä työsuoritukset ja kirjataan puutteet pöytäkirjaan. Tarvittaessa vastaanottoa ei suoriteta vaan sovitaan seuraavasta tarkastuksesta, johon mennessä kirjatut puutteet tulee korjata. Tarkastuspöytäkirjat ovat osa tilan dokumentaatiota välitarkastusten ja suunnitelmien lisäksi.

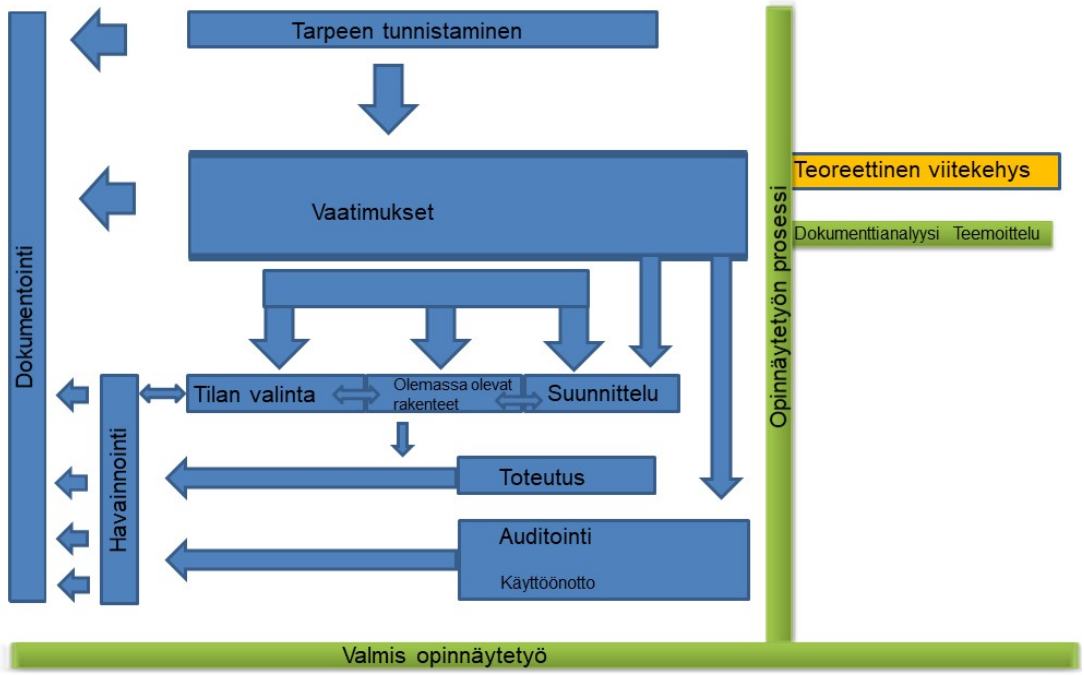
Käyttöönottotarkastuksen jälkeen tila voidaan ottaa käyttöön, mutta vasta viranomaisen auditoinnin jälkeen siellä voidaan säilyttää ja käsitellä aiotun suojaustason dokumentteja. Kohdeyritys koostaa tilasta dokumentaation sekä selosteet toteutuksesta. Kun dokumentit ovat valmiit ja tila valmis käyttöön otettavaksi, sovitaan toimivaltaisen viranomaisen kanssa auditointi.

Auditoinnissa esitetään koostettu dokumentaatio ja tämän jälkeen käydään todentamassa asennukset sekä toteutetut ratkaisut paikan päällä. Fyysisen turvallisuuden osalta viranomainen toteuttaa auditoinnin vertaamalla toteutusta Katakrin vaatimuksiin. Teknisen tietoturvallisuuden osuudet auditoidaan aina hankekohtaisesti, kyseiseen hankkeeseen toteutettujen ICT-ratkaisujen osalta. Mikäli ratkaisuissa on puutteita tai toteutuksessa huomautettavaa, tulee nämä korjata ennen kuin tila saa hyväksynnän ja voidaan ottaa käyttöön. Käyttöönottoaika on hyvä ajankohta toteuttaa viranomaisauditointi, sillä silloin viranomaisen esittämät huomautukset voidaan korjauttaa käyttöönottoaikana ja lopulliset toteutukset saadaan tarkastettua vastaanotossa sekä asianmukaisesti loppudokumentteihin. Viranomaistarkastuksen laajuus ja tarkasteltavat asiat riippuvat toimivaltaisesta viranomaisesta sekä siitä, onko tarkastettavalla organisaatiolla jo Katakri 2015 T-osan mukaisesti tarkastetut yritystasoiset prosessikuvaukset, toimintaohjeet ja muut turvallisuusjohtamisen menettelyt. Viranomainen tekee omasta tarkastuksestaan pöytäkirjan sekä tarvittaessa korjausmääräyksen ennen tilan käyttöönottoa ST-luokitellun materiaalin säilytykseen. Auditoinnit ovat osa yritysturvallisuusselvitystä, jolla todennetaan kohdeyrityksen kyky suojata viranomaisen salassa pidettävää tietoa eri hankkeissa. Yritysturvallisuusselvitystä edellytetään yhteisöturvallisuussopimuksen tekemiseen.

Vastaanottotarkastuksessa tehdään hyvin samanlainen rakenteiden ja teknisten laitteiden tarkastus kuin käyttöönottovaiheessa. Kun vastaanotto on suoritettu hyväksytysti, alkaa takuuaika ja voidaan aloittaa taloudellisen loppuselvityksen tekeminen. Taloudellisessa loppuselvityksessä käydään läpi alkuperäinen urakkasumma, mahdolliset toteutuksen aikaiset lisätyöt ja mahdolliset hyvitykset toteutumattomista asioista sekä myöhästymisestä määrätyt sanktiot. Lisätyöt ja niiden tilaaja tulee eritellä selvityksessä. Jokainen urakoitsija koostaa osaltaan taloudellisen loppuselvityksen, jotka kohdeyrityksen tilaajaedustaja tarkastaa ja mahdollisten korjausten jälkeen hyväksyy. Kun taloudelliset loppuselvitykset on hyväksytty, voidaan urakkasummien viimeiset positiot vapauttaa.

8 Opinnäytetyön prosessi

Tämä opinnäytetyön tarkoitus oli kuvata kohdeyrityksen projektitilan suunnittelu, toteutus sekä käyttöönottoa edeltävää viranomaistarkastusta (kuvio 3). Kuvaamalla projektitilan prosessi tarpeesta käyttöön otettuun tilaan opiskelijan oli tarkoitus kohdeyritykselle dokumentin, johon on koostettu projektitiloja koskevat vaatimukset, suunnittelun keskeiset asiat, toteutukseen liittyvät näkökulmat sekä rakentamisen valvontaan liittyvät asiat. Liitettynä yrityksen toimitilaturvallisuuden ohjeeseen tätä raporttia voidaan käyttää jatkossa projektitilan vaatimukset koostavana sekä prosessin vaiheet ja toteutuksen kuvaavana dokumenttina. Koska rakennustyöt keskeytyivät odottamatta vesivahingon takia, on toteutusaikaiset asiat sekä auditoinnin valmistelu jouduttu käsittelemään aiottuina toimina, jotka tapahtuvat vasta opinnäytetyön valmistumisen jälkeen.



Kuvio 3: Projektitilan suunnittelun ja toteutuksen prosessi

Dokumenttianalyysi oli keskeinen menetelmä niin projektin suunnitteluvaihetta kuin opinnäytetyön teoreettisen viitekehyksen rakentamisessa. Analyysi toteutettiin, jotta vaatimukset projektitilalle saatiin kartoitettua ja suunnittelu toteutettua niin että valmis projektitila täyttää edellytetyt vaatimukset. Keskeisin dokumentti projektitilan kannalta on Katakri 2015, koska valmis tila tullaan arviomaan tätä kriteeristöä käyttämällä. Katakri viittaa toteutusohjeina ISO 27002 standardiin sekä VAHTI 2/2013 ohjeeseen, joten kohdeyrityksen valitsemien toteutusvaihtoehtojen oli täytettävä näiden dokumenttien asettamat vaatimukset. Koska kriteeristö pohjautuu lainsäädäntöön, tuli analyysiin valita myös nämä lait ja asetukset. Lisäksi projektitila toteutetaan olemassa olevaan kiinteistöön, niin lähtötilanteen kartoitus oli olennainen osa suunnittelun aloittamista. Tehokkaalla suunnittelulla pyrittiin käyttämään mahdollisimman kattavasti hyödyksi olemassa olevat rakenteet ja toteuttamaan uudistukset ja vahvistukset kustannustehokkaasti. Projektitilalle vaatimukset antavia dokumentteja analysoitaessa nostettiin esille fyysisen turvallisuuden eri osa-alueita ja teemoittelulla ne koottiin yhtenäisiksi teemakokonaisuuksiksi, joihin perustuen suunnittelu tehtiin ja toteutusaikainen valvonta ja todentaminen tullaan suorittamaan.

Havainnointia käytettiin tämän tutkimuksen kaikissa vaiheissa ja sillä tullaan todentamaan myös valmiin tilan toteutus testauksia ja tarkistuslistoja hyväksi käyttäen. Dokumentaation paikkansa pitävyys tulee varmistaa, eli menetelmää käytetään jäsennellysti. Projektitilan suun-

nitteluvaiheessa tehtyjä havaintoja yhdistettynä dokumenttianalyysin tuloksiin käytettiin tarvittavien rakenteellisten vahvistusten sekä turvateknisten toteutusten suunnitteluun. Toteutuksen eri vaiheet tullaan myös dokumentoida, jotta niiden olemassaolo voidaan myös jälkikäteen osoittaa.

9 Tulokset

Lopputyön kirjoittamisen puitteissa projektitilan toteutusta ei saatu päätökseen. Urakoitsijoiden valitsemisen ja sopimusten teon jälkeen aloitettiin tilassa olevien rakenteiden purkaminen suunnitellusti. Purkujen aikana pääurakoitsija havaitsi lattiarakenteissa mahdollisia kosteusvaurioita. Purut suoritettiin loppuun, mutta muutoin työt keskeytettiin ja tilassa suoritettiin kosteusmittaus. Kosteusmittausraportti osoitti selviä kosteusvaurioita maavaraisessa alapohjassa. Opinnäytetyön valmistumisen hetkellä rakennusurakka on keskeytetty ja korjaustoimenpiteitä suunnitellaan. Tähän mennessä tuotetut dokumentit on koostettu ja esitetty viranomaiselle joka on ne alustavasti hyväksynyt. Urakan keskeytymisestä huolimatta voidaan suunnittelu ja alustavat työt jo arvioida.

Ajallisesti tilan suunnittelu, havainnointi ja dokumenttianalyysi kulkivat käsi kädessä. Projektitilaksi valittu tila katselmoitiin, arvioitiin muutostarpeet ja tehtiin suunnitelmat. Kustannusarviot oli tehty jo eri tilavaihtoehtojen kartoituksen yhteydessä per tila. Valmiiden suunnitelmien pohjalta pyydettiin tarjoukset ja kun ne oli saatu, tarkenettiin kustannusarviota. Kun urakoitsijat oli tarjousten perusteella valittu, tehtiin sopimukset ja työt aloitettiin. Koko prosessin ajan tehtiin dokumentointia, jotta prosessin eteneminen, eri vaiheet ja kustannukset ovat jälkeen päin todennettavissa. Kun toteutusvaihetta tulevaisuudessa päästään jatkamaan, eri vaiheet dokumentoidaan havainnoimalla sekä kuvaamalla eri työvaiheet. Tilan valmistuttua tehdään ensin omat tarkastukset kuten käyttöönottotarkastus ja korjautetaan mahdolliset puutteet tai virheet. Urakoitsijoiden kanssa käydään läpi taloudelliset loppuselvitykset, kun kaikki puutteet on korjattu. Tämän jälkeen toteutetaan viranomaisauditointi. Viranomaisen tarkastuspöytäkirjan mukaisesti tehdään vielä mahdolliset korjaukset, tarkastutetaan ne viranomaisella ja tämän jälkeen tila voidaan ottaa käyttöön. Tilan valmistuttua ja hyväksytysti suoritettujen auditointien jälkeen kootaan dokumentaatio yhteen, arvioidaan projektin vaiheet sekä taloudellisissa tavoitteissa onnistuminen. Lopuksi viimeistellään raportti ja kirjoitetaan yhteenveto.

Suunnittelu toteutettiin Katakri 2015 ja kohdeyrityksen linjaukset, ohjeet ja vaatimukset täyttäen. Itse toteutuksen suunnittelu sujui odotetusti, mutta haasteiksi osoittautuivat olemassa olevien rakenteiden dokumentaatio ja todentaminen. Myöskin rakenteiden vahvistamiseksi suunniteltavat pellitykset ovat haasteellisia tiloissa, joissa on ikkunarakenteita. Liian tiiviisti toteutettaessa ikkunakohtiin saattaa kerääntyä kosteutta ja pitkällä aikavälillä aiheuttaa kosteusvaurioita rakenteille. Toisaalta kosteuden kerääntymisen estävä väljyys tai reiät heikentävät murtosuojausta ja dB-vaimennusta. Kantavien rakenteiden tarkat tekniset tiedot ovat myös

merkittävät, jotta kassakaapeille saadaan riittävä kantavuus ilman alapohjarakenteiden heikentymisen ja sortumisen vaaraa. Lisäksi ST-luokitellun materiaalin käsittelyyn ja tuottamiseen tarkoitetun tilan sijoittaminen on selkeästi haastavaa, kun kohdeyrityksen toimitiloissa tehdään paljon muutakin työtä. Tällöin arvioitavaksi tulee liiketoiminnalliset näkökulmat, mitkä hankkeet ovat sellaisia, että niiden vaatimiin tiloihin kannattaa rahallisesti panostaa ja sijoittaa tilat priorisoidusti. Puhtaasti tätä yksittäistä tilaa ajatellen ihanteellista olisi päästä valitsemaan tila ennen kuin muita toimintoja on sijoitettu ympäröiviin tiloihin. Paras sijainti olisi kohdeyrityksen omien toimintojen ja tilojen sisällä sijaitseva tila, joka on kantavien rakenteiden ympäröivä, ikkunaton ja kiinteistön ylemmissä kerroksissa. Tällöin saadaan helpoiten riittävä kantavuus säilytys-yksiköille, salakatselun estävyys, minimoidaan rakenteellisten muutosten tarve ja saadaan ympäröiviksi tiloiksi kehäsuojauksen periaatteet täyttäviä tiloja ilman suuria muutoksia. Taulukossa yksi esitetään opinnäytetyössä käsitellyn prosessin suunnittelun ja toteutuksen vaatimukset, osa-alueet, vaatimuksenmukaisuuden toteutus sekä toteutusratkaisujen todentaminen.

Projektitilan fyysisen turvallisuus toteutuksen prosessi			
Suunnittelu		Toteutus	
Vaatimus	Osa-alueet	Toteutus	Todentaminen
Monitasoisen suojaamisen periaatteet	• Kehäsuojaus • Tiedon säilytystilat • Turvatekniset järjestelmät • Prosessit ja ohjeet	• Tilan sijoittaminen, ympäröivät vyöhykkeet • Säilytysyksiköt • Sähköiset turvatekniset järjestelmät o Rikosilmoitinlaitteisto o Kulunvalvontalaitteisto o Kameravalvontajärjestelmä • Lukitus o Lukkorungot o Varmuuslukot o Avainpesät • Sisäiset ohjeet ja prosessikuvaukset o Hyväksytyt prosessikuvaukset o Toimintaohjeet o Periaatekuvaukset	• Asemakaava, kiinteistön pohjakuvat • Säilytysyksiköiden asennuspöytäkirjat • Sähköiset turvatekniset järjestelmät o Asennuspöytäkirjat o Testauspöytäkirjat o Järjestelmäkuvaukset ja –selosteet • Lukitus o Lukostokaaviot o Asennuspöytäkirjat o Lukituspiirrustukset o Lukoston dokumnetaatio o Avainhallinnan dokumentointi • Sisäiset ohjeet ja prosessikuvaukset o Tarkastus o ST-luokitusmerkinnät o Versionumerot o Laatijatiedot o Hyväksyntätiedot o Laadintapäivä • Tarkastus- ja käyttöönottopöytäkirjat
Alueet on jaettu turvallisuusvyöhykkeisiin ja suojataan luokituksen mukaisesti	• Julkinen alue • STIV – Hallinnollinen alue • STIII – Turva-alue • STII – Tekninen turva-alue • (STI – Tekninen turva-alue)	• Julkinen alue o Uloin kehä, ei vaatimuksia • STIV – Hallinnollinen alue o Organisaation sisäinen o Rakenteet normaalia toimistorakennetta o Kulku rajoitettu ja henkilöt tunnistetaan o ST-luokitellun materiaalin säilytys Lukitussa säilytystilassa • STIII – Turva-alue o STIV aluetta koskevan lisäksi: o Pääsyoikeudellisten turvallisuusselvitykset o Vierailut luvanvaraisia o Vastuuhenkilöt nimetty ja roolit kuvattu o Rikosilmoitinjärjestelmä o Rakenteiden korotettu murtosuojausluokitus o STIII-luokan tiedolle säilytys-yksiköt o Turvallisuusmenettelyt • STII – Tekninen turva-alue o STIV-III alueita koskevan lisäksi: o Alue lukittu ja valvottu kun ei käytössä o Henkilöliikenne ja aineistoliikenne valvotaan o Ei luvattomia yhteyksiä ja laitteita o Tarkastukset luvattoman tieto- ja viestintäliikenteen varalta • (STI – Tekninen turva-alue)	• Dokumentaatiot o Sisäiset ohjeet ja prosessikuvaukset o Periaatekuvaukset o Tilojen sijoituksen pohjakuvat o Rakenteiden dokumentaatiot o Kulunhallinnan dokumentaatiot o Tarkastus- ja käyttöönottopöytäkirjat o Diaarit o Lokit o Henkilölistaukset

Taulukko 1: Projektitilan fyysisen turvallisuuden toteutuksen prosessi 1/2

Projektitilan fyysisen turvallisuus toteutuksen prosessi			
Suunnittelu		Toteutus	
Tietojen fyysinen suojaus on toteutettu suojaustason mukaisesti ja luvaton pääsy estetty	• Pääsyn estävät ratkaisut • Valvonnan ja todentamisen ratkaisut • Kulunhallinnan ratkaisut	• Lukitus o Murtosuojaluokitus o Oma lukosto o Voimassa oleva patenttisuoja o Varmuuslukot o Avainhallinnan vastuuhenkilö • Rakenteet o Rakenteiden murron kesto o Rajapintojen murronkeston vahvistaminen o Materiaalien äänieristävyys o Läpivientien ääniloukut ja eristeet • Säilytysyksiköt o Murtosuojaluokitus • Rikosilmoitinjärjestelmä o Koodien hallinnointi o Keskuksen luokitus o Ilmaisimien luokitus o Tarkoituksenmukaiset ilmaisimet o Hälytysten vasteaika • Kameravalvontajärjestelmä o Kattavuus o Sijoittelu • Kulunvalvonta o Kulkuoikeuksien vastuuhenkilö o Oikeudet tarveperusteisia o Todennus sisään ja ulos	o Lukostokaavio o Asennuspöytäkirjat o Testauspöytäkirjat o Avainhallinnan kirjanpito • Rakenteet o Rakenteiden selosteet o Tarkastuspöytäkirjat o Materiaaliluettelot • Säilytysyksiköt o Asennuspöytäkirjat o Koodien hallinnoinnin kirjanpito • Rikosilmoitinjärjestelmä o Koodien hallinnoinnin kirjanpito o Asennuspöytäkirjat o Testauspöytäkirjat o Järjestelmäkuvaukset ja -selosteet • Kameravalvontajärjestelmä o Asennuspöytäkirjat o Testauspöytäkirjat o Järjestelmäkuvaukset ja periaatteet • Kulunvalvonta o Asennuspöytäkirjat o Testauspöytäkirjat o Järjestelmäkuvaukset ja hallinnoinnin periaatteet o Kulkuoikeuksien dokumentointi o Kulkujen ja henkilöiden todentaminen ja dokumentointi
Toiminnan jatkuvuuden varmistaminen	• Toiminnan jatkuvuus poikkeusoloissa o Sähkökatkot o Poikkeavat sääolot o Vahinkotilanteet kiinteistössä Palovahinko Vesivahinko Rakenteiden ja laitteiden rikkoutuminen o Organisaation poikkeusolot o Kansalliset poikkeusolot	• Sähkökatkot o Laitteistojen virransaanti, akut o Mekaaniset ratkaisut, avaimet • Poikkeavat sääolot o Rakenteiden lujuus o Tilan sijainti o Laitteistojen sijoitteluja ja suojaus • Vahinkotilanteet kiinteistössä o Laitteistojen sijoitteluja ja suojaus • Palovahinko o Tilan palosuojaus ja osastointi o Varautumis- ja toimintasuunnitelmat • Vesivahinko o Olosuhdeilmaisimet o Rakenteiden kesto o Varautumis- ja toimintasuunnitelmat • Rakenteiden ja laitteiden rikkoutuminen o Valvontalaitteistot o Varautumis- ja toimintasuunnitelmat • Organisaation poikkeusolot o Valvontalaitteistot o Varautumis- ja toimintasuunnitelmat • Kansalliset poikkeusolot o Valvontalaitteistot o Varautumis- ja toimintasuunnitelmat • Organisaation varautumissuunnitelman	• Sähkökatkot o Laitteistojen dokumentaatio o Testauspöytäkirjat • Poikkeavat sääolot o Rakenteiden, tilan ja laitteiden dokumentaatio • Palovahinko o Laitteiston dokumentaatio o Varautumis- ja toimintasuunnitelmat • Vesivahinko o Laitteistojen dokumentaatio o Varautumis- ja toimintasuunnitelmat • Rakenteiden ja laitteiden rikkoutuminen o Varautumis- ja toimintasuunnitelmat • Organisaation poikkeusolot o Varautumis- ja toimintasuunnitelmat • Kansalliset poikkeusolot o Varautumis- ja toimintasuunnitelmat

Taulukko 1: Projektitilan fyysisen turvallisuuden toteutuksen prosessi 2/2

Taulukot havainnollistavat dokumentoinnin ja pöytäkirjojen merkityksen, jotta viranomaisille voidaan todentaa tehdyt toimet sekä niiden perusta. Vaatimuksena ja toteutuksen lähteenä käytetään aina kulloinkin voimassa olevia määräyksiä, säädöksiä ja ohjeita. Olennaista on kuvata näiden vaatimusten, ohjeiden ja standardien sisältö sekä dokumentoida rakennusaikaiset toteutukset. Koska tilaa ei saatu valmiiksi, kuvattiin toteutusvaihetta käsittelevässä luvussa vielä tulossa olevat vaiheet.

10 Johtopäätökset ja loppupohdinta

Raporttina tämä työ kuvaa ST-luokitellun tilan suunnittelun ja toteutuksen fyysisen turvallisuuden vaatimukset. Vaikka Katakri 2015 onkin pääasiallinen työkalu ja vaatimukset kokoava dokumentti viranomaisen salassa pidettävien asiakirjojen suojaamisen ratkaisuissa, viittaa se useaan muuhun dokumenttiin, jotka jälleen viittaavat vielä useampaan dokumenttiin ja standardiin. Vaikka Finanssiala ry:n turvallisuusohjeisiin ei missään näistä viitata, on se organisaatiolle hyödyllinen tietopankki, jonne on koostettu selkeisiin julkaisuihin, ohjeisiin ja listauksiin eri standardien ja vaatimusten mukaiset turvatekniset ratkaisut. Olennaisena osana projektia oleva valmiin tilan vaatimuksenmukaisuuden todentaminen jää kuitenkin tästä raportista puuttumaan. Auditointi tullaan kuitenkin suorittamaan projektin valmistuttua ja dokumentoidaan niin, että kaikki ratkaisut ja materiaalit ovat jälkikäteen luotettavasti todennettavissa.

Rakennusurakat ovat isoja kokonaisuuksia, joissa suunnittelu, tehdyt alkukartoitukset, riskiarvioinnit, materiaalivalinnat sekä toteutusaikaiset asiat, kuten realistinen aikatauluttaminen yhdessä riittävän valvonnan kanssa ovat avainasemassa kokonaishankkeen onnistumisessa. Kaikki virhearvioinnit, väärän tai puutteellisen tiedon pohjalta tehdyt väärät valinnat yhdistettynä valvonnan puutteesta tapahtumaan päässeiden asennusvirheiden ja laatupoikkeamien kanssa vaikuttavat pahimmillaan hyvin pitkälle käytön aikaiseen toimintaan rakennuksessa.

Kohdeyrityksen suunnitteluprosessissa ajan käytön lisääminen ja suunnitteluajan pidentäminen, yksiköiden välisen yhteistyön tiivistäminen sekä projektitilojen suunnittelijoiden aikaisempi osallistaminen kiinteistöprojekteihin tuottaisi kustannustehokkaamman lopputuloksen. Lähtötietojen koostaminen tulee olla tärkeämmässä roolissa, jotta kantavuus- ja kosteuden kerääntymisen ongelmat voidaan välttää jo suunnitteluvaiheessa. Kohdeyrityksessä projektit kaipaavat selkeämpää projektinjohtoa, projektijohdolle resurssien osoittamista sekä prosessien selkeää kuvaamista. Hyvin kuvattu prosessi sekä selkeästi toteutettu loppudokumentaatio palvelevat paremmin käytön aikaisia toimintoja sekä huoltoa ja ylläpitoa, sen lisäksi että kyseessä olevan tilan kohdalla niillä osoitetaan viranomaiselle vaatimuksenmukaisuus.

Aikataulullisesti opinnäytetyö eteni lähes suunnitellusti. Suurimmat haasteet tulivat vastaan työelämän ja raportin kirjoittamisen yhdistämisessä. Raportin kirjoittaminen ja etenkin teemoittelu kuitenkin tukivat oppimista ja jäsensivät vaatimusten alkuperää. Prosessina opinnäytetyö kehitti vaatimusdokumenttien käsittelyä, olennaisten kohtien poimimista ja viemistä käytäntöön. Työn luotettavuus on hyvä, sillä opinnäytetyön aiheen kannalta lähteet ovat yksiselitteiset, lainsäädäntö joka määrittää salassa pidettävät asiakirjat ja niiden käsittelyn reunaehdot sekä viranomaisen työkaluksi luotu auditointikriteeristö. Myös tiedon suojaamisen menetelmät on valittu lähteistä, jotka ovat viranomaisten tuottamia tai kansainvälisesti hyväksyttyjä. Kaikki lähdemateriaalit ovat julkisesti saatavissa ja voidaan tarkistaa. Prosessin kuvaus taas on koottu projektin dokumenteista, joiden perusteella todennetaan toteutukset. Työtä voidaan pitää yleistettävänä, sillä samoihin toteutuksiin voidaan päätyä samoja lähdeaineistoja käyttämällä.

Lähteet

Painetut

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio. Jyväskylä: Gummerus.

Puolustusministeriö 2015. Katakri 2015. Kansallinen turvallisuusauditointikriteeristö. Helsinki: Puolustusministeriö.

Suomen Standardisoimisliitto 2017. SFS-EN ISO/IEC 27002:2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohje. Helsinki: Suomen Standardisoimisliitto.

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

Sähköiset

Aho, T. 2010. Tietoaineiston luokittelu. Suojaustasot ja niitä koskevat merkinnät. Viitattu 5.11.2018. https://www.vahtiohje.fi/web/guest/tietoaineistojen-luokittelu

A681/2010. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. Viitattu 8.11.2018

Eduskunta 2018. Lainsäädäntö. Viitattu 7.11.2018, https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/kotimaiset-oikeuslahteet/Sivut/Lainsaadanto.aspx

Finanssiala 2018a. Lukot. Viitattu 8.11.2018. http://www.finanssiala.fi/vahingontorjunta/dokumentit/Lukot.pdf

Finanssiala 2018b. Murtohälytinjärjestelmät. Keskuslaitteet. Viitattu 8.11.2018. http://www.finanssiala.fi/vahingontorjunta/dokumentit/Murtohalytysjarjestelmat_keskuslaitteet.pdf

Finanssiala 2017a. Kameravalvonnan suunnitteluohje. Viitattu 8.11.2018. http://www.finanssiala.fi/vahingontorjunta/dokumentit/Kameravalvonnan_suunnitteluohje_K-menetelma.pdf

Finanssiala 2017b. Kassakaappiohje. Viitattu 8.11.2018. http://www.finanssiala.fi/vahingontorjunta/dokumentit/Kassakaappiohje.pdf

Finanssiala 2017c. Rakenteellinen murtosuojaus III. Viitattu 8.11.2018. http://www.finanssiala.fi/vahingontorjunta/dokumentit/Rakenteellinen%20murtosuojaus%20III.pdf

Kohdeyritys 2018. Tietoa meistä. Viitattu 5.11.2018.

L726/2014. Turvallisuusselvityslaki. Viitattu 8.11.2018. https://www.finlex.fi/fi/laki/ajantasa/2014/20140726?search%5Btype%5D=pika&search%5Bpika%5D=turvallisuusselvityslaki

L379/2011. Pelastuslaki. Viitattu 8.11.2018. https://www.finlex.fi/fi/laki/ajantasa/2011/20110379?search%5Btype%5D=pika&search%5Bpika%5D=pelastuslaki

L132/1999. Maankäyttö- ja rakennuslaki. Viitattu 8.11.2018. https://www.finlex.fi/fi/laki/ajantasa/1999/19990132?search%5Btype%5D=pika&search%5Bpika%5D=maank%C3%A4ytt%C3%B6%20ja%20rakennuslaki

L621/1999. Laki viranomaisen toiminnan julkisuudesta. Viitattu 15.11.2018. https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Suomen standardisoimisliitto 2018. Standardien laadinta. Viitattu 5.11.2018. https://www.sfs.fi/standardien_laadinta

Valtiovarainministeriö 2018. VAHTI. Viitattu 5.11.2018. https://vm.fi/vahti

Valtiovarainministeriö 2013. VAHTI 2/2013. Toimitilojen tietoturvaohje. Viitattu 7.11.2018. https://www.vahtiohje.fi/web/guest/vahti-2/2013

Vilkka, H. 2014. Tutki ja havainnoi. Viitattu 8.11.2018. http://hanna.vilkka.fi/wp-content/uploads/2014/02/Tutki-ja-havainnoi.pdf

Ympäristöministeriö 2018a. Suomen rakennusmääräyskokoelma. Viitattu 8.11.2018. http://www.ym.fi/rakentamismaaraykset

Ympäristöministeriö 2018b. Ympäristöministeriön asetus rakennusten paloturvallisuudesta. Viitattu 15.11.2018. http://www.ym.fi/download/noname/%7BB71FCDF7-A565-4EEB-8F94-BAEA601533CA%7D/132664

Julkaisemattomat

Insinööritoimisto 2018. Rakennustapaselostus. Viitattu 8.11.2018.

Kohdeyritys 2018a. Avainhallintaprosessi. Viitattu 8.11.2018

Kohdeyritys 2018b. Toimitilaturvallisuusohje. Viitattu 8.11.2018.

Kohdeyritys 2018c. Turvallisuusselvitysprosessi. Viitattu 8.11.2018.

Kohdeyritys 2017. Riskikartoitus. Kartoitusraportti. Viitattu 18.11.2018.

Kohdeyritys 2016. Projektitilaturvallisuusohje. Viitattu 8.11.2018.

Rakennusliike 1992. Kiinteistö x rakennustekniset loppukuvat. Viitattu 8.11.2018.

Kuviot

Taulukot

Liitteet

Liite 1: Välitarkastuspöytäkirja, pohja

Aika

Paikka

Tarkastuksen tekijä

1
Tarkastuksen laajuus, tarkastettavat rakenteet ja järjestelmät

2
Asennusten tilanne

3
Tarkastuksen havainnot

Kuvat

4
Huomautukset ja korjaustarpeet

_____
Paikka ja aika, tarkastuksen tekijän allekirjoitus

LIITTEET

JAKELU

TIEDOKSI

Liite 2: Käyttöönottotarkastuspöytäkirja, pohja

Aika

Paikka

Läsnä , puheenjohtaja

, sihteeri

Poissa

1 TARKASTUKSEN AVAUS

2 TARKASTUKSEN KOHDE

Tarkastettavat rakenteet ja järjestelmät

3 TOTEUTUSAIKAISET MUUTOKSET

4 TEKNISET TARKASTUKSET

Asennuspöytäkirjat ja ennakkotarkastusten tarkastuspöytäkirjat

5 LISÄTYÖT

6 TOIMITUSAIKA

7 KÄYTÖNOPASTUS

8 LUOVUTUSDOKUMENTIT

9 PUUTTEIDEN KORJAAMINEN

10 KOEKÄYTTÖAIKAAN SIIRTYMINEN JA VASTAANOTTOTARKASTUS

LIITTEET

JAKELU

TIEDOKSI

Liite 3: Vastaanottotarkastuspöytäkirja, pohja

Aika

Paikka

Läsnä , puheenjohtaja

, sihteeri

Poissa

1 TARKASTUKSEN AVAUS

2 TARKASTUKSESTA SOPIMINEN

3 VASTAANOTTOTARKASTUKSEN KOHDE

4 TOTEUTUSAIKAISET MUUTOKSET

5 TEKNISET TARKASTUKSET

6 LISÄTYÖT

7 TOIMITUSAIKA

8 KÄYTÖNOPASTUS

9 LUOVUTUSDOKUMENTIT

10 PUUTTEIDEN KORJAAMINEN

11 VASTAANOTTO

12 TALOUDELLINEN LOPPUSELVITYS

13 TAKUUAJAN VAKUUS

14 TAKUUAIKA

15 MUUT VAATIMUKSET

LIITTEET

JAKELU

TIEDOKSI