KATAKRI:n soveltaminen yrityksen turvallisuusratkaisuissa

12. Turvallisuusjohdon koulutusohjelma

Tutkielma

Jussi Haikara

Elektrobit

Oulu 12.3.2013

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Tutkielmassa analysoitiin Kansallisen Turvallisuusauditointikriteeristön (KATAKRI) soveltuvuutta yrityksen turvallisuusratkaisujen vaatimuksiksi sekä haettiin ratkaisua selkeän ja yksiselitteisen KATAKRI:n vaatimuksia vastaavan dokumentointimallin määrittelemiseksi.

Dokumentaatiossa päädyttiin KATAKRI:n rakenteen mukaiseen toteutukseen, missä kutakin vaatimusta kohden on vastaava kappale, jossa toteutus on kuvattu. Valitulla rakenteella pyrittiin selkeyteen ja auditointitapahtuman kannalta yksiselitteiseen lopputulokseen.

KATAKRI:n todettiin olevan rakenteeltaan osin itseään toistava. Valitusta dokumentointirakenteesta johtuen samat ongelmat siirtyivät osittain myös turvallisuusdokumentaatioon.

Turvallisuusvaatimuksena KATAKRI kaipaa tiivistämistä ja rakenteen selkiyttämistä. Vaatimukset sinällään ovat pääosin perusteltuja ja tukevat yritysturvallisuutta, joskin joitakin puutteellisesti määriteltyjä kohtiakin tunnistettiin.

Sisältö

1 Johdanto

1.1 Viitekehys

1.1.1 Elektrobit

Elektrobit on langattomia tietoliikenneratkaisuja ja autojen sulautettuja ohjelmistoja tuottava pörssiyhtiö. Liikevaihto oli vuonna 2012 n. 185 M€ (Elektrobit Oyj:n tilinpäätöstiedote vuodelta 2012) . Elektrobitillä on tuotekehitystoimintaa Suomen lisäksi Saksassa ja USA:ssa. Suomessa toiminta on keskittynyt kolmelle paikkakunnalle: Ouluun, Kajaaniin ja Tampereelle. Yhtiön pääkonttori sijaitsee Oulussa.

Osana langattomia tietoliikenneratkaisuja tuottavaa Wireless - liiketoimintasegmenttiään Elektrobit suunnittelee ja toimittaa Suomen Puolustusvoimille tietoliikenneratkaisuja ja – tuotteita. Yhteistyö edellyttää Puolustusvoimien turvallisuusvaatimusten noudattamista henkilöstöhallinnossa, tilaratkaisuissa ja tietojenkäsittelyssä.

1.1.2 KATAKRI

Kansallinen Turvallisuusauditointikriteeristö (KATAKRI) valmistui 20.11.2009 osana hallituksen sisäisen turvallisuuden ohjelman toista vaihetta (STO II). Ohjelman tavoitteena oli luoda viranomaisille ja yrityksille yhteinen turvallisuuskriteeristö yhteisöturvallisuusmenettelyiden yhtenäistämiseksi omavalvonnan ja auditoinnin parantamiseksi. (Rimpi, Saate KATAKRI:iin 1325/50.01.00/2009 FI.PLM.2009-4910)

Kansallinen turvallisuusviranomainen vahvisti KATAKRI:n ottamisen virallisesti käyttöön kansallisen turvallisuusviranomaisen organisaatiossa 5.11.2010 päivätyssä päätöksessään (Murto, Lähete KATAKRI:n käyttöönottoon HELM545-4). Puolustusvoimien viralliseksi auditointikriteeristöksi KATAKRI otettiin täysimääräisenä kesäkuussa 2011

(www.puolustusvoimat.fi/portal/puolustusvoimat.fi, DSA-tehtävät puolustusvoimissa 12.3.2013,

1.2 Tutkimuksen tavoite

Tutkielmassa arvioitiin KATAKRI:n soveltuvuutta yrityksen turvallisuusratkaisujen perustaksi. Tavoitteeksi asetettiin myös Elektrobitin yritysturvallisuuskartoitus päivittäminen samassa yhteydessä KATAKRI:n vaatimalle tasolle. Elektrobitin yritysturvallisuuskartoitusta ei kuitenkaan liitetä osaksi tutkielmaa salassapitosyistä.

Lisäksi tavoitteeksi asetettiin KATAKRI:n vaatimuksiin pohjautuvan kattavan dokumentaatiomallin luominen. Elektrobitin yritysturvallisuuskartoituksen tulisi noudattaa tätä mallia sisällöltään ja rakenteeltaan. Tavoitteena oli määritellä sellainen dokumenttimalli, että se on myös muiden yritysten hyödynnettävissä.

1.3 Tutkimusmenetelmä

Tutkimusmenetelmänä oli KATAKRI:n läpikäynti ja vertailu Elektrobitin turvallisuusdokumentaatioon sekä auditointitapahtumista saatuihin kokemuksiin. Tutkimus tehtiin olemassa olevaan materiaaliin pohjautuen.

2 Yritysturvallisuuskartoituksen rakenne

2.1 Rakenteelle asetetut tavoitteet

Tutkimuksen yhdeksi tavoitteeksi asetettiin KATAKRI:n vaatimuksiin vastaavan yritysturvallisuuskartoitusmallin määritteleminen. Tavoitteena oli luoda selkeä ja kaikki oleelliset turvallisuustyöhön liittyvät aihealueet kattava yhtenäinen dokumentaatiomalli. Kaikkea turvallisuusdokumentaatiota ei ole järkevää koota yhteen dokumenttiin, mutta tavoitteena oli, että yritysturvallisuuskartoitus on runko, joka sisältää yhteenvedon ja tarvittaessa viitteet kattavampaan dokumentaatioon.

Toinen näkökulma dokumentaation sisällölle ja rakenteelle oli turvallisuusratkaisuja auditoivan viranomaisen näkökulma. Auditointiin liittyen viranomaiselle toimitetaan KATAKRI:n mukainen yhteenveto turvallisuusdokumentaatiosta ennen varsinaista auditointitapahtumaa. Yritysturvallisuuskartoituksen rakenne ja sisältö määriteltiin sellaiseksi, että se voidaan sellaisenaan antaa auditoijalle yhteenvedoksi, jolloin erillistä yhteenvetoa ei tarvittaisi.

Lisäksi yritysturvallisuuskartoituksesta haluttiin tehdä rakenteeltaan KATAKRI:n mukainen, samaa kappalejakoa noudattava selkeä kokonaisuus, jotta itse auditointitapahtuma on helppo toteuttaa ja vastaukset jokaiseen KATAKRI:n vaatimukseen on varmasti etukäteen mietitty, toteutettu ja dokumentoitu. Tällä tavoin auditointitapahtumasta saadaan molempien osapuolten kannalta selkeä ja huolella etukäteen valmisteltu ilman merkittävää ylimääräistä lisätyötä.

Tärkein näkökulma on kuitenkin se, että KATAKRI:n vaatimuksiin vastaavalla dokumentaatiolla taataan, että turvallisuusvaatimukset on käyty kohta kohdalta lävitse ja niiden toteutus on mietitty ja toteutettu asianmukaisesti.

Tämän myötä yrityksen toiminnassa on huomioitu turvallisuuden eri osa-alueet ja yritysturvallisuus on vaatimusten mukaisella tasolla.

2.2 Valittu rakenne

Dokumentaation rakenteessa päädyttiin yksi yhteen KATAKRI:n kappalejaon mukaiseen toteutukseen. Kutakin KATAKRI:n vaatimusta kohden yritysturvallisuuskartoituksessa on kappale, missä kyseistä vaatimusta vastaava toteutus on kuvattu joko kokonaisuudessaan tai yhteenvetona erillisestä dokumentaatiosta.

Pääotsaketasolla dokumentaatio jakautuu viiteen kappaleeseen:

Taulukko 1 Yritysturvallisuuskartoituksen pääotsikot

1. TIEDOT YRITYKSESTÄ
2. HALLINNOLLINEN TURVALLISUUS
3. HENKILÖSTÖTURVALLISUUS
4. FYYSINEN TURVALLISUUS
5. TIETOTURVALLISUUS

Ensimmäinen kappale sisältää yrityksen tiedot sekä määrittelyn, mille suojaustasolle yrityksen turvallisuusmenettelyt on tässä dokumentaatiossa kuvattu.

Loput neljä kappaletta noudattavat KATAKRI:n pääotsaketason jaottelua.

Pääotsakkeiden sisällä yritysturvallisuuskartoituksen jaottelu noudattaa KATAKRI:n rakennetta. Turvallisuuden osa-alueet on jaettu kappaleiksi ja alikappaleiksi seuraavasti

Hallinnollisen turvallisuuden osa-alue sisältää yhdeksän osa-aluetta, jotka jakautuvat yhteensä 58 alikappaleeseen.

Taulukko 2 Hallinnollisen turvallisuuden kappalejako

2. HALLINNOLLINEN TURVALLISUUS
2.1 Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, osa-alue A100
2.2 Turvallisuuden vuotuinen toimintaohjelma, osa-alue A200
2.3 Turvallisuuden tavoitteiden määrittely, osa-alue A300
2.4 Riskien tunnistus, arviointi ja kontrollit, osa-alue A400

2.5 Turvallisuusorganisaatio ja vastuut, osa-alue A500

2.6 Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet, osa-alue A600

2.7 Turvallisuusdokumentaatio ja sen hallinta, osa-alue A700

2.8 Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen, osa-alue A800

2.9 Raportointi ja johdon katselmukset, osa-alue A900

Henkilöstöturvallisuuden osa-alue sisältää kuusi osa-aluetta, jotka jakautuvat yhteensä 30 alikappaleeseen.

Taulukko 3 Henkilöstöturvallisuuden kappalejako

3. HENKILÖSTÖTURVALLISUUS

3.1 Tekninen kriteeristö, osa-alue P100

3.2 Riittävän osaamisen varmistaminen, osa-alue P200

3.3 Henkilön muu soveltuvuus tehtävään, osa-alue P300

3.4 Rekrytointipäätöksen jälkeiset toimet, osa-alue P400

3.5 Toimenpiteet työsuhteen solmimisen yhteydessä, osa-alue P500

3.6 Toimenpiteet työsuhteen aikana, osa-alue P600

Henkilöstöturvallisuuden osa-alue sisältää kolme osa-aluetta, jotka jakautuvat yhteensä 31 alikappaleeseen.

Taulukko 4 Fyysisen turvallisuuden kappalejako

4. *FYYSINEN TURVALLISUUS*

4.1 Alueen turvallisuus, osa-alue F100

4.2 Rakenteellinen turvallisuus, osa-alue F200

4.3 Turvallisuustekniset järjestelmät, osa-alue F300

Henkilöstöturvallisuuden osa-alue sisältää neljä osa-aluetta, jotka jakautuvat yhteensä 41 alikappaleeseen.

Taulukko 5 Tietoturvallisuuden kappalejako

5. TIETOTURVALLISUUS

5.1 Tietoliikenneturvallisuus, osa-alue I400

5.2 Tietojärjestelmäturvallisuus, osa-alue I500

5.3 Tietoaineistoturvallisuus, osa-alue I600

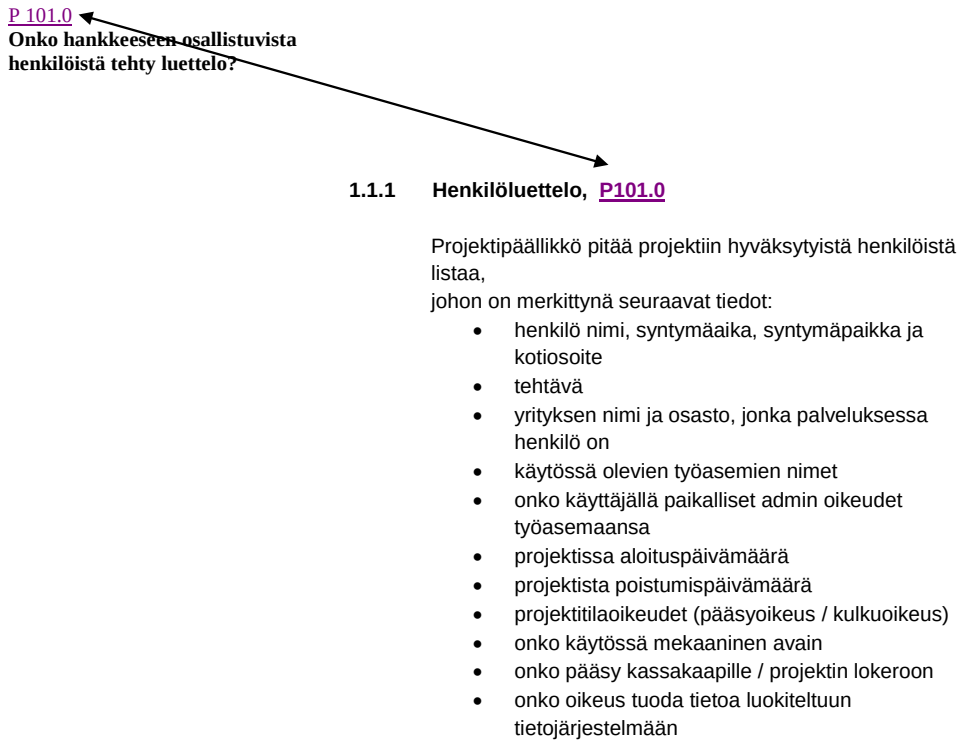
5.4 Käyttöturvallisuus, osa-alue I700

2.3 Dokumenttien välinen linkitys

Yritysturvallisuuskartoituksen kappalenumerointi noudattaa KATAKRI:n kappalenumerointia osa-alueiden otsikoinnista lähtien. Numerointi on mukana suoraan kappaleiden nimissä: Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, osa-alue **A100**

Osa-alueet on jaettu KATAKRI:n kysymyksiä vastaaviin kappaleisiin, joihin on myös tuotu mukaan KATAKRI:n numerointi: 2.1.1 Yrityksen turvallisuuspolitiikka, **A101.0**

Vaatimukset on linkitetty toisiinsa hyperlinkein yritysturvallisuuskartoituksen ja KATAKRI:n välillä. KATAKRI:n vaatimusnumeroa klikkaamalla avautuu yritysturvallisuuskartoituksen vastaava kappale sisältöineen. Ja päinvastoin, yritysturvallisuuskartoituksen kappalenumeroa klikkaamalla avautuu vastaava KATAKRI:n vaatimus sisältöineen.



Kuva 1 Dokumenttien välinen linkitys

Dokumenttien välinen linkitys vaatii toimiakseen, että dokumentit tallennetaan samaan hakemistoon. Molempien dokumenttien tallennusformaatti on Microsoft Word Document.

2.4 Vaatimustasot

Yritysturvallisuuskartoituksen rakenteessa ei ole otettu suoraan kantaa viranomaisvaatimuksen tasoon (Perustaso, Korotettu taso, Korkea taso). Alkuvaiheessa yhtenä ajatuksena oli, että kukin taso kuvataan jokaisen vaatimuksen osalta erikseen, mutta työn kuluessa tämä ajatus osoittautui toimimattomaksi, koska isossa osaa vaatimuksia tasoissa ei ole eroja.

Dokumentissa kuvattu korkein vaatimustaso on määritelty dokumentin ensimmäisessä kappaleessa. Mahdolliset vaatimusten sisäiset, suojaustasoista johtuvat vaatimuserot, on eroteltu kappaleiden sisällä väliotsikoilla ”Suojaustaso x”.

3 KATAKRI:n osa-alueet

Tässä kappaleessa käydään lävitse KATAKRI:n ja sitä vastaavan yritysturvallisuuskartoituksen osa-alueet ja arvioidaan lyhyesti vaatimusten soveltuvuutta yritysturvallisuuden kehittämisen ja toteutuksen näkökulmasta. Arvioinneissa on tuotu esille Elektrobitin näkökulma vaatimuksiin ja tapa toteuttaa yritysturvallisuuden dokumentaatio.

3.1 Hallinnollinen turvallisuus

Hallinnollinen turvallisuus tuli erillisenä vaatimusalueena mukaan KATAKRI:n myötä. Aiemmassa Puolustusviranomaisen vaatimuskokonaisuudessa ja sen mukaisessa yritysturvallisuuskartoituksessa vastaavat asiat oli käsitelty huomattavasti suppeammin.

Hallinnollinen turvallisuus on kokonaisuutena raskas ja osittain itseään toistava. Pääotsakkeet ovat aiheina perusteltuja ja kokonaisturvallisuuden kannalta oleellisia asioita, mutta osan aiheista olisi voinut yhdistää ja saada sillä tavoin kokonaisuuden tiiviimmäksi ja helpommaksi käsitellä.

Aihepiirien pilkkominen kysymyksiksi ei ole täysin onnistunut, mistä syntyy vaikutelma, että samoja asioita kysytään useampaan kertaan hieman eri sanoin.

3.1.1 Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt

Turvallisuuspolitiikan osa-alue sisältää yhteensä yhdeksän kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 6 Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, kappalejako

2.1.1 Yrityksen turvallisuuspolitiikka, A101.0

2.1.2 Turvallisuuspolitiikan kattavuus, A102.0

2.1.3 Turvallisuuspolitiikan taso, A103.0

2.1.4 Turvallisuuspolitiikan mukainen toiminta, A104.0

2.1.5 Yleiset lainsäädännön asettamat velvoitteet, A105.0

2.1.6 Toiminnan lakisääteiset vaatimukset, A105.1

2.1.7 Turvallisuuspolitiikan tiedottaminen, A106.0

2.1.8 Henkilöstön sitoutuminen turvallisuuden parantamiseen, A107.0

2.1.9 Organisaation keskeiset turvallisuustavoitteet, A108.0

Turvallisuuspolitiikasta on yritysturvallisuuskartoituksessa lyhyt kuvaus. Laajempi kuvaus on erillisessä dokumentissa, joka kattaa kaikki Elektrobitin liiketoiminnot, ei pelkästään viranomaiskenttää. Tällä tavoin jaettuna turvallisuuspolitiikka voidaan jakaa koko henkilöstölle omana dokumentaationaan, mikä on edellytyksenä ohjeistuksen ja koulutuksen onnistumiselle.

Turvallisuuspolitiikka on aihepiirinä olennainen osa hallinnollista turvallisuutta ja turvallisuustyötä. Politiikassa kuvataan yleiset periaatteet yritysturvallisuuden kehittämiselle ja se antaa pohjan turvallisuustyölle. Olennaista on, että turvallisuuspolitiikka jalkautetaan koko organisaatioon ja kaikki tasot johdosta alkaen toimivat turvallisuuspolitiikan mukaisesti.

3.1.2 Turvallisuuden vuotuinen toimintaohjelma

Turvallisuuden vuotuinen toimintaohjelma sisältää yhteensä neljä kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti

Taulukko 7 Turvallisuuden vuotuinen toimintaohjelma, kappalejako

2.2.1 Turvallisuuden toimintaohjelma, A201.0

2.2.2 Menetelmät, vastuut ja aikataulut, A202.0

2.2.3 Toimintaohjelman ajantasaisuus, A203.0

2.2.4 Tietoturvallisuuden johtaminen, A204.0

Turvallisuuden vuotuisen toimintaohjelman suunnittelu ja toteutus on Elektrobitillä keskitetty turvallisuusasioita koordinoivan ryhmän, Security Boardin, tehtäväksi. Security Boardiin on koottu asiantuntijat yritysturvallisuuden eri osa-alueilta. Security Board kokoontuu säännöllisesti ja käsittelee vakioaiheiden lisäksi vuotuisen toimintaohjelman mukaisia erityisaiheita.

Vaatimuksena toimintaohjelma on perusteltu ja täydentää hallinnollisen turvallisuuden kokonaisuutta. Toimintaohjelma edellyttää toimiakseen, että siitä generoituu käytännön toimia ja aktiviteetteja, joiden toteutus aikataulutetaan ja toteutusta seurataan.

3.1.3 Turvallisuuden tavoitteiden määrittely

Turvallisuuden tavoitteiden määrittely sisältää yhteensä kuusi kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti

Taulukko 8 Turvallisuuden tavoitteiden määrittely, kappalejako

2.3.1 Turvallisuuspolitiikan liiketoiminnalliset perusteet, A301.0
2.3.2 Turvallisuustavoitteet organisaation eri tasoilla, A302.0
2.3.3 Turvallisuustavoitteiden mitattavuus, A303.0
2.3.4 Turvallisuustavoitteiden aikataulutus, A304.0
2.3.5 Turvallisuustavoitteiden sisältö, A305.0
2.3.6 Suojattavan tiedon käsittely-ympäristö, A306.0

Turvallisuuden tavoitteiden määrittely on KATAKRI:ssa erotettu omaksi kappaleekseen. Aihepiirinä liittyy läheisesti edelliseen kappaleeseen. Kokonaisuus toimisi paremmin, jos nämä kaksi kappaletta olisi yhdistetty tiiviimmäksi kokonaisuudeksi.

Tietotekniikkaan liittyvä kysymys A306.0 on kappaleen muusta sisällöstä irrallinen, eikä suoraan liity otsikon aiheeseen. Toimisi paremmin, jos tämä kysymys olisi osa Tietoturvallisuus-kappaletta.

3.1.4 Riskien tunnistus, arviointi ja kontrollit

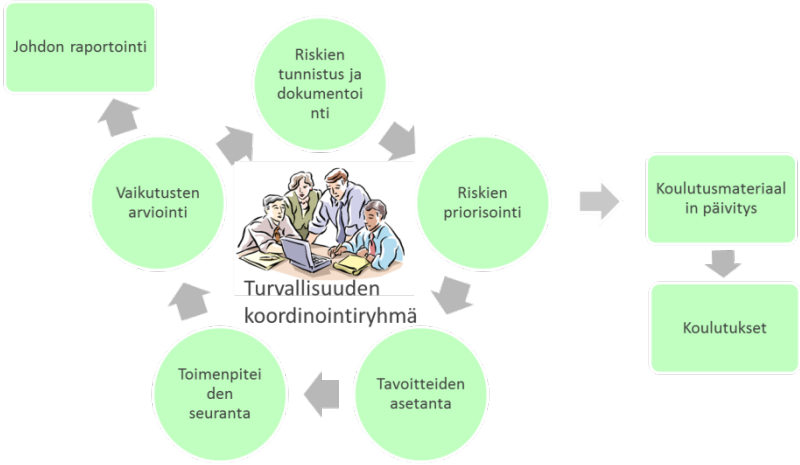
Riskien tunnistus, arviointi ja kontrollit – osa-alue sisältää yhteensä 12 kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti

Taulukko 9 Riskien tunnistus, arviointi ja kontrollit, kappalejako

2.4.1 Riskien arviointimenetelmät, A401.0
2.4.2 Suojattavien kohteiden tunnistus, A401.1
2.4.3 Suojattaviin kohteisiin kohdistuvien riskien arviointi, A401.2
2.4.4 Riskiarvioiden kattavuus, A402.0
2.4.5 Riskiarvioiden dokumentointi ja seuranta, A403.0
2.4.6 Riskiarvioiden vaikutus turvallisuustoiminnan tavoitteisiin, A404.0
2.4.7 Riskien priorisointi, A405.0
2.4.8 Riskiarvioiden vaikutus turvallisuuskoulutuksiin, A406.0
2.4.9 Riskiarvioiden perusteella tehtyjen toimenpiteiden tehokkuus, A407.0
2.4.10 Tietoturvallisuuden arviointi, A408.0
2.4.11 Tietoturvallisuuden huomiointi alihankinnassa, A409.0
2.4.12 Toiminta tietoturvapoikkeamatilanteissa, A410.0

Riskienhallinta on aihepiirinä tärkeä ja koko turvallisuustyön perusta. On perusteltua käsitellä riskienhallintaa omana kappaleenaan, mutta toisaalta toiminta on vahvasti sidoksissa turvallisuuden vuotuiseen toimintaohjelmaan.

Elektrobitillä riskienhallinta on osa Security Boardin toimintaa ja osa vuotuista toimintaohjelmaa. Riskienhallintaa koordinoidaan seuraavassa kuvassa esitetyn prosessin mukaisesti.



Kuva 2 Riskienhallinnan vuotuinen prosessi

Tietoturvallisuuteen ja tietoturvapoikkeamiin liittyvät KATAKRI:n kysymykset, A408.0, A409.0 ja A410.0, ovat osin aihepiiristä irrallisia ja soveltuisivat paremmin osaksi kappaletta Tietoturvallisuus.

3.1.5 Turvallisuusorganisaatio ja vastuut

Turvallisuusorganisaatio ja vastuut – osa-alue sisältää yhteensä seitsemän kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti

Taulukko 10 Turvallisuusorganisaatio ja vastuut, kappalejako

2.5.1 Turvallisuustyön vastuiden määrittely, A501.0
2.5.2 Johdon tuki tietoturvallisuudelle, A501.1
2.5.3 Turvallisuusorganisaation roolien tiedottaminen, A502.0
2.5.4 Turvallisuustyön resursointi, A503.0
2.5.5 Turvallisuustoiminnan johtaminen, A504.0
2.5.6 Turvallisuusjohdon valtuutus, A505.0
2.5.7 Johdon sitoutuminen turvallisuustavoitteisiin, A506.0

Vastuumäärittelyt on pitkälti kuvattu yrityksen turvallisuuspolitiikassa, jota käsitellään Hallinnollisen turvallisuuden ensimmäisessä kappaleessa. Vastuiden eriyttäminen omaksi kappaleeseen aiheuttaa yritysturvallisuuskartoitukseen toistoa ja viittauksia muihin kappaleisiin.

3.1.6 Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet

Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet – osa-alue sisältää yhteensä kahdeksan kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti

Taulukko 11 Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet, kappalejako

2.6.1 *Jatkuvuudenhallintamenettely, A601.0*
2.6.2 Vastuuhenkilöt poikkeustilanteissa, A602.0
2.6.3 Poikkeustilanteiden vaikutusten ennaltaehkäisy, A603.0
2.6.4 Turvallisuuspoikkeamien havainnointi ja korjaavat toimenpiteet, A604.0
2.6.5 Suojaavien ja korjaavien toimenpiteiden arviointi, A605.0

2.6.6 Korjaavista toimenpiteistä aiheutuvat riskit, A606.0

2.6.7 Toimenpiteiden vaikutusten analysointi, A607.0

2.6.8 Tietojenkäsittely-ympäristön muutosten hallinta, A608.0

Jatkuvuudenhallinta on tärkeä osa turvallisuustoimintaa ja on perusteltua käsitellä sitä omassa kappaleessaan. Toisaalta jatkuvuudenhallinta ja riskienhallinta liittyvät läheisesti toisiinsa, mikä puoltaisi myös näiden kahden kappaleen yhdistämistä. Erillisinä kappaleina nämä aihealueet aikaansaavat ristiviittauksia yritysturvallisuuskartoituksen kappaleiden välillä.

Elektrobitin jatkuvuudenhallintadokumentaatio koostuu erillisistä dokumenteista: jatkuvuudenhallintasuunnitelma (Business Continuity Plan) ja erilliset toipumissuunnitelmat (Disaster Recovery Plans). Yritysturvallisuuskartoituksessa aihealueet ja dokumentaatio on kuvattu lyhyesti, varsinaisen sisällön osalta viitataan näihin erillisiin dokumentteihin.

Dokumentaation jakaminen erillisiin jatkuvuudenhallinta- ja toipumissuunnitelmiin on perusteltua, jotta dokumentaatiota voidaan käyttää omina kokonaisuuksinaan koulutuksissa ja poikkeustilanteissa sekä ylläpitää joustavasti.

3.1.7 Turvallisuusdokumentaatio ja sen hallinta

Turvallisuusdokumentaatio ja sen hallinta – osa-alue sisältää yhteensä neljä kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti

Taulukko 12 Turvallisuusdokumentaatio ja sen hallinta, kappalejako

2.7.1 Turvallisuusohjeistuksen ja poikkeamien dokumentointi, A701.0

2.7.2 Turvallisuustavoitteiden saavuttamisen taso, A702.0

2.7.3 Koulutusrekisterit, A703.0

2.7.4 Turvallisuuskoulutuksen taso, A704.0

Turvallisuusdokumentaatiota käsitellään myös osana aiempia Hallinnollisen turvallisuuden kappaleita, näiltä osin kappaleet olisi voinut yhdistää. Eriyttämisen seurauksena aiheutuu toistoa ja ristiviittauksia.

Koulutusrekisterit on käsitelty osana tätä kappaletta, vaikka toisaalta koulutuksesta on oma kappaleensa hallinnollisen turvallisuuden alla.

3.1.8 Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen

Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen – osa-alue sisältää yhteensä kahdeksan kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti

Taulukko 13 Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen, kappalejako

2.8.1 Henkilöstön tietoisuus turvallisuusvaatimuksista, A801.0
2.8.2 Henkilöstön tietoisuus turvallisuusriskeistä, A802.0
2.8.3 Henkilöstön toiminta poikkeamatilanteissa, A803.0
2.8.4 Tietoturvaohjeiden noudattamisen valvonta, A803.1
2.8.5 Turvallisuuskoulutuksen tason arviointi, A804.0
2.8.6 Turvallisuuskoulutuksen tason varmistaminen, A805.0
2.8.7 Ohjeistus, koulutus ja tiedottaminen, A806.0
2.8.8 Tietojenkäsittelyn säännöt, A807.0

Koulutuksia ja koulutusrekistereitä käsitellään edellisessä kappaleessa sekä myös osana Henkilöstöturvallisuutta. Tämän aihealueen keskittäminen yhteen kappaleeseen parantaisi kokonaisuutta ja vähentäisi toistoa.

Koulutus ja sen eri tasot on kuvattu Elektrobitin yritysturvallisuuskartoituksessa. Turvallisuuteen liittyviä koulutuksia järjestetään usealla tasolla yleisistä koko henkilökuntaa koskevista turvallisuusperehdytyksistä hankekohtaisiin yksityiskohtaisiin koulutuksiin.

3.1.9 Raportointi ja johdon katselmukset

Raportointi ja johdon katselmukset – osa-alue sisältää yhteensä viisi kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti

Taulukko 14 Raportointi ja johdon katselmukset, kappalejako

2.9.1 Turvallisuusjohdon raportointikanava, A901.0
2.9.2 Turvallisuusasioiden raportointi johtoryhmään, A902.0
2.9.3 Turvallisuustoimien mitattavuus johdon katselmoinneissa, A903.0
2.9.4 Seurantatarkastusten dokumentointi, A904.0
2.9.5 Johdon katselmusten vaikutukset toiminnan kehittämiseen, A905.0

Raportointiin ja turvallisuusjohtoon liittyvät asiat on pitkälti kuvattu edellisissä kappaleissa. Käsittely KATAKRI:n mukaisesti omana kappaleenaan aiheuttaa dokumentaatioon päällekkäisyyttä tai ristiviittauksia.

3.2 Henkilöstöturvallisuus

Henkilöstöturvallisuus on laajempi kokonaisuus kuin KATAKRI:a edeltäneissä DSA-vaatimuksissa. Uusina elementteinä kappaleeseen on lisätty henkilöstön rekrytointiin, perehdytykseen ja yleensä työsuhteeseen liittyviä vaatimuksia. Näiden aihealueiden myötä Henkilöstöturvallisuus kattaa koko työsuhteen, eikä pelkästään viranomaishankkeisiin liittyvän henkilöstön käsittelyn.

3.2.1 Tekninen kriteeristö

Tekninen kriteeristö – osa-alue sisältää yhteensä viisi kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti

Taulukko 15 Tekninen kriteeristö, kappalejako

3.1.1 Henkilöluettelo, P101.0
3.1.2 Muutokset henkilöstössä, P102.0
3.1.3 Turvallisuuskoulutus, P103.0
3.1.4 Vierailut tiloissa, P104.0
3.1.5 Rekrytointi, P105.0

Tekninen kriteeristö kuvaa ne toimenpiteet, mitä henkilöstöön kohdennetaan viranomaishankkeita tehtäessä. Kappaleessa on määritelty, miten henkilöitä hyväksytään hankkeisiin. mitä tietoja henkilöistä ylläpidetään, miten henkilömuutokset käsitellään ja miten hankkeeseen hyväksymättömiä henkilöitä käsitellään.

Turvallisuuskoulutus on myös tämän otsakkeen alla yhtenä vaatimuksena. Turvallisuuskoulutusta käsitellään monipuolisemmin osana Hallinnollista turvallisuutta. Toiston välttämiseksi ja kokonaisuuden selkiyttämiseksi tämä aihealue toimisi paremmin yhdistettynä yhteen kappaleeseen.

3.2.2 Riittävän osaamisen varmistaminen

Riittävän osaamisen varmistaminen – osa-alue sisältää yhteensä kolme kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 16 Riittävän osaamisen varmistaminen, kappalejako

3.2.1 Dokumentaatio, P201.0
3.2.2 Tietojen tarkistaminen, P202.0
3.2.3 Osaamisen tarkistaminen, P203.0

Kappale sisältää yleisiä vaatimuksia henkilöstön rekrytointiin. Elektrobitin osalta toiminta on kuvattu tarkemmin erillisessä ohjeistuksessa, johon tässä ja tulevissa kappaleissa viitataan. Samat periaatteet pätevät kaikkeen rekrytointiin riippumatta siitä, mitä hankkeita henkilö tulee tekemään.

Henkilöstön osaaminen varmistetaan todistuksista, tarkistamalla edellisistä työpaikoista ja oppilaitoksista sekä kysymällä haastattelutilanteessa.

3.2.3 Henkilön muu soveltuvuus tehtävään

Henkilön muu soveltuvuus tehtävään–osa-alue sisältää yhteensä kolme kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 17 Riittävän osaamisen varmistaminen, kappalejako

3.3.1 Yrityksen arvojen mukainen toiminta, P301.0
3.3.2 Huumausainetesti, P302.0
3.3.3 Soveltuvuusarviointi, P303.0

Soveltuvuusarviointi on sisällöltään jatkoa edelliseen kappaleeseen ja olisi voitu yhdistää yhteen. Toiminta näiden osalta on kuvattu tarkemmin erillisessä dokumentaatiossa.

3.2.4 Rekrytointipäätöksen jälkeiset toimet

Rekrytointipäätöksen jälkeiset toimet – osa-alue sisältää yhteensä kahdeksan kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 18 Rekrytointipäätöksen jälkeiset toimet, kappalejako

3.4.1 Salassapito- ja vaitiolositoumus, P401.0

3.4.2 Koeaika, P402.0
3.4.3 Vastuut ja yrityskytkennät, P403.0
3.4.4 Suppea turvallisuusselvitys, P404.0
3.4.5 Perusmuotoinen turvallisuusselvitys, P405.0
3.4.6 Luottotietojen tarkistus, P406.0
3.4.7 Tehtäväkohtaiset salassapito- ja vaitiolositoumukset, P407.0
3.4.8 Avainhenkilöriippuvuus, P408.0

Kappale sisältää yleiseen työsuhteeseen liittyviä kysymyksiä ja vaatimuksia, kuten vaitiolositoumus ja koeaika. Lisäksi kappaleessa on viranomaishankkeisiin liittyviä vaatimuksia, kuten tehtäväkohtaiset salassapitosopimukset ja taustantarkistukset.

Yleiset toimet ja periaatteet on Elektrobitillä kuvattu erillisessä dokumentaatiossa, mihin yritysturvallisuuskartoituksesta viitataan. Viranomaishankkeita koskevat vaatimukset on kuvattu suoraan yritysturvallisuuskartoituksessa. Henkilöstöturvallisuuden osalta rakenne olisi toimivampi, jos yleiset toimet ja viranomaishankkeita koskevat toimet olisi jaoteltu omiin osakokonaisuuksiinsa.

3.2.5 Toimenpiteet työsuhteen solmimisen yhteydessä

Toimenpiteet työsuhteen solmimisen yhteydessä – osa-alue sisältää yhteensä viisi kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 19 Toimenpiteet työsuhteen solmimisen yhteydessä, kappalejako

3.5.1 Työntekijän vastuut, P501.0
3.5.2 Perehdytys turvallisuusmääräyksiin, P502.0
3.5.3 Muu perehdytys, P503.0
3.5.4 Tietoturvakoulutus, P504.0
3.5.5 Oikeuksien myöntäminen, P505.0

Kappaleessa listatut toimenpiteet työsuhteen solmimisen yhteydessä ovat pitkälti turvallisuuteen liittyviä. Perehdytykseen ja koulutukseen liittyviä vaatimuksia on esitetty myös osana Hallinnollista turvallisuutta sekä osana aiempia Henkilöstöturvallisuuden kappaleita.

3.2.6 Toimenpiteet työsuhteen aikana

Toimenpiteet työsuhteen aikana – osa-alue sisältää yhteensä kuusi kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 20 Toimenpiteet työsuhteen aikana, kappalejako

3.6.1 Sijaisuusjärjestelyt, P601.0
3.6.2 Työtyytyväisyys, P602.0
3.6.3 Työssä jaksaminen, P603.0
3.6.4 Poikkeava käyttäytyminen, P604.0
3.6.5 Työsuhteen päättäminen, P605.0
3.6.6 Vierailukäytäntö, P606.0

Kappale sisältää kysymyksiä henkilöstön työtyytyväisyydestä, työssä jaksamisesta ja poikkeamatilanteisiin varautumisesta. Kappaleen sisältö menee osittain päällekkäin aiempien kappaleiden kanssa.

Vierailukäytäntö on kappaleen aihepiiristä irrallinen asia ja on käsitelty tarkemmin kappaleessa Henkilöstöturvallisuus – Tekninen kriteeristö

3.3 Fyysinen turvallisuus

Fyysisen turvallisuuden kappale on KATAKRI:n osa-alueista selkein. Vaatimukset ovat suurelta osin teknisiä vaatimuksia tilojen ja toimintaympäristön rakentamiseksi. Kappale sisältää jonkin verran toistoa, mutta ei siinä määrin kuin kaksi edellistä kappaletta.

Joiltakin osin tekniset vaatimukset voisivat olla vielä selkeämpiä ja yksiselitteisempiä. Etenkin vanhoja kiinteistöjä vahvistettaessa vaatimukset aiheuttava tulkintaa ja ovat myös riippuvaisia auditoijan mielipiteestä ja suojattavan kohteen luonteesta.

3.3.1 Alueen turvallisuus

Alueen valvonta – osa-alue sisältää yhteensä neljä kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 21 Alueen valvonta, kappalejako

4.1.1 Pysäköinti, F101.0

4.1.2 Lastaus- ja purkualueet, F102.0

4.1.3 Kiinteistön alueella liikkuminen, F103.0

4.1.4 Alueen videovalvonta, F104.0

Alueen turvallisuuteen liittyvät vaatimukset ovat selkeitä. Vaatimusten toteutuksessa jätetään myös sijaa harkinnalle riippuen suojattavasta kohteesta.

Elektrobitin osalta fyysinen turvallisuus on pitkälti toteutettu kiinteistön rakenteellisilla ratkaisuilla ja teknisellä valvonnalla. Toiminnan luonne ei edellytä erityisratkaisuja alueen osalta.

3.3.2 Rakenteellinen turvallisuus

Rakenteellinen turvallisuus – osa-alue sisältää yhteensä 21 kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 22 Rakenteellinen turvallisuus, kappalejako

4.2.1 Rakenteet, F201.0

4.2.2 Ikkunat, F202.0

4.2.3 Kattoikkunat, F203.0

4.2.4 Aukot seinärakenteissa, F204.0

4.2.5 Ovet, F205.0

4.2.6 Halliovet, F206.0

4.2.7 Tilojen äänieristys, F207.0

4.2.8 Kassakaapit ja holvit, F208.0

4.2.9 Pääsyoikeuksien myöntäminen, F209.0

4.2.10 Pääsyoikeuksien hallinta, F209.1

4.2.11 Vierailut tiloissa, F209.2

4.2.12 Tilojen lukitus, F210.0

4.2.13 Avainten hallinta, F211.0

4.2.14 Avainten käyttö, F212.0

4.2.15 Yleisavainten käyttö, F213.0

4.2.16 Vartiointi- ja huoltohenkilöiden kulkuoikeudet, F214.0

4.2.17 Tilojen huoltotoimenpiteet, F215.0

4.2.18 Laitetilojen huolto ja siivous, F216.0

4.2.19 Hajasäteilyyn varautuminen, F217.0

4.2.20 LVIS-järjestelyt, F218.0

4.2.21 Näyttöpäätteiden suojaus, F219.0

Rakenteellinen turvallisuus ja erityisesti seinä- lattia- ja kattorakenteiden kuvaus on Fyysisen turvallisuuden osa-alueista epäselvimmin määritelty ja on aiheuttanut Elektrobitillä eniten keskustelua ja lisämäärittelyn tarvetta tilojen vahventamisessa. Rakenteellisia puutteita on osittain korvattu teknisen valvonnan lisäämisellä. KATAKRI ei suoraan anna tähän ohjeistusta, mistä johtuen kirjaimellinen tulkinta voi aiheuttaa mittaviakin rakenteellisia muutoksia.

Esimerkiksi Perustason määritelmä: ”Kuoren rakenne normaalia toimistorakennetta” jättää sijaa tulkinnoille. Mikä on normaali toimistorakenne? Vaatimus voisi olla parempi esimerkiksi muodossa: ”Ei erityisvaatimuksia”.

Korkean tason ja Korotetun tason määritelmä: ” Tilan seinät, katto ja lattia on oltava betonia, terästä, tiiltä tai vahvaa puuta” on epäselvä ja vaikea todentaa erityisesti vanhoissa kohteissa. Betonin, teräksen ja tiilen vahvuutta ei ole määritelty. Samoin vaatimus ”vahva puu” on epäselvä.

Etenkin vanhojen toimistorakenteiden vahventamisessa epämääräiset rakennevaatimukset aiheuttava tulkintaa. Uudiskohteen toteuttamisessa selkeintä olisi toteuttaa rakenteet vahvoina teräsbetonirakenteina.

Rakenteellinen turvallisuus sisältää myös selkeitä vaatimuksia, kuten ikkunat, kattoikkunat, ovet, ja aukot seinärakenteissa. Näiden osalta ei synny tarvetta tulkintaan.

Rakenteellisen turvallisuuden alla on listattu myös joukko vaatimuksia liittyen turvallisuuden prosesseihin, kuten avaintenhallinta ja pääsyoikeuksien hallinta. Vaatimukset ovat turvallisuustyön kannalta oleellisia, mutta olisi selkeämpää erotella nämä omaksi kappaleekseen erilleen Rakenteellisesta turvallisuudesta.

Kappaleessa on myös joitakin aiempien kappaleiden kanssa päällekkäin meneviä vaatimuksia, kuten tiloissa vierailut. Samaa aihetta käsitellään Henkilöstöturvallisuuden osa-alueessa kahdessakin eri kappaleessa.

3.3.3 Turvallisuustekniset järjestelmät

Turvallisuustekniset järjestelmät – osa-alue sisältää yhteensä kahdeksan kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 23 Turvallisuustekniset järjestelmät, kappalejako

4.3.1 Rikosilmoitinjärjestelmä, F301.0
4.3.2 Kulunvalvontajärjestelmä, F302.0
4.3.3 Tilojen kameravalvonta, F303.0
4.3.4 Palvelintilojen kameravalvonta, F304.0
4.3.5 Rikosilmoitinjärjestelmän toimintakunnon valvonta, F305.0
4.3.6 Kulunvalvontajärjestelmän hallinnointi, F306.0
4.3.7 Rikosilmoitinjärjestelmän hallinnointi, F307.0
4.3.8 LVI-automaation hallinnointi, F308.0

Turvallisuustekniset järjestelmät on osa-alueena selkeä. Kappale sisältää vaatimuksia järjestelmien toteutukseen ja hallinnointiin. Vaatimukset ovat pääosin toteutettavissa ja todennettavissa ilman tulkintaa.

3.4 Tietoturvallisuus

Tietoturvallisuus on KATAKRI:n osa-alueista selkeästi vaativin yrityksen näkökulmasta katsottuna. Etenkin jos toiminnan luonne on tietoteknisten palveluiden ja ratkaisujen tuottaminen ja toteuttaminen, tietoturvallisuus-vaatimusten täyttäminen on haasteellista toteuttaa niin, että käytännön työ ei liikaa vaikeudu.

Tietoturvallisuus ja sen tekninen toteutus on luottamuksellisin osa-alue KATAKRI:a ja yritysturvallisuuskartoitusta. Tämä aiheuttaa omat haasteensa myös dokumentoinnille ja dokumentaation esittelylle. Tästä johtuen yritysturvallisuuskartoituksessa ei esitellä teknisiä yksityiskohtia.

3.4.1 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus – osa-alue sisältää yhteensä kymmenen kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 24 Tietoliikenneturvallisuus, kappalejako

5.1.1 Tietoliikenneverkon rakenne, I401.0
5.1.2 Palomuurisäännöt, I402.0
5.1.3 Tietoliikennettä valvovat järjestelmät, I403.0
5.1.4 Hallintayhteyksien suojaus, I404.0
5.1.5 Verkon aktiivilaitteiden kovennus, I405.0

5.1.6 Langattomien verkkojen suojaus, I406.0
5.1.7 Yhteydet muihin verkkoihin, I407.0
5.1.8 Verkon ja järjestelmien valvonta, I408.0
5.1.9 IPv6:n turvallisuus, I409.0
5.1.10 Reitityksen turvallisuus, I410.0

Kappale sisältää yksityiskohtaisia teknisiä vaatimuksia tietoliikenteen turvaamiseksi. Vaatimukset myös perustellusti kovenevat siirryttäessä Perustasolta Korotetulle tasolle ja Korkealle tasolle.

Elektrobitin yritysturvallisuuskartoituksessa tietoliikenneturvallisuus on kuvattu yleisellä tasolla ja tarvittaessa viitataan tarkempaan tekniseen dokumentaatioon. Tietoliikenneratkaisujen toteutuksesta on erillinen yksityiskohtainen dokumentaatio, mitä ei ole mielekästä sellaisenaan liittää osaksi yritysturvallisuuskartoitusta.

3.4.2 Tietojärjestelmäturvallisuus

Tietojärjestelmäturvallisuus – osa-alue sisältää yhteensä 14 kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 25 Tietojärjestelmäturvallisuus, kappalejako

5.2.1 Tietoverkon käyttäjien todennus, I501.0
5.2.2 Verkkolaitteiden asennusprosessi, I502.0
5.2.3 Haittaohjelmariskien hallinta, I503.0
5.2.4 Laitteiden ja palveluiden lokimenettelyt, I504.0
5.2.5 Suojattavan tiedon säilytys tietojärjestelmissä, I505.0
5.2.6 Liikuteltavien tallennuslaitteiden suojaus, I506.0
5.2.7 Tallenteiden tyhjentäminen huollon ja käytöstä poiston yhteydessä, I507.0
5.2.8 Luvattomien laitteiden tunnistus, I508.0
5.2.9 Käytetyt salausratkaisut, I509.0
5.2.10 Salausavainten hallinta, I510.0
5.2.11 Istunnonhallinta, I511.0
5.2.12 Autentikaatiodatan säilytys, I512.0
5.2.13 Käytettyjen ohjelmistojen turvallisuus, I513.0
5.2.14 Tietoteknisten laitteiden turvallisuus, I514.0

Tietojärjestelmäturvallisuus on samaa aihealuetta edellisen kappaleen kanssa, näiden eriyttämiselle ei ole selkeää perustetta. Rakenne toimisi yhtä lailla, jos vaatimukset olisi listattu samassa kappaleessa.

Vaatimukset ovat hyvin teknisiä ja yksityiskohtaisia. Siitä huolimatta joihinkin vaatimuksiin on ollut vaikeaa löytää toimivaa toteutusmallia. Teknisiä vaatimuksia laadittaessa olisi syytä olla myös tiedossa oleva ratkaisu, jolla vaatimus voidaan toteuttaa.

Elektrobitin osalta yksityiskohtainen tekninen dokumentaatio on omissa dokumenteissaan. Yritysturvallisuuskartoituksesta viitataan näihin tarvittavilta osin.

3.4.3 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus – osa-alue sisältää yhteensä seitsemän kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 26 Tietoaineistoturvallisuus, kappalejako

5.3.1 Tiedon luokittelu, I601.0
5.3.2 Suojattavan aineiston säilytys, I602.0
5.3.3 Suojattavan aineiston tuhoaminen, I603.0
5.3.4 Suojattavan aineiston kopiointi ja tulostus, I604.0
5.3.5 Suojattavan aineiston sähköinen välitys, I605.0
5.3.6 Suojattavan aineiston välitys postilla ja kuriirilla, I606.0
5.3.7 Suojattavan aineiston välityksen seuranta, I607.0

Tietoaineistoturvallisuus on selkeä ja toimiva vaatimuskokonaisuus. Kappaleessa kuvataan tiedon luokitteluun, säilytykseen, kuljetukseen ja tuhoamiseen liittyvät vaatimukset.

Puutteena on materiaalien ja laitteiden logistiikkaan liittyvien vaatimusten puuttuminen kokonaan.

3.4.4 Käyttöturvallisuus

Käyttöturvallisuus – osa-alue sisältää yhteensä kymmenen kappaletta. Yritysturvallisuuskartoituksessa kappaleet on nimetty ja numeroitu seuraavasti.

Taulukko 27 Käyttöturvallisuus, kappalejako

5.4.1 Jatkuvuuden varmistavat suunnitelmat, I701.0
5.4.2 Poikkeustilanteista toipuminen, I702.0
5.4.3 Tietoliikennelaitteiden ja – ohjelmistojen asentaminen, I703.0
5.4.4 Etä- ja matkatyö, I704.0
5.4.5 Kehitys-, testaus- ja tuotantojärjestelmien eriyttäminen, I705.0
5.4.6 Verkon ja palveluiden haavoittuvuus, I706.0
5.4.7 Työasemien suojaaminen työskentelyn päätyttyä, I707.0
5.4.8 Materiaalien tallennus työskentelyn päätyttyä, I708.0
5.4.9 Vastuullisten työtehtävien eriyttäminen, I709.0
5.4.10 Varmuuskopiointi, I710.0

Käyttöturvallisuus on hajanaisin osa-alue Tietoturvallisuutta. Kappaleessa määritellyt käyttäjän toimintaan liittyvät vaatimukset ovat selkeitä ja yksiselitteisiä. Jatkuvuuden hallinta ja poikkeustilanteista toipuminen ovat taas päällekkäistä asiaa hallinnollisen turvallisuuden osa-alueen kanssa.

4 Tutkimuksen tulokset

Tutkimukselle asetettiin kolme tavoitetta: KATAKRI:n vaatimusten läpikäynti ja arviointi niiden soveltuvuudesta yrityksen turvallisuusratkaisuja määriteltäessä, KATAKRI:n rakenteeseen pohjautuva yritysturvallisuuskartoitusmalli sekä Elektrobitin yritysturvallisuuskartoituksen päivittäminen KATAKRI:n rakenteen mukaiseksi ja vaatimukset täyttäväksi.

Seuraavissa kappaleissa arvioidaan tavoitteiden toteutumista ja tehdään johtopäätöksiä tutkimuksen tuloksista.

Lisäksi tuloksiin sisältyy yhteenveto havainnoista KATAKRI:n kehittämiseksi

4.1 KATAKRI:n soveltuvuus yrityksen turvallisuusratkaisujen määrittelyyn

KATAKRI:n vaatimukset ovat pääosin perusteltuja ja tukevat yritysturvallisuuden rakentumista. Jotkin, etenkin Henkilöstöturvallisuuden alaiset rekrytointiin liittyvät vaatimukset, tuntuvat itsestään selviltä. Esimerkkinä kysymys: ”P 203.0 Varmennetaanko haastattelutilanteessa työnhakijan osaamista asiantuntevilla kysymyksillä.” (KATAKRI versio 2)

Isoimmat puutteet ovat KATAKRI:n rakenteessa. Samoja vaatimuksia toistetaan eri otsakkeiden alla. Ja toisaalta aihealueita on sekoitettu eri pääotsikoiden alle. Rakenteesta aiheutuva epäselvyys vaikeuttaa ratkaisujen dokumentointia, erityisenä haasteena on turhan toistamisen välttäminen.

4.2 KATAKRI:n rakenteen mukainen yritysturvallisuuskartoitusmalli

4.2.1 Rakenne

Tavoitteeksi otettiin KATAKRI:n rakenteen mukainen yritysturvallisuuskartoitus. Päädyin rakenteessa KATAKRI:n mukaiseen kappalejakoon ja ratkaisuun, missä jokaiselle vaatimukselle on yritysturvallisuuskartoituksessa oma kappaleensa.

Vaatimusten ja toteutuksen kuvauksen yhteneväinen rakenne mahdollisti myös KATAKRI:n ja yritysturvallisuuskartoituksen kappaleiden keskinäisen linkityksen toisiinsa hyperlinkein.

4.2.2 Valitun rakenteen edut

Yksiselitteisen kappalerakenteen etuna on selkeys etenkin auditoijan kannalta. Hyperlinkein toteutettu linkitys dokumenttien välillä helpottaa ja nopeuttaa toteutusten tarkastelua.

Yhtenä etuna on myös todettava päällekkäisen dokumentaation väheneminen. KATAKRI:n rakenteen mukaisena toteutettu yritysturvallisuuskartoitus poistaa tarpeen tehdä erillinen yhteenveto vaatimuksista auditointia varten tai tarjousten liitteeksi.

Selkeänä etuna on myös todettava, että jokainen vaatimus on tällä tavoin toteutettuna käsiteltävä erikseen, mikä osaltaan takaa, että toteutus on kaikki vaatimukset huomioiva.

4.2.3 Valitun rakenteen haitat

Rakenteesta tuli tällä tavoin toteutettuna KATAKRI:n tavoin itseään toistava. Tämä korostui etenkin Hallinnollisen turvallisuuden kodalla, missä vaatimuksissa on paljon toistoa. Toistoa pyrittiin välttämään viittaamalla kappaleisiin, missä sama asia oli jo kertaalleen määritelty.

Rakenne on tällä tavoin toteutettuna kömpelö, jos yritysturvallisuuskartoitusta lukee irrallisena dokumenttina ilman KATAKRI:a. Jos dokumentaatiota käsittelee dokumenttiparina, kokonaisuus on toimivampi.

4.2.4 Johtopäätökset

KATAKRI:n rakenteen mukainen yritysturvallisuuskartoitusmalli ei ole sellaisenaan riittävän toimiva. Rakenteen selkeys ei korvaa dokumentaation kömpelyyttä ja kaavamaisuutta.

Dokumentaatiomallin saisi paremmaksi tiivistämällä kappaleita yhteen niiltä osin kuin toisto ja päällekkäisyys esiintyvät samassa pääkappaleessa. Esimerkkinä tästä on useat Hallinnollisen turvallisuuden kappaleet, kuten Riskien tunnistus, arviointi ja kontrollit. Kappaleen sisällöstä tulisi tiiviimpi ilman väliotsikoita ja alikappaleita. KATAKRI:n viittaukset tulisi tässä mallissa niputtaa osoittamaan isompia kokonaisuuksia. Auditoinnin näkökulmasta tämä ei olisi niin selkeä, koska jokaiselle kysymykselle ei olisi suoraa vastinparia yritysturvallisuuskartoituksessa.

Yksi vaihtoehto dokumentaation jatkokehitykselle olisi KATAKRI:n rakenteen muuttaminen siihen suuntaan, että se tukisi paremmin vaatimusten dokumentointia. Jos halutaan KATAKRI:a tukeva yritysturvallisuuskartoitus, joka toimii sekä itsenäisenä dokumentaationa että tukee mahdollisimman hyvin auditointia, tämä on ainut toimiva vaihtoehto.

4.3 Elektrobitin yritysturvallisuuskartoitus

Elektrobitin yritysturvallisuuskartoitus päivitettiin vastaamaan KATAKRI:n mukaista mallia. Dokumentaatio oli aiemmin hajanainen ja pitkälti aiempien DSA-vaatimusten mukainen. Nyt kukin KATAKRI:n vaatimus tuli läpikäydyksi ja dokumentaatio täydennetyksi ja yhtenäistetyksi vastaamaan samaa rakennetta.

Edelleen osa toteutuksesta on kuvattu tarkemmin erillisissä dokumenteissaan, eikä kaiken yhdistämiselle yhteen dokumenttiin ole edes perusteita. Esimerkiksi poikkeustilanteisiin varautumissuunnitelmat ja toipumissuunnitelmat on selkeintä pitää erillisinä dokumentteina. Yritysturvallisuuskartoituksessa kuvataan sisältö lyhyesti ja viitataan kyseisiin dokumentteihin.

Yritysturvallisuuskartoitus ja sen mukainen toteutus ovat tämän myötä Elektrobitillä sillä tasolla, että auditointitapahtuma tullee olemaan molemmille osapuolille helppo ja auditin läpäisy erittäin todennäköistä.

4.4 Havaintoja ja ehdotuksia KATAKRI:n kehittämiseksi

4.4.1 Toisto ja päällekkäiset vaatimukset

Samaan aihealueeseen liittyviä vaatimuksia on esitetty eri aihealueiden alla. Esimerkkinä tästä turvallisuuskoulutukset, joita on kuvattu osana Hallinnollista turvallisuutta ja Henkilöstöturvallisuutta. Toisena esimerkkinä poikkeustilanteiden hallinta, jota on käsitelty osana Hallinnollista turvallisuutta ja Tietoturvallisuutta.

Toistosta aiheutuva ongelma tulee erityisesti esille, kun yritysturvallisuuskartoituksen rakentaa KATAKRI:n rakenteen mukaisesti. KATAKRI:n käytettävyyttä ja etenkin sitä vastaavan dokumentaation kokoamista helpottaisi, jos turha toisto ja päällekkäisyys poistettaisiin.

4.4.2 Rakenne

KATAKRI:n rakennetta voisi tiivistää sekä osa-alueiden sisällä että niiden välillä. Hallinnollisen turvallisuuden kappaleita voisi tiivistää ja yhdistää ja näin vaatimukset ja etenkin niitä vastaava dokumentaatio olisi tiiviimpi ja luettavampi.

4.4.3 Sisällölliset puutteet

Selkeimpänä kokonaisuutena KATAKRI:sta puuttuu materiaalilogistiikkaan liittyvät vaatimukset. Postin lähettäminen ja vastaanottaminen on kuvattu, mutta miten toimia esimerkiksi rahtikuljetusta edellyttävän materiaalin kuljettamisessa. Tähän odotetaan päivitystä KATAKRI:n seuraavan version myötä.

Fyysisen turvallisuuden alueella on epäselviä vaatimuksia, kuten -seinä, katto-, ja lattiarakenteet. Esimerkiksi määritelmä ”vahva puu” on epäselvä ja tulkinnanvarainen. Myöskään metallisille seinärakenteille ei ole annettu selkeitä vaatimuksia.

5 Yhteenveto

Tutkimukselle asetetut tavoitteet pääosin saavutettiin. Yrityksen kannalta tärkein, Elektrobitin yritysturvallisuuskartoituksen päivittäminen, toteutui. Yleisen yritysturvallisuuskartoitusmallin määrittely ei onnistunut täysin tavoitteen mukaisena. Mallista tuli kömpelö ja irrallisena dokumenttipohjana liian kaavamainen. Tämä on pitkälti seurausta KATAKRI:n rakenteesta ja sen noudattamisesta dokumentin rakenteessa. KATAKRI:n soveltuvuuden arviointi yrityksen näkökulmasta jäi aika pinnalliseksi. Arvioinnin selkeimpänä tuloksena nousi esille KATAKRI:n rakenteen kömpelyys ja itsensä toistaminen.

Aiheena KATAKRI:n tutkiminen ja sitä vastaavan turvallisuusdokumentaation laatiminen oli haasteellista ja vei runsaasti aikaa vaikka KATAKRI oli entuudestaan tuttu useiden auditointien myötä. Työn kuluessa kutakin KATAKRI:n vaatimusta joutui pohtimaan vielä uudelleen ja useampaan kertaan. Etenkin Hallinnollisen turvallisuuden kysymyksiin oli tarvetta pohtia vastauksia ja miettiä järkevää tapaa toteuttaa dokumentaatio. Teknisimmät osiot, tietoliikenneturvallisuus ja tietojärjestelmäturvallisuus, vaativat yksityiskohtien osalta sellaista tietämystä ja ammattitaitoa, että niiden analysointiin ja dokumentointiin tarvitaan aiheeseen erityisesti perehtyneen henkilöstön työpanosta. Tästä osin Elektrobitin yritysturvallisuuskartoitusta täytyy vielä täydentää.

Dokumentointimalli on vapaasti hyödynnettävissä ja jatkokehitettävissä. Kuten todettu, malli itsessään antaa kömpelön ja kaavamaisen vaikutelman ja osittain se sitä onkin. Mutta mallin mukainen Elektrobitin dokumentaation toteutus osoitti, että se on käyttökelpoinen ja täyttää tarkoituksensa. Auditoinnissa dokumentointimallia ei ole vielä koeponnistettu, mutta uskon, että siinä sen parhaat puolet tulevat vasta esille.

Lopuksi haluan kiittää tutkielman ohjaajia Matti Kesäläistä ja Arto Pietilää sekä opponenttina toiminutta kurssitoveria Heidi Alhoa antamastanne tuesta ja opastuksesta tutkielman tekemiseen.

6 Lähteet

Elektrobit Oyj:n tilinpäätöstiedote vuodelta 2012

Kansallinen Turvallisuusauditointikriteeristö (KATAKRI) versio II

Murto Kari, Lähete KATAKRI:n käyttöönottoon HELM545-4

www.puolustusvoimat.fi/portal/puolustusvoimat.fi, DSA-tehtävät puolustusvoimissa 12.3.2013

Rimpi Kari, Saate KATAKRI:iin 1325/50.01.00/2009 FI.PLM.2009-4910

7 Liitteet

Kansallinen Turvallisuusauditointikriteeristö (KATAKRI) versio II

Yritysturvallisuuskartoitus (malli)