Sitoumuksen valvontakyvyn hallinta-malli Puolustusvoimien sidosryhmille

18. Turvallisuusjohdon koulutusohjelma

Lopputyöraportti

Jani Rantanen

Puolustusvoimat

Helsinki 1.4.2024

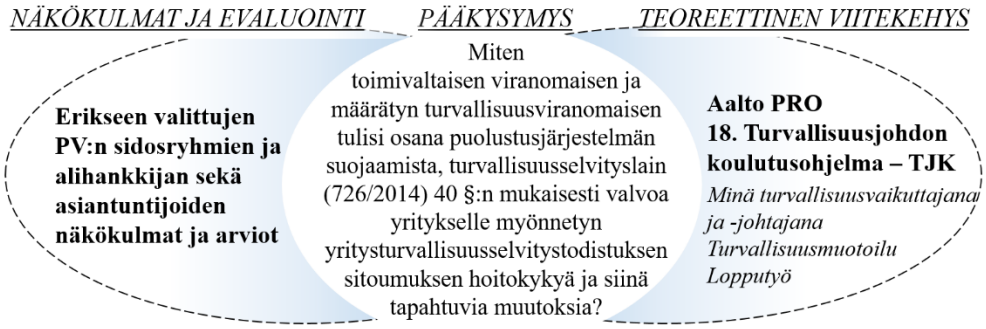
Aalto University Executive Education and Professional Development

Tiivistelmä

Lopputyössä esitän mallin, miten toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen tulisi osana puolustusjärjestelmän suojaamista, turvallisuusselvityslain (726/2014) 40 §:n mukaisesti valvoa yritykselle myönnetyn yritysturvallisuusselvitystodistuksen sitoumuksen hoitokykyä ja siinä tapahtuvia muutoksia. Tavoitteena oli laatia sitoumuksen valvontakyvyn hallintamalli, mikä velvoittaa ja osallistaa Puolustusvoimien (PV) sidosryhmät riskienhallinnan kehittämiseen osana puolustusjärjestelmän suojaamista. Lopputyön lähtökohtana sekä päämääränä oli puolustusjärjestelmän turvaaminen. Sitoumuksen valvontakyvyn hallintaa tarvitaan PV:n turvallisuusluokiteltujen asiakirjojen suojaamisen varmistamiseksi. Turvallisuusluokiteltujen asiakirjojen joutuminen ulkopuolisten henkilöiden ja toimijoiden haltuun saattaa aiheuttaa haittaa, vahinkoa, merkittävää vahinkoa tai erityisen suurta vahinkoa PV:n sidosryhmille, maanpuolustukselle, Suomen turvallisuudelle ja kansainvälisille suhteille.

Tutkimussuunnitelman laadinnassa koin erittäin tärkeäksi huomioida PV:n sidosryhmien näkökulmat. Sitoumuksen valvontakyvyn hallintamallia ei laadittu yksin Pääesikunnan (PE) ohjaamana. Erikseen valituille PV:n sidosryhmille mahdollistettiin sitoumuksen valvontakyvyn hallintaan liittyvien näkökulmien esilletuominen. Kyselyyn vastasi anonyymisti yhteensä 30 henkilöä. Arvolupauksen ja periaatteiden laatimiseksi haastattelin lopputyöhön PE:n valmiuspäällikköä lippueamiraali J. Huuskoa, Elinkeinoelämän keskusliiton (EK) johtavaa asiantuntijaa M. Rajamäkeä, Kansallista turvallisuusviranomaista (National Security Authority, NSA) P. Kaukorantaa ja Valtioneuvoston kanslian (VNK) johtavaa asiantuntijaa J. Pallaspuroa.

Lopputyön laadinnassa hyödynsin osin 18. Turvallisuusjohdon koulutusohjelman (TJK) turvallisuusmuotoiluprosessia, minä turvallisuusvaikuttajana ja -johtajana oppimisprosessia ja koulutusta mm. turvallisuusjohtaminen, tietoturvallisuus, henkilöturvallisuus, riskienhallinta, fyysinen turvallisuus, turvallisuusviestintä ja erityistilannejohtaminen. Sitoumuksen valvontakyvyn hallintamalli evaluoitiin yhteistyössä Telia Finland Oyj:n, Nokia Oyj:n, EK:n, Huld Oy:n ja Withsecure Cyber Security Services Oy:n kanssa. Evaluointitulokset auttoivat ymmärtämään hallintamallin toimivuutta yritysten näkökulmasta.



KUVA 1. Lopputyön pääkysymys, näkökulmat, evaluointi ja teoreettinen viitekehys.

Motivoitunut ja osaava henkilöstö on tärkeä riskienhallintavoimavara. Henkilöstöllä on tietoa riskienhallintakulttuurin kehittämiseksi. Henkilöstönäkökulman huomioiminen on tärkeä osa sitouttamisperusteista päätöksentekoprosessia. Sitoumuksen valvontakyvyn hallintamalli auttaa kartoittamaan henkilöstön turvallisuustarpeet ja -tunteet: tietoisuus, huolellisuus, kyvykkyys, asenteet, motivaatio, ohjeet, työvälineet, työympäristö, kulttuuri ja johtaminen. Sitoumuksen valvontakyvyn hallintamallin avolupaus: lisäarvon tuottaminen yrityksen ja alihankkijan liiketoimintaan, henkilöstön turvallisuustarpeeseen ja -tunteeseen, monitasoiseen luottamukseen, puolustusjärjestelmän suojaamiseen ja kansalliseen turvallisuuteen osana läntistä arvomaailmaa!

Toimin PE:ssa hoitaen toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen avustajan tehtäviä. Olen Suomen Riskienhallintayhdistyksen ry:n jäsen. Uskon yhdessä tehtävän valvontatyön merkityksellisyyteen uhkakuvien arvioinnissa ja inhimilliseen tietoturvallisuuskäyttäytymiseen liittyvän kulttuurin kehittämisessä. Päivitetyllä uhkatilannekuvalla PV:n sidosryhmille mahdollistetaan analysoituun tietoon perustuva johtaminen ja turvallisuusresurssien tarkoituksenmukainen käyttö.

Avainsanat: yritysturvallisuus, riskienhallinta, tietoturvallisuus, valvonta ja turvallisuuskulttuuri.

Sisältö

1 Johdanto

1.1 Konteksti

Presidentti Sauli Niinistö:

> *Eduskuntaan kohdistunut kyberhyökkäys on vakava loukkaus suomalaista demokratiaa ja yhteiskuntajärjestystä vastaan. On tärkeää, että tekijät saataisiin selville. On edelleen syytä kehittää suojautumismenetelmiä tällaista hyökkäystä vastaan.*[1]

Puolustusvoimain komentaja, kenraali Timo Kivinen:

> *On sinisilmäistä ajatella, etteikö Suomessakin tiedustelijoita toimi ja yhteistoiminnassa suojelupoliisin kanssa Puolustusvoimien vasta-tiedustelu tietysti sitä ennaltaehkäisee ja torjuu*[2].

Suojelupoliisi (Supo): tiedustelun ja vaikuttamisen keinoina ovat yleinen mielipideilmasto, poliittinen päätöksenteko ja erityisesti sen valmistelu sekä huipputeknologian tutkimus ja tuotekehitys. Suomelle merkittävimmän tiedustelun ja valtiollisen vaikuttamisen uhan muodostavat Venäjä ja Kiina. Suomen Nato-jäsenyys tekee Suomesta Venäjälle aiempaa kiinnostavamman tiedustelun ja vaikuttamisen kohteen. Kiinan Suomeen kohdistama tiedustelu jatkuu arvion mukaan aktiivisena sekä henkilötiedustelun keinoin että kyber-vakoiluyrityksinä.[3] Ulkomaiset valtiot pyrkivät hankkimaan Suomesta tieto-lähteitä päästäkseen käsiksi tietoihin, joita ei ole julkisesti saatavilla. Värväyskohteeksi voi joutua esimerkiksi virkamies tai yrityksen edustaja, joka käsittelee työssään vakoilevaa valtiota kiinnostavaa tietoa.[4]

---

[1] Ilta-Sanomat. Uutiset. 28.12.2020.
[2] Yleisradio. Ykkösaamu. 26.11.2022.
[3] Suojelupoliisi. Kansallisen turvallisuuden katsaus. 2022.
[4] Suojelupoliisi. Sinäkin voit olla värväyksen kohde. 2023.

PV:n turvallisuusluokiteltua materiaalia käsittelevät yritykset ovat PV:n sidosryhmiä. Riskien hallitsemiseksi ja turvallisuuskulttuurin kehittämiseksi PV:n sidosryhmän hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja tekninen tietoturvallisuus auditoidaan kansallisella turvallisuusauditointikriteeristöllä (Katakri 2020[5]), minkä jälkeen yritykselle myönnetään yritysturvallisuusselvitystodistus. PE:n tiedusteluosasto vastaa määrätyn turvallisuusviranomaisen tehtävistä PV:ssa[6]. Kaariste kuvasi 14. TJK-lopputyössä yritysturvallisuusselvityksen laatimista PE:ssa[7]. Toimivaltainen viranomainen valvoo turvallisuusselvityslain (726/2014) 40 §:n mukaisesti yritykselle annetun yritysturvallisuustodistuksen sitoumuksen hoitokykyä ja siinä tapahtuvia muutoksia[8].

1.2 Lopputyön tavoite ja taustat

Lopputyön tavoitteena oli laatia toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen sitoumuksen valvontakyvyn hallintamalli, mikä velvoittaa ja osallistaa PV:n sidosryhmät sitoutumaan riskienhallinnan kehittämiseen yhteistyössä toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen kanssa.

Turvallisuusselvityslain (726/2014) 40 §:ssä elinkeinonharjoittaja sitoutuu huolehtimaan tietoturvallisuustason säilyttämisestä ja antamaan tietoturvallisuustason säilyttämisen valvomiseksi viranomaiselle luvan päästä yrityksen tiloihin sekä antaa seurannassa tarvittavia tietoja[8].

Valvontatyön ja turvallisuuskontrollien merkitys on keskeinen puolustusjärjestelmän suojaamisessa motivoitunutta valtiollista toimijaa vastaan. Sitoumuksen valvontakyvyn hallinnassa esille tulleisiin haavoittuvuuksiin voidaan ajoissa puuttua riskienhallinnan keinoin ja näin suojata yritystä, henkilöstöä ja kriittistä tietoa. Arvioidaan, että organisaation ulkopuolisen valvojan tekemä tarkastus paljastaa herkemmin henkilöstön inhimilliset luotettavuus- ja turvallisuuskulttuuritekijät.

Toimivaltainen viranomainen ja määrätty turvallisuusviranomainen tulee panostamaan antamiensa yritysturvallisuusselvitystodistusten valvontakyvyn hallintaan. Valvonta koetaan perustavaa laatua olevaksi asiaksi ja tärkeäksi

[5] Katakri 2020, tietoturvallisuuden auditointityökalu viranomaisille. 2020.
[6] Puolustusvoimat, Pääesikunnan tiedusteluosasto. 2023.
[7] Kaariste, R. 14. TJK-kehitysprojekti. 2017.
[8] Turvallisuusselvityslaki 19.9.2014/726, § 40.

sitoumuksen hoitokyvyn arvioimiseksi tehtäväksi työksi. Lopputyö on tärkeä puolustusjärjestelmän suojaamiseksi, jossa ei ole varaa epäonnistua.

Sitoumuksen valvontakyvyn hallintamallilla pyritään innostamaan yritysturvallisuusselvitystodistuksessa mainittuja vastuuhenkilöitä omaehtoiseen ja aktiiviseen valvontatyöhön PV:n turvallisuusluokiteltujen asiakirjojen suojaamiseksi. Sitoumuksen valvontakyvyn hallintamalli skaalautuu yrityksen koon ja suojattavan tiedon mukaan palvellen strategisella ja operatiivisella tasolla toteutettavaa liiketoimintaa. Onnistuessaan sitoumuksen valvontakyvyn hallintamalli velvoittaa ja osallistaa PV:n sidosryhmiä turvallisuuskulttuurin kehittämisessä myös ilman PE:n aktiivista roolia.

Liitteenä 1 on turvallisuusmuotoilun Business Objective and Context.

1.3 Tutkimuskysymykset

Pääkysymys.

1. Miten toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen tulisi osana puolustusjärjestelmän suojaamista, turvallisuusselvityslain (726/2014) 40 §:n mukaisesti valvoa yritykselle myönnetyn yritysturvallisuusselvitystodistuksen sitoumuksen hoitokykyä ja siinä tapahtuvia muutoksia?

Alakysymykset.

2. Mitkä ovat PV:n sidosryhmien tavoitteet ja huolet laadittavaan sitoumuksen hoitokyvyn valvontamalliin liittyen?
3. Miten evaluointiin osallistuneet PV:n sidosryhmien edustajat ja riskienhallinnan asiantuntijat suhtautuvat sitoumuksen hoitokyvyn valvontamalliin?

1.4 Rajaukset

Lopputyö rajattiin PV:n intressien mukaisesti erikseen määritettyihin PV:n sidosryhmiin, toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen antamien yritysturvallisuusselvitystodistusten sitoumuksen valvontakyvyn hallintaan ja puolustusjärjestelmän suojaamiseen. Turvallisuusselvitysmenettelyjä ja niiden valvontaa säätelee myös esimerkiksi kansainvälisten toimittajien asettamat vaatimukset.

1.5 Teoreettinen viitekehys

Lopputyössä ei käytetty suoraan vakioitua käsitteellistä näkökulmaa tai teoreettista viitekehystä, pois lukien yleiset riskienhallinnan ja turvallisuustoimialan normit ja käytänteet.

Lopputyössä hyödynsin osin seuraavia näkökulmia lopputyön tematiikan ja rakenteen saralla:

- 18. TJK[9].
- Turvallisuusmuotoiluprosessi[10].
- Riskienhallinnan standardi[11].
- Enterprise Security Risk Management Guideline[12].
- Enterprise Risk Management Guideline[13].

1.6 Tutkimusmenetelmät

Tutkimusmenetelmien valinnassa puolustusjärjestelmän suojaaminen ja PV:n sidosryhmien näkökulmat olivat tärkeitä yhteisymmärryksen aikaansaamiseksi ja lisäarvon tuottamiseksi. Tämän pohjalta lopputyön tutkimusmenetelmiksi valittiin seuraavat kolme parhaiten soveltuvaa menetelmää:

- Kysely ja haastattelut.
- Kvalitatiivinen sisällön analyysi.
- Analyysi ja teemoittelu.

Erikseen valituille PV:n sidosryhmien edustajille mahdollistettiin osallistuminen anonyymisti sitoumuksen valvontakyvyn hallintamalliin liittyvien tavoitteiden ja huolien esille tuomiseen. Kyselytutkimus toteutettiin anonyymisti, muun aineistohankinnan ollessa julkista.

Tavoitteiden ja huolien tunnistamiseksi analysoin vastausaineiston itsenäisesti aivoriihi-tekniikalla. Tämän, TJK-luentojen ja asiantuntijalähteiden haastattelun perusteella tunnistin johtamisen fundamentit periaatteet, jotka toimivat ohjenuorana sitoumuksen valvontakyvyn hallintamallia laadinnassa.

[9] Aalto PRO, 18. TJK 2022.
[10] The Lean Service Creation Handbook 2019.
[11] SFS-ISO 31000:2018.
[12] ASIS ESRM:2019.
[13] COSO ERM:2016.

Tämän jälkeen laadin turvallisuusmuotoiluprosessilla ensimmäisen version sitoumuksen valvontakyvyn hallintamallista.

Esiymmärryksen periaatteista antoi ISO 31000 riskienhallintastandardi, johon hallintamallia verrattiin. Syvällisen ymmärryksen lisäämiseksi EK:n johtava asiantuntija ja PV:n sidosryhmien asiantuntijat arvioivat yksitellen sitoumuksen valvontakyvyn hallintamallin toimintaperiaatteiden tärkeysjärjestyksen painoarvovertailulla (Weighted Ranking). Tästä muodostui haastateltujen asiantuntijoiden yhdistetty näkemys sitoumuksen valvontakyvyn hallintamallin periaatteiden tärkeysjärjestyksestä.

Empirian saamiseksi sitoumuksen valvontakyvyn hallintamallia evaluoitiin soveltuvin osin yhteistyössä EK:n, Telia Finland Oyj:n, Nokia Oyj:n, Huld Oy:n ja Withsecure Cyber Security Services Oy:n kanssa. Evaluoinnin lopussa jokaisen sidosryhmän tai alihankkijan edustaja arvioi sitoumuksen valvontakyvyn hallintamallin periaatteiden toteutumista vastaamalla anonyymisti toimintaperiaatteita koskeviin suljettuihin väittämiin ja antoivat asiakaspalautteen avoimiin kysymyksiin oman kokemuksen, riskivastuualueensa ja edustamansa organisaation näkökulmasta.

Ymmärryksen lisäämiseksi evaluointiin osallistuneiden sidosryhmien kanssa käytiin aivoriihi (Brainstorming) sitoumuksen valvontakyvyn hallintamallista ja täydennettiin SWOT-nelikenttä (Strengths, Weaknesses, Opportunities, Threats). Evaluointi auttoi arvioimaan sitoumuksen valvontakyvyn hallintamallin käytännön toimivuutta.

Prosessin eri vaiheissa tehtiin turvallisuusmuotoilua, itsearviointia, haastateltiin asiantuntijoita, lisättiin TJK:ssa tietoisuutta, sparrattiin vertaissparraajan kanssa ja käytiin ohjaajan kanssa keskustelua. Keskustelut ovat osin luottamuksellisia.

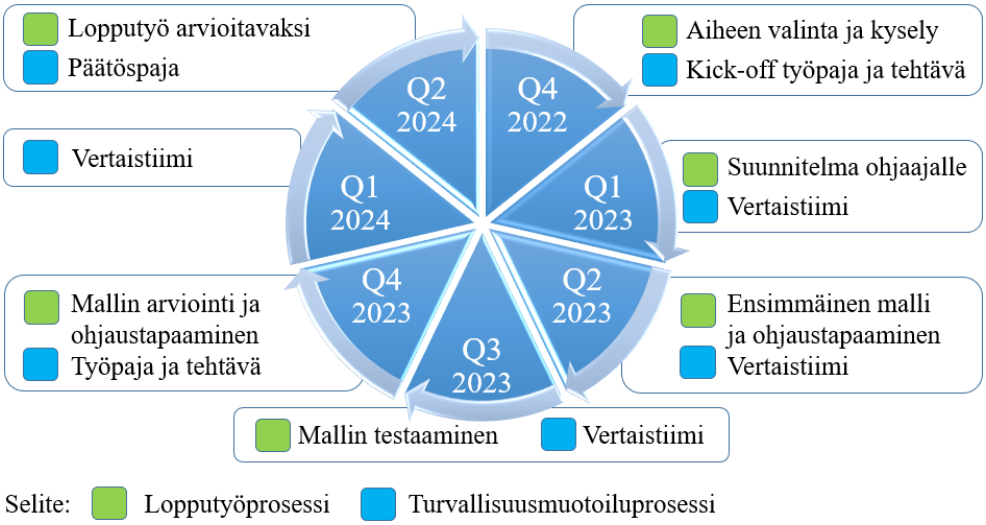
1.7 Aineisto ja sen hankinta

PV:n sidosryhmien ennakkonäkemykset sitoumuksen valvontakyvyn hallintamallista kartoitettiin kyselyllä joulukuussa 2022. Kysely sisälsi monivalintakysymyksen vastaajan organisaation henkilöstömäärään liittyen ja kolme avokysymystä hallintamallin tavoitteista, huolista ja huomioitavista asioista. Aktiivisille sidosryhmille mahdollistettiin tarkentavien kysymysten esittäminen kyselyn laatijalle ja tuoda esille halukkuus osallistua sitoumuksen

valvontakyvyn hallintamallin testaamiseen ja kehitystyöhön. Kyselyyn vastasi 30 henkilöä ja muutama sidosryhmä ilmaisi halukkuutensa sitoumuksen valvontakyvyn hallintamallin evaluointiin. Vastaajat ilmoittivat kyselyssä oman työnantajan henkilöstömäärän seuraavasti: alle 50 henkilöä 7 vastaajaa, 50-249 henkilöä 5 vastaajaa ja 250+ henkilöä 18 vastaajaa. Kyselyn vastaukset ovat kyselytutkimuksen käsittelijän hallussa.

Lopputyössä esitettävän sitoumuksen valvontakyvyn hallintamallin luotettavuutta ja käytettävyyttä arvioitiin asiantuntijahaastatteluin ja TJK-tiedoilla. Oman tärkeän näkökulman kertoivat EK:n johtava asiantuntija, Kansallinen turvallisuusviranomainen NSA, PE:n valmiuspäällikkö ja VNK:n johtava asiantuntija. Hyödynsin osin Aalto PRO 18. TJK-kouluttajien ja vierailevien luennoitsijoiden esille tuomia tietoja.

1.8 Aikataulu



KUVA 2. Lopputyö- ja turvallisuusmuotoiluprosessin aikataulu.

1.9 Hallintamallin keskeiset termit

Asenne

Henkilöstön asenne kruunun tietojen varovaiseen käsittelyyn ja säilytykseen on joko positiivinen tai negatiivinen.

Huolellisuus

Huolellisuudella tarkoitetaan kruunun tietojen huolellista ja ohjeiden mukaista käsittelyä ja säilytystä työkiireistä huolimatta.

Johtaminen

Johtamisella tarkoitetaan sitä, kuinka koko henkilöstö sitoutetaan tunnetasolla turvallisuusviestinnän ja -johtamisen keinoin sitoumuksen valvontakyvyn jatkuvaan seurantaan, suunnitteluun, toteutukseen, kehittämiseen, tietoisuuden lisäämiseen ja ylläpitoon.

Kruunun tiedot

Kruunun tiedoilla tarkoitetaan kriittisiä tietoja ja turvallisuusluokiteltuja asiakirjoja, joiden joutuminen ulkopuolisten henkilöiden ja toimijoiden haltuun saattaa aiheuttaa joko haittaa, vahinkoa, merkittävää vahinkoa tai erityisen suurta vahinkoa yrityksen liiketoiminnalle, maanpuolustukselle ja Suomen turvallisuudelle.

Kulttuuri

Kulttuurilla tarkoitetaan ajattelua ja käytänteitä sitä, kuinka avoimesti ja luottamuksellisesti kruunun tietoihin kohdistuvista riskeistä keskustellaan ja riskienhallintaa kehitetään yhdessä koko henkilöstön kanssa.

Kyvykkyys

Kyvykkyydellä tarkoitetaan riskienhallinnan toteuttamista osaavasti kruunun tietojen suojaamiseksi, esimerkiksi turvallisuuspoikkeamien tunnistaminen ja ilmoittaminen.

Motivaatio

Motivaatiolla tarkoitetaan sisäisiä ja ulkoisia motivaatiotekijöitä, jotka vaikuttavat kruunun tietojen turvalliseen käsittelyyn ja säilytykseen.

Ohjeet

Ohjeilla tarkoitetaan kruunun tietojen käsittelyyn ja säilytykseen liittyvien turvallisuusohjeiden selkeyttä, ymmärrettävyyttä ja helppoa saatavuutta.

Sitoumuksen valvontakyvyn hallintamalli

Puolustusjärjestelmän suojaamiseen lisäarvoa tuottava hallintamalli. Koostuu kolmesta osa-alueesta (viestintäsykli, periaatteet ja sitoutuminen), joissa arvolupauksen tuottamiseksi henkilöstön turvallisuustarpeet ja -tunteet ovat tärkeitä.

Tietoisuus

Tietoisuudella tarkoitetaan henkilöstön tietoisuutta kruunun tiedoista, haavoittuvuuksista ja uhkakuvista.

Työvälineet

Työvälineillä tarkoitetaan kruunun tietojen käsittelyyn ja säilytykseen tarkoitettuja teknisiä työvälineitä, jotka mahdollistavat henkilöstölle tarkoituksenmukaisen ja turvallisen työskentelyn.

Työympäristö

Työympäristöllä tarkoitetaan kruunun tietojen fyysistä käsittely- ja säilytysympäristöä, mikä mahdollistaa henkilöstölle tarkoituksenmukaisen ja turvallisen käyttäytymisen.

2 Teoreettinen viitekehys

2.1 Turvallisuusjohtaminen

Turvallisuus on PV:n sidosryhmiin, alihankkijoihin ja ihmisiin kohdistuvan myrskyn eli epävarmuuden tunnistamista, siihen varautumista ja resilienssiä toimia tilanteessa. Turvallisuus on yrityksen johdon ja yksilön tunnetila, että tulevasta myrskystä selvitään. Turvallisuus voi olla PV:n sidosryhmälle, alihankkijalle tai yksilölle elämänkysymys.

Limnéll totesi turvallisuuden strategisen johtamisen merkityksestä organisaatioissa: turvallisuus on strateginen asia, joka on nähtävä ensisijaisesti positiivisesti mahdollistajana. Asiakkaiden luottamus yrityksen arvona – ilman luottamusta ei ole turvallisuutta ja ilman turvallisuutta ei ole luottamusta. Turvallisuus on digitaalisella aikakaudella yhä vahvemmin kamppailua mielikuvista ja tunteista. Limnéll muistutti, että turvallisuus on yrityksille kilpailuetu.[14]

Todellisuuden muutosnopeus, ennalta-arvaamattomuus ja kompleksisuus ovat osa turvallisuutta. Ihmisten mielikuvia todellisuudesta ja koettua turvallisuutta ei saa väheksyä. Turvallisuusviestinnällä ja johtamisella on keskeinen vaikutus ihmisten turvallisuustunteeseen. Yhteiskunnalla, yrityksillä ja ihmisillä on oltava resilienssiä toimia oikealla tavalla. Turvallisuus on myös opittuja toimintatapoja. Myös henkisellä sietokyvyllä on merkitystä – Limnéll pohti turvallisuuden eri tekijöitä.[14]

Haukkovaara korosti, että yrityksen ylin johto on vastuussa riskienhallinnasta. Yritysten ajattelutapa, ettei kukaan ole kiinnostuneita meistä, ei Haukkovaaran mielestä pidä paikkaansa. Tästä ovat esimerkkinä Supon raportit ja kyberturvallisuuskeskuksen katsaukset. Yrityksen hallituksen vastuulla on voitontuotto omistajille. Sijoittajille on tärkeää yrityksen maine

[14] Limnéll, J. Aalto PRO, 18. TJK-luento 10.11.2022.

ja vastuullisuus, tämän takia yrityksen digitaalisen turvallisuuden tulee olla kunnossa. Yrityksen johdon tulee turvallisuusjohtamisessa huomioida kyberiskit.[15]

Aalto-yliopiston yliopistonlehtori, Jari Ylitalo:

> *Vaikuttamisen ympäristö muuttuu koko ajan*[16].

Investoidun turvallisuuskampanjan toteutuksen jälkeen yrityksen johto saattaa ajatella, että nyt kaikki on kunnossa. Ylitalon mukaan kovin usein näin ei ole, koska jälkihoito unohtuu. Tällöin ihmiset saattavat turhautua, koska asioita ei saatu kuntoon. Johtamisen näkökulmasta turvallisuuskampanja tulisi kokea aloituksena, jossa tärkeisiin koettuihin asioihin halutaan jatkossa kiinnittää huomiota. Näiden saaminen osaksi turvallisuuskulttuuria vaatii työtä.[16]

Asiakkaan odotukset ja turvallisuuden keinojen on vastattava odotuksia. Henkilöstön kanssa toimiminen on lisääntynyt, ja se koetaan tärkeäksi osaksi organisaation resilienssiä. Tulee pohtia, miten tietoturvallisuuskokonaisuus saadaan organisaatiossa toimimaan. Luottamuksellisuus vaikuttaa henkilöstön halukkuuteen kertoa turvallisuusasioista. Tulee pohtia, ollaanko etsimässä syyllisiä vai laittamassa asiat kuntoon. Tasapainoa valvonnan ja luottamuksellisuuden välillä on arvioitava. Ylitalo korosti henkilöstön osallistavan roolin tärkeyttä. Henkilöstön omassa työympäristössä tekemät turvallisuushavainnot ovat tärkeä huomioida. Myös tapa, miten turvallisuudesta puhutaan, on merkitystä. Ylitalo kertoi, että vaikuttamisen ja vaikuttavuuden rakentamisessa on huomioitava: 1. Vaikuttamisen kohteet – mihin pyritään vaikuttamaan? 2. Vaikuttamisen konteksti – missä pyritään vaikuttamaan? ja 3. Vaikuttamisen keinot – miten pyritään vaikuttamaan?[17]

Vaikuttamisen tyyliä on vaihdettava kohderyhmän mukaan. Odotusten hallintaa ovat kuuntelemisen taito, osallistamisen mahdollistaminen ja tavoitteisiin sitouttaminen, ratkaisukeskeisyys, asian kiteyttäminen, tiedon lisäämi-

[15] Haukkovaara, T. Aalto PRO, 18. TJK-luento 14.4.2023.
[16] Ylitalo, J. Aalto PRO, 18. TJK-luento 8.11.2023.
[17] Ylitalo, J. Aalto PRO, 18. TJK-luento 11.11.2022.

nen, faktoihin perustuva keskustelu ja mentorointi. Merkittävä osa vaikuttamista on tunteiden mukaan ottaminen viestintätilanteisiin. Myös johdon roolin tunnistaminen on tärkeää systeemistason vaikuttamisessa.[18]

Tutkimuksessa 16 prosenttia 19 maan tutkitusta työntekijöistä (jokaisesta maasta tutkittiin noin 1 000 sattumanvaraisesti valittua työntekijää hyvin erilaisista ammateista ja tehtävistä) oli erittäin sitoutuneita. Sitoutumisen tasoa pidetään varsin alhaisena. Tiimeissä työskenteleminen tuplaa sitoumuksen verrattuna niihin, jotka eivät ole tiimeissä. Jäsenet tiimissä ovat kahdeksan kertaa todennäköisemmin hyvin sitoutuneita, jos he luottavat esimieheensä vahvasti. Luottamus on avainsana ja perusta tiimin jäsenten sitoutumiselle.[19]

Toimela korosti, että turvallisuusasioissa yrityksen johdon sitoutuminen ja turvallisuusviestintä ovat äärimmäisen tärkeää. Vuoropuhelua tulee käydä henkilöstön kanssa – henkilöstöä tulee osallistaa riskien kartoitukseen, jolloin samalla syntyy vahvempi sitoutuneisuus riskien hallintaan.[20]

Sarvas totesi, että ymmärtämistä auttaa, jos tunnetaan henkilöstön toiminnan taustalla olevat rationaaliset, emotionaaliset ja empaattiset tasot. Motivaation, tunteiden, tavoitteiden, arvojen, asenteen, ennakkoluulojen, käyttäytymisen, tekemisen ymmärtämiseksi on tärkeä osata kysyä: *”Miksi?”.* Syvällisen ymmärryksen aikaansaamiseksi ja turvallisuustavoitteiden saavuttamiseksi tulee ymmärtää paremmin henkilöstön tarpeet ja tunteet.[21]

2.2 Tietoturvallisuus

PV:n sidosryhmissä kehittyvän tietoturvallisuuskulttuurin edellytyksenä on sotilasilmailun kaltainen toimintatapa, jossa matalalla kynnyksellä ilmoitetaan lentoturvallisuuta vaarantavista asioista. Avoimessa ja luottamuksellisessa ilmapiirissä henkilöstö uskaltaa ilmoittaa tietoturvallisuushavainnoista vertaisilleen, asiantuntijoille ja esimiehille. Havaintojen perusteella organisaatiolla on mahdollisuus kehittää tietoturvallisuutta. PV:n sidosryhmissä tulisi tavoitella sotilasilmailun kaltaista avointa, luottamuksellista, vastuullista, ammattitaistoista ja yhdessä tekemisen tapaa kehittää tietoturvallisuuskulttuuria.

[18] Ylitalo, J. Aalto PRO, 18. TJK-luento 11.11.2022.
[19] Buckingham, M. & Goodall, A. The Power of Hidden Teams 2019.
[20] Toimela, E. Aalto PRO, 18. TJK-luento 25.5.2023.
[21] Sarvas, R. Aalto PRO, 18. TJK-luento 24.5.2023.

Aktia Pankki Oyj:n Director, Head of Information Security Henri Heinonen:

> *Kulttuuri on sitä, mitä tapahtuu, kun ihminen jää omilleen*[22].

Turvallisuuskulttuurin kehittämisessä ja tietoisuuden lisäämisessä henkilöstöllä on tärkeä merkitys. Vastuu tietoturvallisuudesta on organisaation johdolla ja koko henkilöstöllä. Henkilöstö ei ole heikoin lenkki, vaan se on arvokas voimavara. Henkilöstön on ymmärrettävä oma rooli tietoturvallisuuden toteuttajana. Kulttuuria tulee kehittää oikeaan suuntaan esimerkiksi huumorilla, palkitsemisella, ihmisläheisemmällä tavalla, matalalla kynnyksellä ja viestinnällä, joilla saadaan tulosta ilman pakollista koulutusta. Tietoturvallisuus on liiketoimintalähtöistä, jossa huomioidaan yrityksen strategian muutokset ja teknologian kehittyminen.[22]

Pennanen piti henkilöstöä tietoturvan vahvimpana lenkkinä. Koko henkilöstön sitouttaminen tietoturvallisuuden toteuttamiseen lisää tietoturvallisuutta. Tietoturvallisuuskulttuuria on kehitettävä kannustamalla henkilöstöä. Kokonaisturvallisuuden varmistamisessa, kehittämisessä ja riskiin varautumisessa turvallisuuden ja tietoturvallisuuden on tehtävä yhteistyötä. Esimerkkinä Pennanen mainitsi ulkopuoliset luennoitsijat ja videot, joista voi tunnistaa virheellisiä toimintatapoja.[23]

Tietoevry Oyj:n Quality, Security & Privacy Lead, Jari Pirhonen:

> *Brändi on tärkeää digitaalisessa maailmassa ja sen voi romuttaa hetkessä*[24].

Pirhonen arvioi, että digitaalisessa maailmassa asiakkaan luottamus on tärkeää. Sopimuksissa on tärkeä määritellä, mitä tietoturvallisuudella tarkoitetaan. Asiakasluottamuksen hankkimiseksi yritysten on osoitettava verkkojen, palveluprosessien ja tietojen suojaamisen taso. Yritysten hallitus vastaa organisaation tietoturvallisuudesta.[24]

Kulttuurin kehittäminen on tärkeässä osassa tietoturvallisuutta. Riskienhallinnassa on tunnistettava yritykselle tärkeäksi koetut palvelut ja prosessit. Yrityksen johdon tietoturvallisuuden tahtotilasta, riskinottohalukkuudesta ja

[22] Heinonen, H. Aalto PRO, 18. TJK-luento 13.4.2023.
[23] Pennanen, J. Aalto PRO, 18. TJK-luento 14.4.2023.
[24] Pirhonen, J. Aalto PRO, 18. TJK-luento 13.4.2023.

strategiasta on viestittävä työntekijöille. Koska yrityksen ylin johto määrää resurssit, tulisi yrityksen tietoturvallisuuden tasoa verrata vastaavan toimialan yrityksiin, Pirhonen kertoi. Projektipäälliköiden ja henkilöstön on ymmärrettävä tietoturvallisuuden tärkeys, jotta tiedot voidaan suojata niiden koko elinkaaren ajan. Suojattavan tiedon tunnistamisen lisäksi yrityksissä on kiinnitettävä huomiota perusasioihin ja johdon on näytettävä esimerkkiä. Kokonaisuuden huomioimiseksi henkilöstöä on koulutettava ja motivoitava tietoturvalliseen käyttäytymiseen. Tietoturvallisuus on nivottava liiketoimintaan, Pirhonen painotti.[25]

Henkilöstön roolia organisaation turvallisuudessa, inhimillisiä tekijöitä ja vastuuta arvioitiin. Keskustelussa henkilöstön rooli koettiin tärkeäksi. Tämän takia henkilöstön perusvalveutuneisuuden ja vastuun tasoa tulisi nostaa. Henkilöstöä tulee opettaa tunnistamaan riskejä. Monimutkaisissa teknisissä toimintaympäristöissä asiantuntijoiden tulee neuvoa henkilöstöä. Pirhonen korosti, että turvallisuutta tulee automatisoida mahdollisimman paljon ja henkilöstön ymmärrys tulee varmistaa. Keskustelussa tuli esille inhimillisten heikkouksien ilmenemisen tunnistaminen ja niiden parempi huomioiminen. Henkilöstöllä tulee olla riittävä osaaminen ja kyvykkyys. Esimerkkinä mainittiin ohjeiden helpon saatavuuden tärkeys tarpeen ilmaantuessa. Henkilöstöä tulee osallistaa turvallisuuden kehittämiseen. Pirhonen totesi, että kehittämisessä on tärkeää, että parannusehdotukset tulevat henkilöstöltä. Henkilöstö tunnistaa paremmin missä inhimillinen heikkous ilmenee.[25]

Tietoevry Oyj:n Quality, Security & Privacy Lead, Jari Pirhonen:

Koko henkilöstön toiminnan muuttaminen vaatii työtä[26].

Yrityksen henkilöstön turvallisuuskäyttäytymisen kartoittamien on tärkeää sitoumuksen hallintakyvyn arvioimiseksi, jotta esimerkiksi turvallisuuskoulutus voidaan kohdentaa oikein. Kartoituksessa havaitaan osaamisen puutteet, tunnistetaan toiminnallisia esteitä, toimimattomia työkaluja ja kulttuurillisia kehitettäviä asioita. Yrityksen henkilöstölle on mahdollistettava tietoturvallinen toimintatapa, Pirhonen painotti.[26]

[25] Pirhonen, J. Aalto PRO, 18. TJK-luento 14.4.2023.
[26] Pirhonen, J. Haastattelu 14.4.2023.

Pirhonen kokee yrityksen johdon roolin tärkeäksi tietoturvallisuuskulttuurin luomisessa. Esimiesten on tuettava henkilöstöä tietoturvallisuudessa eri tasoilla. Tietoturvallisuuden johtaminen on tehokkaampaa, jos päätöksenteko perustuu ajantasaiseen tilannetietoon. Henkilöstön turvallisuuskäyttäytymistä voidaan mitata esimerkiksi haastatteluin ja kyselyin. Päätöksenteossa tarvittava taustatieto voi perustua myös turvallisuuspoikkeamatietoihin tai Red Team haavoittuvuushavaintoihin. Motivoinnin takia tulee kertoa tarve-aspekti, jotta henkilöstö ymmärtää tietoturvallisuuden tärkeyden.[27]

Allianz riskibarometri on globaaleja liiketoimintariskejä kartoittava tutkimuskysely. Kysely perustuu noin 2700 riskienhallinnan asiantuntijan näkemykseen yli 80 maasta ja yli 20 toimialalta.[28] Tuloksissa korostuivat kyberriskit ja liiketoiminnan keskeytysriskit.

TAULUKKO 1. Allianz riskibarometri 2022-2024[29].

Aalto-yliopiston työelämäprofessori, Timo Seppälä:

> *Teknologiaosaamisella ei ole koettu olevan yhteyttä yrityksen strategiaan*[29].

[27] Pirhonen, J. Haastattelu 14.4.2023.
[28] Allianz Global Corporate & Speciality, Allianz Risk Barometer 2022-2024.
[29] Seppälä, T. Aalto PRO, 18. TJK-luento 12.4.2023.

Seppälä totesi, että 11 prosentissa Suomalaisissa yrityksissä on puute digiosaajista. Viimeisen 30 vuoden aikana osaaminen on monessa yrityksessä ulkoistettu. Tämä johtaa tilanteeseen, jossa uuden teknologian esimerkiksi tekoälyn mahdollisuutta ei ymmärretä. Seppälä peräänkuulutti yrityksiltä digitaalista suunnitelmaa ja tarvittavaa digiosaamista.[30]

2.3 Henkilöturvallisuus

Turvallisuuden vaarantaminen on joko tahallista tai tahatonta. Insider-uhka ilmenee monin eri tavoin esimerkiksi väkivallalla, vakoilulla, sabotaasilla, varkauksilla ja kyberteoilla. Cybersecurity and Infrastructure Security Agency (CISA) määrittelee Insider-uhkan seuraavasti:

> *…insider will use their authorized access, wittingly or unwittingly, to do harm to the department´s mission, resources, personnel, facilities, information, equipment, networks, or systems.*[31]

Suojattavaan tietoon pääsyssä ulkomaan tiedustelupalvelut hyödyntävät värväysprosessissa ihmisen persoonallisuuden piirteitä. Yhteisöllisten tunteiden puuttuminen mahdollistaa kansallisen, yrityksen ja ihmisten turvallisuuden vaarantamisen. Sisäinen oikeutus toiminnalle saadaan esimerkiksi koetun vääryyden, arvostuksen puutteen tai tyytymättömyyden tunteen kautta. Taustalla saattaa olla myös hallitsemattomat taloudelliset ongelmat, pitkäaikainen stressi, poikkeuksellisesti psykoottiset mielenterveysongelmat, perheväkivalta, päihteiden väärinkäyttö, ääriajattelu ja ohjeiden vastainen toiminta.[32]

Niuvanniemen sairaalan johtava lääkäri, Allan Seppänen:

> *…kaikki elementit ovat tämän päivän maailman politiikassa*[32].

Ihmisen käyttäytymisen ja päätöksenteon taustalla vaikuttavat persoonallisuuden ominaisuudet ja psykiatriset poikkeavuudet. Riskin kärjistymisen taustalla on myös riskinottohalua ja henkilön vakiopiirteitä provosoivia ulkoisia tekijöitä. Riskejä ottava, omaa etua tavoitteleva, alistava ja aggressiivinen henkilö voi olla äärimmillään narsisti, psykopaatti, äärimmäisen itsekeskeinen omaa egoa tavoitteleva ja täydellistä välinpitämättömyyttä

[30] Seppälä, T. Aalto PRO, 18. TJK-luento 12.4.2023.
[31] Cybersecurity & Infrastructure Security Agency. Defining Insider Threats 2023.
[32] Seppänen, A. Aalto PRO, 18. TJK-luento 15.3.2023.

muista osoittava henkilö. Arvion mukaan antisosiaalisia persoonallisuushäiriöitä omaavia on noin yksi prosentti väestöstä. Seppänen toteaa, että mahdollinen henkilöriski konkretisoituu, mikäli organisaatiossa suhtaudutaan välinpitämättömästi huolestuttaviin käytöksiin.[33]

Sallinen totesi, että ihmisten turvallisuustunteeseen vaikuttavat Ukrainan sota, inflaatio, polttoaineen kallistuminen, ruuan hinnannousu ja poliittisen retoriikan muuttuminen. Yhteiskunnan vastakkainasettelun, syrjäytymisen, maalittamisen, järjestäytyneen rikollisuuden ja epäoikeudenmukaisuuden tunteen lisääntyminen vaikuttavat ihmisten lisäksi myös yrityksiin.[34]

Maalittamisen ennaltaehkäisyn ja varautumisen keinoina Sallinen tuo esille henkilöturvallisuusstrategian tärkeyden henkilöstöriskien tunnistamiseksi, vastuiden ja velvollisuuksien määrittämiseksi, hallinnollisten prosessien laatimiseksi, konkreettisten toimenpiteiden tekemiseksi ja henkilöstön kouluttamiseksi. Sallinen korostaa luottamuksen ja turvallisuuskontrollien merkitystä yrityksissä. Objektiivisen tilannekuvan, motiivien ja eri tekijöiden ymmärtäminen on päätöksenteossa tärkeää.[34]

Inhimilliset tekijät (Human Factor, HF):

> *…tarkoitetaan yksilön, ryhmän, työn, organisaation toiminnassa ilmeneviä tekijöitä, jotka voivat joko heikentää tai vahvistaa turvallisuutta, terveyttä ja työn sujuvuutta* [35].

HF näkökulmat tulee huomioida organisaation turvallisuuden kehittämisessä. Teperi totesi, että tietoturvallisuudessa tulisi olla HF-ajattelua, koska ihminen on turvallisuuden tekijä ja osa resilienssiä. HF:ssä kiinnitetään huomiota onnistumisiin, ihmisten toiminnan kokonaisvaltaiseen ymmärtämiseen, toimenpide-ehdotuksiin, luottamuksen ja avoimuuden lisäämiseen. Henkilöstöä ei syyllistetä ja ylimmän johdon linjaukset ovat tärkeitä. Osallistavassa ja yhteistyötä lisäävässä turvallisuuden kehittämisessä on tärkeää ennakoivuus ja ratkaisukeskeisyys. Teperi: HF auttaa juurisyiden tunnistamisessa, luottamuksen lisäämisessä ja turvallisuuskulttuurin muuttamisessa.[36]

---

[33] Seppänen, A. Aalto PRO, 18. TJK-luento 15.3.2023.
[34] Sallinen, S. Aalto PRO, 18. TJK-luento 16.3.2023.
[35] Työterveyslaitos 2023.
[36] Teperi, A-M. Aalto PRO, 18. TJK-luento 12.12.2023; Teperi, A-M. Ihminen turvallisuuden tekijänä 2023.

2.4 Riskienhallinta

Turvallisuusjohtamisen ja ISO 31000-riskienhallinnan periaatteet:

- on integroitu organisaation prosesseihin,
- on järjestelmällistä ja jäsenneltyä,
- on toteutettu organisaation tarpeiden mukaan,
- on kattava ja läpinäkyvä,
- on dynaamista, toistuvaa ja muutoksiin reagoivaa,
- perustuu parhaaseen saatavilla olevaan tietoon,
- ottaa inhimilliset ja kulttuurilliset tekijät huomioon sekä
- tukee ja ajaa jatkuvaa kehittämistä[37].

ASIS International ESRM- ja COSO ERM-ohjeissa korostuvat strateginen lähestymistapa, joissa tuetaan organisaation tavoitteiden saavuttamista. Riskienhallinnan ammattilaisten rooli on tukea organisaation johtoa päätöksentekoprosessissa ja tavoitteiden saavuttamisessa. Toiminnassa painottuvat organisaation suorituskykyyn vaikuttavien asioiden tunteminen, tavoitteiden saavuttamiseen kohdistuvien riskien tunnistaminen, arviointi ja käsittely. Riskienhallintaprosessin toteuttaminen edellyttää avointa turvallisuuskulttuuria, jossa korostuu jatkuva kehittäminen ja seuranta.[38]

Fortum Oyj:n Head of Enterprise Risk Management and Insurances,
Tiia Mukkala:

> *ERM on sateenvarjo, mikä kokoaa yhteen kaikki riskienhallinnan osa-alueet – turvallisuusriskit muodostavat yhden näistä osa- alueista*[39].

Suurimmat haasteet riskienhallinnan toteuttamisessa liittyvät liiketoimintojen maturiteettiin ja resursseihin. Isossa organisaatiossa haasteena on riskivastuullisten tunnistaminen ja riskienhallintaan vaadittavan ajan löytäminen, mikäli sitä ei nähdä tuottavana työnä, Mukkala kertoi.[39]

Rajamäki kertoi kolmesta puolustuslinjasta (Three Lines of Defence). Mallissa liiketoiminta omistaa liiketoiminnan riskit ja toteuttaa riskienhallintaprosessia ensimmäisessä puolustuslinjassa. Toisessa puolustuslinjassa tuetaan liiketoimintaa riskienhallinnan implementoinnissa ja kehitetään

[37] Rajamäki, M. Aalto PRO, 18. TJK-luento 13.12.2022; SFS-ISO 31000:2018.
[38] ASIS ESRM 2019 & COSO ERM 2017.
[39] Mukkala, T. Aalto PRO, 18. TJK-luento 13.12.2022.

riskienhallintaa. Kolmannen puolustuslinjan tehtävänä on tuottaa riippumatonta tietoa ja varmennusta ylimmälle johdolle. Kolmannessa puolustuslinjassa arvioidaan kahden muun puolustuslinjan tehokkuus suhteessa organisaation tavoitteisiin ja visioihin.[40]

Paavilainen painotti yrityksissä riskien tunnistamisen tärkeyttä, jotta niitä voidaan hallita. Riskit tulee laittaa tärkeysjärjestykseen ja riskienhallintatoimenpiteitä tulee pohtia. Riskien pienentäminen ei Paavilaisen mielestä vaadi aina rahaa. Organisaatioissa voidaan simuloida esimerkiksi jatkuvuussuunnitelmia. Resilienssin nostaminen edellyttää tilanteiden läpikäymistä. Tämä helpottaa toiminnan ymmärtämistä ja lopulta päätöksentekoa.[41]

Raivio totesi, että vastuullisuuden osoittaminen edellyttää riskienhallintatyötä. Turvallisuus on kytkettävä liiketoiminnan hyötyihin. Tämä helpottaa resurssien saamista. Vastuuhenkilöiden tulee pyrkiä hyödyntämään syntyvää momenttumia. Vastuullisuutta toteutetaan yrityksissä arvopohjaisesti, ja sitä voidaan hyödyntää yhteistyössä alihankkijoiden kanssa.[42]

Tilannekuva on kooste organisaation toimintaympäristöstä. Tilannekuvan laatimisprosessilla tuotetaan analysoitua tietoa päätöksenteon tueksi faktoista, näkökulmista, resursseista ja tunteista. Tilannetietoisuus on kohderyhmäsidonnaista. Tilannekuvan laatijan ja kohderyhmän välillä tulisi olla luottamusta ja avoimuutta. Dolk totesi, että pitää pyrkiä ymmärtämään omia ajatusvääristymiä eli kognitiivisia vinoumia. Taustalla olevat vinoumat on tunnistettava – sama kohde, monta tilannekuvaa. Parhaimmillaan turvallisuustilannekuva edistää organisaation resilienssiä.[43]

2.5 Turvallisuusviestintä

Sarvas totesi, että 2000-luvulla epävarmuus on kasvanut ja sykli on kiihtynyt. Tästä ovat esimerkkinä innovoinnin nopeus, uusi teknologia, asiakkaiden odotusten kasvaminen ja muuttuminen – vanhat rakenteet harovat vastaan ja perinteiset liiketoiminnan johtamisen periaatteet eivät toimi. Epävarmassa toimintaympäristössä on keskityttävä ratkaisemaan tietyt organisaation tavoitteet suhteessa asiakkaiden tarpeisiin ja tavoitteisiin. Sarvas korosti, että ratkaisun löytämiseksi tulee palata perusasioiden äärelle – toiminnan tulee

[40] Rajamäki, M. Aalto PRO, 18. TJK-luento 13.12.2022.
[41] Paavilainen, T. Aalto PRO, 18. TJK-luento 9.11.2023.
[42] Raivio, T. Aalto PRO, 18. TJK-luento 24.5.2023.
[43] Dolk, L. Aalto PRO, 18. TJK-luento 13.3.2024.

olla asiakaslähtöistä ja arvoa tuottavaa sekä fundamentaalit asiat on tunnistettava sumun keskellä.[44]

Aalto-yliopiston yliopistonlehtori, Jari Ylitalo:

> *Viesti ei synny silloin kun avaan suuni, vaan kun se tavoittaa toisen ihmisen*[45].

Vaikuttamisen tyyliä on vaihdettava kohderyhmän mukaan. Odotusten hallintaa ovat kuuntelemisen taito, osallistamisen mahdollistaminen, tavoitteisiin sitouttaminen, ratkaisukeskeisyys, asian kiteyttäminen, tiedon lisääminen, faktoihin perustuva keskustelu ja mentorointi. Merkittävä osa vaikuttamista on tunteiden mukaan ottaminen viestintätilanteisiin. Johdon roolin tunnistaminen on tärkeää systeemitason vaikuttamisessa.[45]

Maula totesi, että turvallisuusviestinnän periaatteiden ja pääviestin tulee olla selkeitä. Organisaation johdon kanssa tulee keskustella tilannekuvasta sekä päätavoitetason asettamisesta ja kiteyttämisestä. Tavoitteiden saavuttamiseen tarvitaan koko organisaation työpanosta, jossa avoimuus luo toiminnalle pohjan. Turvallisuusviestinnän tulee sitouttaa ja kannustaa myös sidosryhmät toimintaan. Luottamuksen rakentaminen, rehellinen ja nöyrä lähestymistapa ovat tärkeitä periaatteita, Maula korosti.[46]

Korpiola painotti inhimillisen näkökulman huomioimista, jotta faktapohjaisen turvallisuusviestinnän lisäksi argumentoidaan myös tunteella. Menestystarinaan tarvitaan myös tilannekuva nykyhetkestä (josta johdetaan sen hetkinen tilanneymmärrys) ja (tuodaan) näkymä tulevaisuudesta. Toimintakulttuuriin tulee ottaa mukaan tunnevaste, kehonkieli ja intensiteetti, jonka jälkeen ne sovitetaan yhteen kohderyhmän tunteeseen. Esimerkiksi sosiaalisella medialla voidaan tavoittaa yleisö ja olla suoraan yhteydessä sidosryhmiin. Kuka asettaa agendan? Miten ihmisistä tulee tärkeä osa maanpuolustuksen tarinaa? Toivon ja uskon luomisessa tunnekomponentti tulee kytkeä turvallisuuden agendaan, jolloin viestintä tulee automaattisesti ja vastinreaktiot saadaan aikaan, Korpiola korosti.[47]

---

44 Sarvas, R. Aalto PRO, 18. TJK-luento 12.12.2022.
45 Ylitalo, J. Aalto PRO, 18. TJK-luento 26.1.2023.
46 Maula, H. Aalto PRO, 18. TJK-luento 26.1.2023.
47 Korpiola, L. Aalto PRO, 18. TJK-luento 27.1.2023.

2.6 Fyysinen turvallisuus

Securitas Oy:n toimitusjohtaja, Jarmo Mikkonen:

> *Turvallisuus on monen organisaation etu*[48].

Toimintaympäristön äkilliset muutokset ja teknologian nopea kehitys on muuttanut maailmaa, jossa turvallisuusvastuullisuus korostuu. Syvyyssuuntaista turvallisuutta toteutetaan rakenteellisella turvallisuudella, teknisellä valvonnalla ja henkilövalvonnalla. Toimitilaturvallisuudella pyritään mm. ennaltaehkäisemään, rajoittamaan, hidastamaan, ohjaamaan ja hälyttämään. Edellä mainituilla toiminnoilla on liityntä turvallisuuskulttuuriin ja imagoon. Fyysisen turvallisuuden toteuttamiseksi kaupallista tarjontaa ja ohjeita on runsaasti. Organisaatioissa työskennellään yhä enemmän joustavasti työntekijöiden ehdoilla. Kriittisissä organisaatioissa fyysiset testaukset, auditoinnit, premortem-analyysit, karttaharjoitukset, toiminnalliset ja pelilliset harjoittelut tulisi ottaa osaksi organisaatioiden omavalvontaa. Poikkeamat ovat usein positiivisia löydöksiä, joiden mukaan yrityksen toimitilaturvallisuutta voidaan parantaa, Mikkonen totesi.[48]

Fyysinen turvallisuus vaikuttaa olennaisesti yksilön kokemaan turvallisuustunteeseen ja käyttäytymiseen. Turvallisuustunne on hyvin yksilöllistä, mihin vaikuttavat mm. omat rutiinit ja ympäristö. Alanko korosti, että turvallisuuskävelyissä pielessä olevien asioiden tunnistamisen lisäksi tulee kiinnittää huomiota turvallisuutta edistäviin asioihin. Kävelyt ja kyselyt mahdollistavat osallistumisen. Alanko: ihmiset tulkitsevat fyysistä turvallisuusympäristöä eri tavalla.[49]

Waittinen totesi, että turvallisuuskulttuurin arvioimisessa turvallisuuskävelyllä on tärkeä osa. Henkilöillä on mahdollisuus liittää oma työ turvallisuuteen, tunnistamalla ympäristöstä tärkeitä henkilöturvallisuuteen liittyviä asioita esimerkiksi poistumistieopasteita. Henkilöstön osallistaminen turvallisuuskävelyn aikana on tärkeää. Käytännön harjoittelulla on tärkeä merkitys turvallisuuskulttuurin kehittämisessä, Waittinen painotti.[50]

[48] Mikkonen, J. Aalto PRO, 18. TJK-luento 17.1.2024.
[49] Alanko, M. Aalto PRO, 18. TJK-luento 17.1.2024.
[50] Waittinen, M. Aalto PRO, 18. TJK-luento 5.10.2023.

3 Näkökulmat

3.1 PV:n sidosryhmät

Kyselyyn vastaaja:

> *Valvontamalli on liiketoimintaa ja sen turvallisuuden kehittämistä tukeva toimintamalli*[51].

Erikseen valituille PV:n sidosryhmille suunnatussa sitoumuksen valvontakyvyn hallintamallin etukäteistavoitteita kartoittavan kyselyyn vastanneiden vastauksissa painottui liiketoiminnan mahdollistaminen ja tuki oikeiden toimintatapojen varmistamisessa. Vastaajien näkökulmasta sitoumuksen valvontakyvyn hallintamallin tulee edistää PV:n sidosryhmien liiketoimintaa. Laadittava toimintamalli ei saa aiheuttaa haittaa ja viivettä liiketoiminnalle. Vastaajien mielestä saavutetun turvallisuustason ylläpitämistä motivoi aktiivinen kaupallinen yhteistyö PV:n kanssa. Sitoumuksen valvontakyvyn hallintamallin tulee vastata liiketoiminnan vaatimuksiin mahdollisimman tehokkaasti. Korkea tietoturvallisuustaso koetaan vastaajien keskuudessa olevan oleellinen osa liiketoiminnan ydintä.[51]

Tietoturvallisuuteen liittyvien vaatimuksien ja Katakrin soveltamisohjeiden tulee kyselyyn vastaajien mielestä olla määrityksen mukaisesti kunnossa. Sitoumuksen valvontakyvyn hallintamalli tulisi kuvata yksiselitteisesti yritysturvallisuussopimuksen liitteessä sekä nimetä vastuutahot ja henkilöt. Sopimuskauden aikana tapahtuva tietoturvallisuustason muutokset tulee minimoida. Vastaajien näkemyksen mukaan sitoumuksen valvontakyvyn hallinta voitaisiin liittää esimerkiksi viiden vuoden välein toteutettavaan yritysturvallisuusselvitystodistuksen uusimiseen. Sitoumuksen valvontakyvyn hallintamallin tulee olla julkinen. Eräs vastaaja toi esille vaihtoehdon

[51] Lopputyön kysely 2022.

keskittyä sitoumuksen valvontakyvyn hallinnassa nykyistä enemmän muutosten ja poikkeamien selvittämiseen.[52]

Sitoumuksen valvontakyvyn hallintakokonaisuuteen koetaan liittyvän keskeisesti myös resurssit. Yritysturvallisuusselvitykset vaativat eri toimijoilta aikaa ja henkilöresursseja. Rajallisista resursseista johtuen yhteyshenkilön toteuttama valvonta saattaa jäädä joissakin sidosryhmissä vaatimattomaksi. Useampi vastaaja totesi, että prosessin kuvaus ja toteutus tulee olla tehokas. Sitoumuksen valvontakyvyn hallinnassa tulisi luottaa nykyistä enemmän yritysten itsearvioon. Sidosryhmissä tehdään jatkuvaa omavalvontaa ja toiminnan kehittämistä. Eräs vastaaja piti erinomaisena, että välillä ulkopuolinen viranomainen tulee tarkastamaan toimintaa.[52]

Vastaajat ymmärtävät PV:n tarpeen sitouttaa sidosryhmät sovittuun tietoturvallisuustasoon ja toiminnan tarkastamiseen. Vastaajien näkemyksen mukaan sitoumuksen valvontakyvyn hallintamallin tulee olla organisaation kyvykkyyttä kehittävä ja siihen tulee sitouttaa koko henkilöstö. Vastaajat haluavat sitoumuksen valvontakyvyn hallintamallin perustuvan riskiarvioon, jossa mm. kriittiset tiedot tunnistetaan ja tietoja vaihdetaan avoimesti. Huomioitavana asiana vastaajat toivat esille sitoumuksen valvontakyvyn hallinnan ulottamisen myös alihankintaketjuihin. Kokemuksen mukaan ketjuttaminen heikentää turvallisuustasoa. Sitoumuksen valvontakyvyn hallintamallin tulee kannustaa yritysten johtoa, alihankintaketjuja ja turvallisuusvastuuhenkilöitä aktiiviseen yhteistyöhön. PV:n sidosryhmissä tarkoituksenmukainen valvontatoiminta koetaan vastaajien keskuudessa olevan osa normaalia yritysturvallisuutta ja sen ylläpitämistä.[52]

Kyselyn vastauksissa painottui huoli toiminnasta, joka aiheuttaa aikatauluviiveitä ja ongelmia liiketoiminnalle. Sitoumuksen valvontakyvyn hallinnan on vastattava nopeasti muuttuviin turvallisuustilanteisiin. Toimintamallin tulee mahdollistaa säännöllinen ja nopea tietojen vaihtaminen sekä molemminpuolinen riskitietoisuuden lisääminen. Nopeasti muuttuvan toimintaympäristön takia vastaajat toivovat mahdollisimman nopeaa ja vuorovaikutteista toimintatapaa esimerkiksi tilojen tarkastuksissa tai turvallisuusilmoitusten käsittelyssä. Lopputuloksena tulee olla selkeitä ja dokumentoituja kehitysehdotuk-

[52] Lopputyön kysely 2022.

sia, jotka on laadittu tiiviissä yhteistyössä PV:n sidosryhmän kanssa. Vastaajat kokevat hyväksi toimintatavaksi, jos sidosryhmille annetaan hyviä käytänteitä (Best Practices) turvallisuustason täyttämisessä. Dokumentoidulla prosessilla varmistetaan molemminpuolinen oikeusturva ja väärinkäsityksiltä vältytään.[53]

Sitoumuksen valvontakyvyn hallintamalliin voitaisiin vastaajien näkemyksen mukaan liittää PV:n yritysturvallisuuspäivän kaltaisia ja kahdenvälisiä tiedotustilaisuuksia. Vastaajat arvostavat PV:n avointa tiedonvaihtoa ja koulutustuen tarjoamista. Se on koettu oikeiden toimintatapojen varmistamisessa tärkeäksi. Yritysturvallisuuspäiviin, auditointiin ja turvallisuussopimuksiin liittyvät koulutukset koetaan hyödyllisiksi, joiden toivotaan jatkuvan. Myös PV:n sidosryhmille suunnattu tietoturvallisuuden perusteet-verkkokurssi koetaan hyväksi. Lisäksi toivotaan riskitietoisuuden lisäämistä ja yleisiä tietoiskuja esimerkiksi häirintä- ja urkintayrityksistä.[53]

3.2 EK:n johtava asiantuntija

EK:n johtava asiantuntija totesi, että kyselyyn vastaajien esille tuomat tavoitteet ovat erinomaisia. Rajamäki koki erittäin tärkeäksi, että sitoumuksen valvontakyvyn hallintamalli perustuu kokonaisvaltaiseen riskienarvioon.[54]

Rajamäki kokee turvallisuuskriittiset organisaatiot positiivisena ja hyvänä asiana yrityksille. Yhteistyö PV:n kanssa auttaa kehittämään yritysten sisäistä turvallisuutta. Turvallisuuden parantuminen lisää liiketoimintaa myös muiden korkeaa turvallisuutta arvostavien asiakkuuksien kanssa, jos referenssinä voidaan käyttää viranomaisasiakkuuksia ja kansallista turvallisuusauditointikriteeristöä. Tämä tukee yrityksissä liiketoiminnan laajentamista ja uusien asiakkaiden saamista.[54]

Rajamäki painotti yritysten näkökulman huomioimisen tärkeyttä, kun turvallisuusratkaisuja peilataan Katakrin turvallisuustasojen täyttymiseen. Kriteeristöjä käytettäessä ja kehittämisessä tulisi aina mahdollisuuksien mukaan huomioida vaihtoehtoiset turvallisuustason toteuttamisratkaisut, jolloin kokonaisturvallisuudesta saadaan yrityksen näkökulmasta järkevä ja sen liiketoimintaa parhaiten palveleva ratkaisu. Tärkeintä tulee olla vaaditun turvallisuustason toteutuminen, eikä se, millä keinoilla se on toteutettu.

[53] Lopputyön kysely 2022.
[54] Rajamäki, M. Haastattelu 18.1.2023.

Kokonaisturvallisuuden ymmärtäminen vaatii eri turvallisuustoimijoilta toimintaympäristön hahmottamista ja osaamista.[55]

Verkostoitumisen arvo on tärkeä turvallisuustietoisuuden lisäämisessä ja parhaiten turvallisuuskäytänteiden jakamisessa. Yritysturvallisuuskentässä otetaan vastaan hyviksi koettuja toimintatapoja – tästä hyvänä esimerkkinä ja kokemuksena Rajamäki mainitsee toteutuneet PV:n yritysturvallisuuspäivät ja kahdenväliset tapaamiset. Yrityksissä arvostetaan tiedon jakamista ennakoidusti. Arviot uhkakuvista ja toimintaympäristön muutoksista antavat yrityksille aikaa valmistautumiseen ja mahdollisuuden arvioida yrityksen näkökulmasta muita perusteltuja syitä muutostarpeeseen.[55]

EK:n johtava asiantuntija, Markku Rajamäki:

> *Yhteistoiminnassa pitäisi miettiä kansakunnan etua*[55].

Rajamäki toi esille sitoumuksen valvontakyvyn hallintamallin tehokkuuden tärkeyden. Yritykset miettivät turvallisuutta taloudellisista ja henkilöresurssien käytön lähtökohdista. PV:n ja yritysten välisissä kumppanuuksissa tulee minimoida yhteistyön käynnistymisen jälkeiset muutokset. Yritysten ja eri turvallisuusviranomaisten välisen yhteistyön lisääminen vähentää mm. päällekkäisiä auditointeja ja lisää tehokkuutta. Yritykset arvostaisivat toimintatapaa, jossa heidän suostumuksella turvallisuusviranomaiset vaihtavat keskenään tietojaan. Tiedonvaihdon parantamista ja ylläpitämistä laajemmassakin mittasuhteessa tulisi miettiä. PV:n turvallisuusvaatimukset tulisi nähdä yrityksissä ja alihankintaketjuissa mahdollisuutena turvallisuuden kehittämiseen yhteistyössä johdon, vastuuhenkilöiden ja kaupallisen puolen kanssa, kun se koetaan perustelluksi.[55]

3.3 VNK:n johtava asiantuntija

VNK:n johtava asiantuntija piti yritysturvallisuusselvitystodistuksien saamista ja henkilöturvallisuusselvityksien laatimista yrityksille mahdollisuutena päästä kilpailutuksiin. Kansainvälisille markkinoille pääsemisessä yrityksen kyvykkyys käsitellä ja säilyttää kansainvälisesti suojattavaa tietoa voi olla jopa elinehto. Turvallisuusjärjestelyt lisäävät kustannuksia, mutta

[55] Rajamäki, M. Haastattelu 18.1.2023.

annetulla yritysturvallisuusselvitystodistuksella yritys pääsee markkinoille, joissa se ei ole aiemmin ollut.[56]

Yritysten tekemä itsearvio on lähtökohta turvallisuusvaatimusten sisäistämiseksi: hallinnollisten turvallisuusmenettelyiden kuten riskienhallinnan ja vastuiden jakaantumisen arvioimiseksi, fyysisen turvallisuuden kuten avaintenhallinnan ja turvallisuusluokiteltujen asiakirjojen käsittelyn ohjeistamisen riittävyyden arvioimiseksi. Hyviksi koettuja toimintatapoja tulee Pallaspuron mielestä toteutuksessa ehdottomasti hyödyntää. Kasvaviin turvallisuuskustannuksiin vastataan organisaatioissa tekemällä perustyö riittävällä tarkkuudella, ja siihen voidaan käyttää tarvittaessa ulkopuolisia konsultteja. Lopulta ulkopuolinen taho tulee todentamaan paikan päälle turvallisuusohjeiden ja järjestelyiden olemassaolon sekä sitoutumisen tason. Pallaspuro piti tärkeänä, että sitoumuksen valvontakyvyn hallinta perustuu riskiarvioon ja toimenpiteitä tulee peilata suojattavaan tietoon! Sitoumuksen valvontakyvyn hallintamalli on esille tuotujen vaatimuksien hallintaa. Sitoumuksen valvontakyvyn hallintamallista voisi laatia kaksisivuisen ohjeen.[56]

Kilpailutukseen lähdettäessä henkilöturvallisuusselvitysmenettelyn kesto on otettava suunnittelussa huomioon. Toiminnassa korostuvat myös oikeiden henkilöiden valinta ja sijaisuusjärjestelyt. Henkilöstön suuri vaihtuvuus saattaa aiheuttaa ongelmia organisaatiossa. Tätä tulisi hallita organisaatiossa, jossa on tehtävien hoitajia.[56]

VNK:n johtava asiantuntija, Juha Pallaspuro:

Vastuut tulee sitoa organisaatioon ja siellä vastuuhenkilöihin[56].

Pallaspuro kommentoi turvallisuusresurssien rajallisuutta. Organisaation riskiarvioinnin perusteella tunnistetaan riskit ja ne asetetaan tärkeysjärjestykseen. Lopulta laaditaan suunnitelma keskeisimpien riskien hallitsemiseksi. Tarvittaessa laaditaan useampivuotinen suunnitelma ja päätöksenteon jälkeen sidotaan riittävät resurssit haavoittuvuuksien pienentämiseksi. Vastuuhenkilöiden on ymmärrettävä vaatimukset ja he ovat vastuussa niiden käytäntöön viemisessä.[56]

[56] Pallaspuro, J. Haastattelu 3.2.2023.

Turvallisuusvastuiden ketjuttaminen heikentää turvallisuutta – Pallaspuro korosti, että sopimusosapuoli on vastuussa ja käytännöt on ulotettava alihankintaketjuihin. Myös alihankintaketjujen henkilöstöltä edellytetään turvallisuussopimuksiin sitoutumista. Turvallisuussopimuksessa organisaatio on velvollinen perehdyttämään ja kouluttamaan alihankkijan turvallisuussopimuksen mukaisiin asiakokonaisuuksiin ja henkilöstöturvallisuusmenettelyyn. Perustyön jälkeen viranomainen ulottaa todentamisen alihankintaketjuun.[57]

Turvallisuustietoisuuden lisäämisessä Pallaspuro pitää digitaalisesti toteutettuja koulutusmateriaaleja kannatettavina ja hyvinä. Toteutuksen tulisi mahdollistaa myös kurssin suorituksen seurannan.[57]

Turvallisuustilannekuvan muodostaminen ja jakaminen ovat kehitettäviä asioita – hyvänä esimerkkinä Pallaspuro mainitsi Traficomin turvallisuustilannekuvan, ja siinä ilmoitusten tekemisen ja havaintojen jakamisen. Vastaavaa ei turvallisuuden osalta ole ja siihen Pallaspuron mielestä on laajempi tarve. Toteutustavan tulee olla mahdollisimman yksinkertainen, selkeä, helppo ja digitalisoitu. Turvallisuushankkeissa on tärkeä, että sopimusosapuolten kesken voidaan helposti olla myös ennakkoon yhteydessä. Aktiivinen yhteistyö edellyttää sopimista myös välittömästi ilmoitettavien asioiden osalta.[57]

VNK:n johtava asiantuntija, Juha Pallaspuro:

Asiakastietojen suojaaminen on turvallisuuden perusasioita[57].

Pallaspuro: Asiakastietojen suojaaminen huomioidaan organisaation hallinnollisessa turvallisuudessa. Useita luottamuksellisia asiakastietoja käsittelevän organisaation sisäisissä ohjeissa korostuu tilaan ja tietoon pääsyn eriyttäminen. Kun hallinnolliset ohjeet, käsittely- ja kulkuoikeudet ovat organisaatiossa kunnossa, ei sitoumuksen hoitokyvyn arvioinnin aikana ole pääsyä muihin asiakastietoihin, Pallaspuro totesi.[57]

[57] Pallaspuro, J. Haastattelu 3.2.2023.

3.4 PE:n valmiuspäällikkö

PE:n valmiuspäällikkö, lippueamiraali Janne Huusko:

Turvallisuus on olennainen osa toimintakulttuuria[58].

Huusko painotti, että laadittavan sitoumuksen valvontakyvyn hallintamallin tulee lisätä monitahoisesti luottamusta ja sen tulee olla ymmärrettävä. Valvonnan tulee olla oikein kohdennettu. Läpileikkaavassa toiminnassa huomioidaan yksilö- ja organisaatiotasot sekä näihin vaikuttavat tekijät.[58]

Huusko totesi, että organisaatio tietää omat tehtävät ja tavoitteet sekä käytössä olevat resurssit. Sisäinen valvonta on organisaation johdon tukena, jotta voidaan varmistua toiminnan riittävästä tasosta. Organisaatiot hoitavat päivittäin valvontaa ja sisäinen valvonta tekee tarkastuksia.[58]

Sitoumuksen valvontakyvyn hallinnassa luottamusta ylläpidetään kahteen suuntaan – sidosryhmät huolehtivat valvonnasta omalta osaltaan ja PV omalta osaltaan. Turvallisuusluokitelluissa hankkeissa mukana olevat yritykset ovat etulinjassa, kun yhteistyötä tehdään alihankkijoiden kanssa.[58]

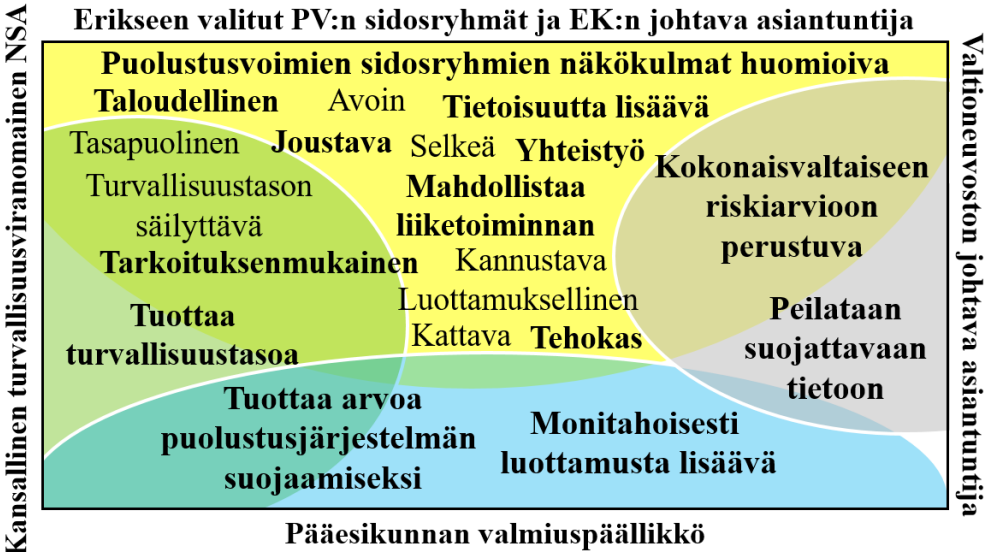
3.5 Kansallinen turvallisuusviranomainen NSA

Ulkoministeriössä toimivan kansallisen turvallisuusviranomaisen (National Security Authority, NSA) tehtävänä on kansainvälisen tietoturvallisuusvelvoitelain mukaisesti ohjata ja valvoa, että Suomelle toimitettu kansainvälinen turvallisuusluokiteltu tieto suojataan ja sitä käsitellään asianmukaisesti. Suojaus- ja käsittelyohjeet perustuvat velvoitteisiin, joita Suomella on sekä EU:n turvallisuussääntöjen, että kahden- ja monenvälisten tietoturvallisuussopimusten johdosta. Sopimukset luovat puitteet Suomelle ja suomalaisyrityksille osallistua hankkeisiin, jotka edellyttävät turvallisuusluokitellun tiedon vaihtamista. Puolustusministeriö, PE ja Supo toimivat määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA), joille on jaettu omat vastuualueet kansallisen turvallisuusviranomaisen kokonaisvastuukentästä.[59]

[58] Huusko, J. Haastattelu 26.5.2023.
[59] Ulkoministeriö. Kansallinen turvallisuusviranomainen. 2023.

Kansallinen turvallisuusviranomainen NSA totesi, että on kansallinen intressi mahdollistaa yritysten osallistuminen turvallisuusluokiteltuja tietoja sisältäviin hankkeisiin ja turvata tietojen uskottava käsittely. Vaadittujen turvallisuustasojen ja yhteisten kriteeristöjen käyttäminen vaikuttaa tasapuolisuuden toteutumiseen. NSA:n näkökulmasta sitoumuksen valvontakyvyn hallintamallin täytyy olla tarkoituksenmukainen, joka tuottaa turvallisuustasoa.[60]

3.6 Yhteenveto näkökulmista



KUVA 3. Neljä näkökulmaa sitoumuksen valvontakyvyn hallintaan.

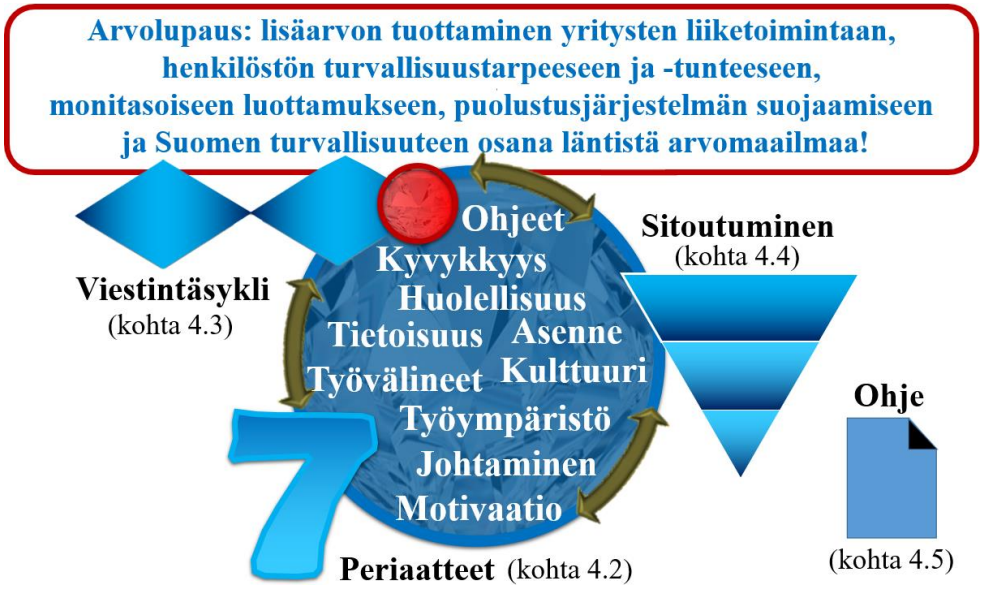
Erikseen valitut PV:n sidosryhmien edustajat ja EK:n johtava asiantuntija painottavat sitoumuksen valvontakyvyn hallintamalliin liittyen mm. seuraavia näkökulmia: PV:n sidosryhmien näkökulmat huomioiva, kokonaisvaltaiseen riskiarvioon perustuva, mahdollistaa liiketoiminnan, tehokas, tarkoituksenmukainen, yhteistyötä lisäävä ja joustava. VNK:n johtava asiantuntija painottaa kokonaisvaltaisen riskiarvion ja suojattavaan tietoon peilaamisen tärkeyttä. PE:n valmiuspäällikkö korostaa monitahoisen luottamuksen lisäämistä. Kansallinen turvallisuusviranomainen NSA korosti tarkoituksenmukaisuutta, tasapuolisuutta ja turvallisuustason tuottamista. PV:n sidosryhmien ja asiantuntijoiden näkökulmat ovat yhdensuuntaisia ja ne mahdollistavat tarkoituksenmukaisen sitoumuksen valvontakyvyn hallintamallin laatimisen. Liitteenä 2 on turvallisuusmuotoilun Customer Grouping ja liitteenä 3 on Insight.

[60] Kaukoranta, P. Haastattelu 28.2.2023.

4 Sitoumuksen valvontakyvyn hallintamalli

4.1 Hallintamalli

Sitoumuksen valvontakyvyn hallintamalli mahdollistaa yritysturvallisuusselvitystodistuksen sitoumuksen hoitokyvyn ja siinä tapahtuvien muutoksien arvioinnin. Sitoumuksen valvontakyvyn hallintamalli perustuu monitasoiseen luottamukseen. PV:n sidosryhmät ja alihankkijat vastaavat omasta riskienhallinnasta. Yrityksessä päätöksen hallintamallin hyödyntämisestä tekee yritysturvallisuusselvityssopimuksessa nimetty vastuuhenkilö. Toiminnan tarkoituksenmukaisuus ja tehokkuus saavutetaan yrityksen johdon ohjauksessa. Yritysten vastuulla on huomioida alihankkijoiden kanssa sopimuksellisesti sitoumuksen valvontakyvyn hallinnan toteutuminen. Yritys käsittelee valvontatulokset liiketoiminnallisista lähtökohdista. Toimivaltainen viranomainen ja määrätty turvallisuusviranomainen arvioivat yritykselle myönnetyn yritysturvallisuusselvitystodistuksen sitoumuksen hallintakykyä ja siinä tapahtuvia muutoksia osana puolustusjärjestelmän suojaamista.



KUVA 4. Sitoumuksen valvontakyvyn hallintamalli.
(Liitteenä 4 on turvallisuusmuotoilun Rational Concept Sheet.)

Sitoumuksen valvontakyvyn hallintamalli muodostuu kolmesta toistensa kanssa vuorovaikutuksessa olevasta osasta: seitsemästä toimintaperiaatteesta, viestintäsyklistä ja sitouttamisesta. Tavoitteena on tuottaa lisäarvoa yritysten liiketoimintaan, henkilöstön turvallisuustarpeeseen ja -tunteeseen, monitasoiseen luottamukseen, puolustusjärjestelmän suojaamiseen ja Suomen turvallisuuteen osana läntistä arvomaailmaa! PV:n sidosryhmien ja alihankkijoiden henkilöstöllä on keskeinen rooli arvolupauksen tuottamisessa.

PV:n sidosryhmän henkilöstön turvallisuustarpeiden ja -tunteiden selvittäminen on tärkeää lisäarvon tuottamisessa. Tunnepohjaisella turvallisuusjohtamisella ja -viestinnällä vaikutetaan koko henkilöstön sitoutumisen tasoon. Haasteellisissakin kulttuureissa oikein valittu viestintätyyli saa aikaan tunnejäljen, millä on positiivinen vaikutus turvallisuuteen. Organisaatioiden tavoitteiden ja visioiden saavuttamiseksi henkilöstön sitoutuminen on tärkeää. Henkilöstön turvallisuustarpeiden ja -tunteiden taso kartoitetaan ja arvioidaan sitouttamisperusteisen johtamistoiminnan mahdollistamiseksi. Arvioitavat osa-alueet ovat: tietoisuus, huolellisuus, kyvykkyys, asenne, motivaatio, ohjeet, työvälineet, työympäristö, kulttuuri ja johtaminen.

Toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen tuki PV:n sidosryhmälle liittyy annetun yritysturvallisuusselvitystodistuksen sitoumuksen valvontakyvyn hallintaan ja siinä tapahtuvien muutosten arviointiin. Yhteistyössä mahdollistetaan puolustusjärjestelmän suojaaminen, esim. yritysturvallisuusselvitystodistuksen uusiminen ja siten liiketoiminnan turvallinen jatkuminen PV:n kanssa.

4.2 Periaatteet

Sitoumuksen valvontakyvyn hallintaa ohjaavat periaatteet ovat:

1. ***Kokonaisvaltainen riskienhallinta***

Kokonaisvaltaisessa riskienhallinnassa sitoumuksen hallintakyvyn tasoa ja siinä tapahtuvia muutoksia arvioidaan ja säädellään PV:n sidosryhmissä ja alihankkijoissa liiketoiminnallisista lähtökohdista osana puolustusjärjestelmän suojaamista ja Suomen turvallisuutta.

2. ***Henkilöstön turvallisuustarpeet ja -tunteet***

PV:n sidosryhmien ja alihankkijoiden henkilöstön turvallisuustarpeet ja -tunteet asetetaan keskiöön arvolupauksen tuottamiseksi. Toimintaympäristöstä arvioidaan tietoisuus, huolellisuus, kyvykkyys, asenne, ohjeet, motivaatio, työvälineet, työympäristö, kulttuuri ja johtaminen.

3. ***Avoin ja luottamuksellinen viestintä***

Avoimessa ja luottamuksellisessa viestinnässä on käytössä parhaat saatavilla olevat tiedot ja kokemus. Viestintä vaikuttaa mm. kokonaisvaltaisen riskiarvion laatimiseksi tarvittavien kruunun tietojen, niihin kohdistuvien riskien ja suojaamistoimenpiteiden tunnistamiseen.

4. ***Koko henkilöstöä tunnetasolla sitouttava***

Henkilöstö sitoutetaan tunnetasolla turvallisuusviestinnän ja -johtamisen keinoin sitoumuksen valvontakyvyn jatkuvaan seurantaan, suunnitteluun, päätöksentekoon, toteutukseen, kehittämiseen, tietoisuuden lisäämiseen ja ylläpitoon.

5. ***Arvolupauksen tuottaminen***

Sitoumuksen valvontakyvyn hallinta tuottaa lisäarvoa PV:n sidosryhmien ja alihankkijoiden liiketoimintaan, henkilöstön turvallisuustarpeeseen, monitasoiseen luottamukseen, puolustusjärjestelmän suojaamiseen ja Suomen turvallisuuteen osana läntistä arvomaailmaa. Yhdessä laaditut riskienhallintakontrollit ovat kustannustehokkaita.

6. ***Riskienhallintapäätökset***

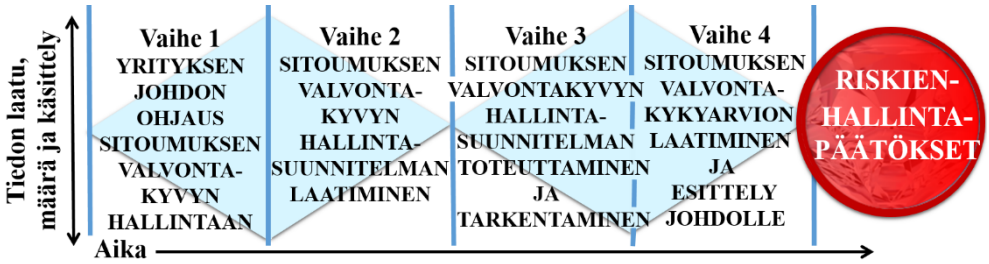
PV:n sidosryhmille ja alihankkijoille tuotetaan analysoituun tietoon perustuvia dokumentoituja suosituksia uskottavan sitoumuksen hallintakyvyn resilienssin varmistamiseksi.

7. ***Riskien jatkuva arviointi, ilmoittaminen ja oppiminen***

PV:n sidosryhmissä ja alihankkijoissa sitoumuksen hoitokyvyn riskitasoa ja siinä tapahtuvia muutoksia arvioidaan jatkuvasti sekä ryhdytään tarvittaessa sopimuksenmukaisiin toimenpiteisiin.

4.3 Viestintäsykli

Sitoumuksen valvontakyvyn hallintamallin viestintäsykli auttaa käsittelemään tietoa oikea-aikaisesti ja luottamuksellisesti. Eri vaiheiden aikana fasilitoijalla on keskeinen rooli avoimen ja luottamuksellisen keskusteluilmapiirin luomisessa sekä annettujen resurssien tehokkaassa käytössä.



KUVA 5. Sitoumuksen valvontakyvyn hallintamallin viestintäsykli.

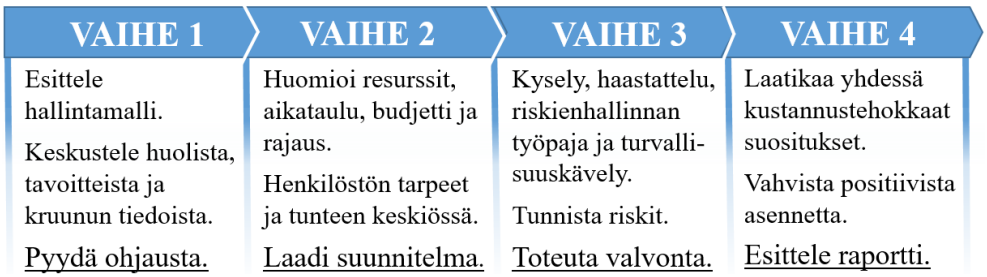
Viestintäsykli muodostuu neljästä loogisesti toisiinsa liittyvästä vaiheesta. Viestintäsyklin eri vaiheisiin vaikuttaa käytettävissä olevan tiedon laatu, määrä ja sen käsittely. Kiireellisessä tilanteessa viestintäsykli toteuttamaan vuorokaudessa. Kiireettömissä tilanteissa viestintäsykli on pitempi, riippuen tehtävänannon laajuudesta, aikataulusta ja resursseista. Viestintäsyklin vaiheiden läpikäyminen tuottaa yrityksen johdolle tilannekuvan riskienhallintapäätöksentekoa varten.

4.4 Sitoutuminen

Sitoutuminen sitoumuksen valvontakyvyn hallintaan ja siinä tapahtuvien muutosten ilmoittamiseen mahdollistetaan aktiivisella ja osallistavalla yhteistyöllä. Vaikuttavan yhteistyön edellytyksenä on monitasoiset luottamukselliset suhteet. Turvallisessa keskusteluilmapiirissä kulttuuria kehitetään positiivisuuden kautta ilman syyllistävää ilmapiiriä. Tavoitteena on innostaa ja osallistaa henkilöstö tunnetasolla sitoumuksen hoitokyvyn jatkuvaan seurantaan, suunnitteluun, päätöksentekoon, toteutukseen, kehittämiseen, tietoisuuden lisäämiseen ja ylläpitoon. Sitoutuminen perustuu ymmärrykseen henkilöstön turvallisuustarpeista ja -tunteista. Onnistumisen ratkaisee se, kuinka kaikilla organisaation tasoilla henkilöstön sitoutuminen on linjassaan organisaation johdon päätöksenteon kanssa. Henkilöstön on tiedettävä oman työn merkitys osana organisaation tavoitteita ja visiota.

4.5 Ohje

Ohje auttaa organisaation vastuutahoja ja henkilöitä hyödyntämään konkreettisesti sitoumuksen valvontakyvyn hallintamallia yrityksen toimintaympäristössä. Fasilitoijalta edellytetään avointa ja aktiivista yhteistyötä sekä sitoumuksen valvontakyvyn hallintamallin omaksumista.



KUVA 6. Ohje sitoumuksen valvontakyvyn hallintamallin hyödyntämiseen. (Vaiheet ovat samat kuin viestintäsyklissä.)

Yrityksen johdolle esitellään sitoumuksen valvontakyvyn hallintamalli ja pyydetään ohjausta. Yrityksen johdon tavoitteet ja huolet selvitetään sekä kruunun tiedoista keskustellaan. Johdon näkökulma ohjaa ja rajaa sitoumuksen valvontakyvyn hallintatyön yrityksen näkökulmasta tarkoituksenmukaiseksi riskienhallintatyöksi, jossa huomioidaan kansallinen turvallisuus.

Toisessa vaiheessa laaditaan suunnitelma sitoumuksen valvontakyvyn hallinnan toteuttamiseksi. Toiminnan tulee olla linjassa johdolta saadun ohjauksen kanssa. Sitoumuksen valvontakyvyn hallintasuunnitelma sisältää perusajatuksen henkilöstön turvallisuustarpeiden ja -tunteiden mittaamiseksi. Laaditun suunnitelman merkitys yrityksen liiketoiminnalle ja puolustusjärjestelmän suojaamiselle on ymmärrettävä.

Kolmannessa vaiheessa sitoumuksen valvontakyvyn hallintaa toteutetaan suunnitelman mukaan. Turvallisuustarpeita ja -tunteita mittaavaan kyselyyn tulisi riittävän otannan saamiseksi osallistua anonyymisti vähintään 25 henkilöä (liite 5). Kyselyn tuloksia käsitellään riskienhallinnan työpajassa. Riskienhallinnan työpajatyöskentely on tehokasta 4-6 henkilön ryhmässä ja siihen on hyvä varata aikaa 3-5 tuntia. Osallistuminen tulisi perustua vapaaehtoisuuteen. Osallistujien valinnassa tulisi huomioida henkilösuhteet ja esimiesroolit. Työskentelyssä korostuu luottamuksellinen ja avoin keskuste-

luilmapiiri. Työpajassa keskustellaan kruunun tiedoista ja niihin kohdistuvista riskeistä, jonka jälkeen havaintoja peilataan henkilöstön turvallisuustarpeisiin ja -tunteisiin. Samalla esitetään tarkentavia kysymyksiä ja selvitetään syy-seuraussuhteet. Lopuksi suoritetaan turvallisuuskävely, jonka aikana tehdään havaintoja ja keskustellaan turvallisuuskulttuurista.

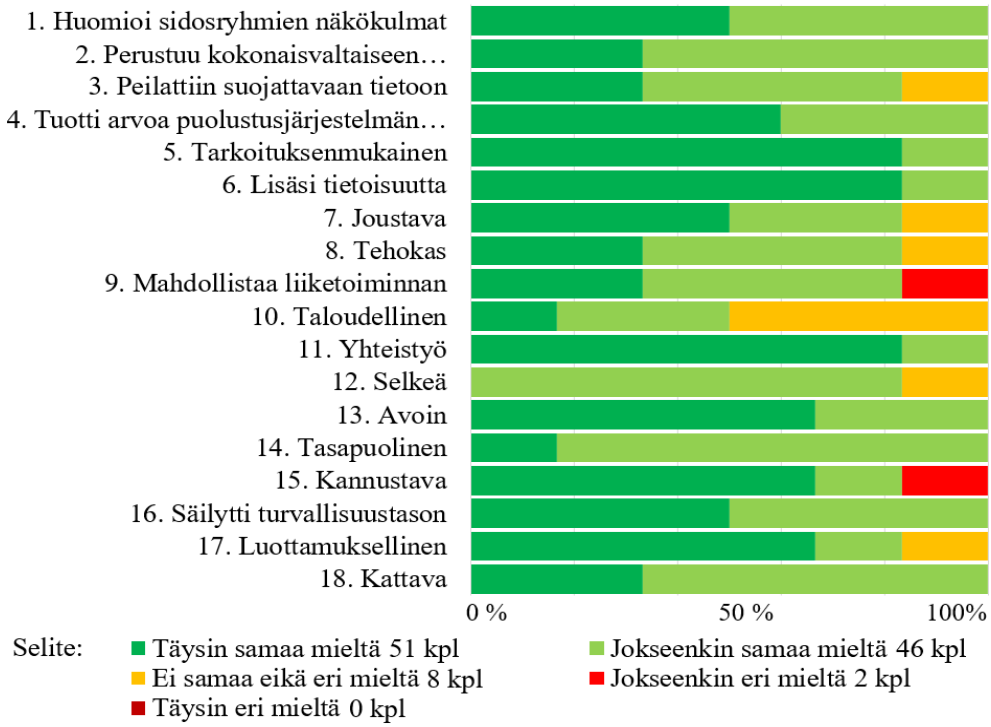
Neljännessä vaiheessa laaditaan johdolle tilannekuva päätöksentekoa varten. Havainnot dokumentoidaan tarkoituksenmukaisella tavalla jatkokäsittelyn mahdollistamiseksi. Liitteenä 6 on esimerkkipohja turvallisuustarpeiden ja -tunteiden dokumentoimiseksi. Dokumentaation laadinnassa hyödynnetään yrityksen riskienhallinnan ohjeistusta. Kustannustehokkaat suositukset esitellään yrityksen johdolle. Samalla mahdollistetaan tarkentavien kysymysten esittäminen. Riskien tunnistaminen, riskiluokan määrittäminen, kustannustehokkaiden jatkotoimenpidesuosituksien laatiminen, liiketoiminnan ja puolustusjärjestelmän suojaamisen näkökulmien huomioiminen, yritysjohdon päätökset, vastuutahojen ja henkilöiden tunnistaminen, resurssien arvioiminen, budjetointi, tavoiteaikataulun asettaminen ja seurannan huomioiminen helpottavat jatkokäsittelyä.

5 Evaluointi

5.1 Näkökulmien huomioiminen

Asiantuntijat arvioivat liitteellä 7, kuinka näkökulmat huomioitiin sitoumuksen valvontakyvyn hallintamallissa[61].

TAULUKKO 2. Näkökulmien huomioimisen tulokset[61].



Tulosten perusteella sitoumuksen valvontakyvyn hallintamalli täytti parhaiten seuraavat tavoitteet: tarkoituksenmukainen, lisää tietoisuutta ja yhteistyötä. Suurin hajonta oli liiketoiminnan mahdollistamisessa ja kannustavuudessa. Kokonaisuudessaan asiantuntijat olivat 90 prosenttisesti joko täysin tai jokseenkin samaa mieltä, että näkökulmat huomioitiin sitoumuksen valvontakyvyn hallintamallissa.

[61] Nykänen, R. ja Räsänen, I. Haastattelut 5.4.2023; Rajamäki, M. ja Nurminen, K. Haastattelut 24.4.2023; Korhonen, P. Haastattelu 1.11.2023; Rasila, T. Haastattelu 15.1.2024.

5.2 Periaatteiden painoarvovertailu

Asiantuntijat asettivat sitoumuksen valvontakyvyn hallintamallin seitsemän periaatetta tärkeysjärjestykseen[62].

TAULUKKO 3. Periaatteiden painoarvovertailun (Weighted Ranking) tulokset[62].

Järj.	Pist.	SEITSEMÄN PERIAATETTA		1	2	3	4	5	6	7
1	24	Kokonaisvaltainen riskienhallinta	1		5	3	4	3	5	4
5	15	Henkilöstön turvallisuustarpeet ja -tunteet	2	1		3	4	4	2	1
6	14	Avoin ja luottamuksellinen viestintä	3	3	3		4	1	2	1
7	12	Koko henkilöstöä tunnetasolla sitouttava	4	2	2	2		1	2	3
2	22	Arvolupauksen tuottaminen	5	3	2	5	5		4	3
4	17	Riskienhallintapäätökset	6	1	4	3	4	2		3
3	19	Riskien jatkuva arviointi, ilmoittaminen ja oppiminen	7	2	5	3	3	3	3	

Periaatteiden tärkeysjärjestys:

1. Kokonaisvaltainen riskienhallinta.
2. Arvolupauksen tuottaminen.
3. Riskien jatkuva arviointi, ilmoittaminen ja oppiminen.
4. Riskienhallintapäätökset.
5. Henkilöstön turvallisuustarpeet ja -tunteet.
6. Avoin ja luottamuksellinen viestintä.
7. Koko henkilöstöä tunnetasolla sitouttava.

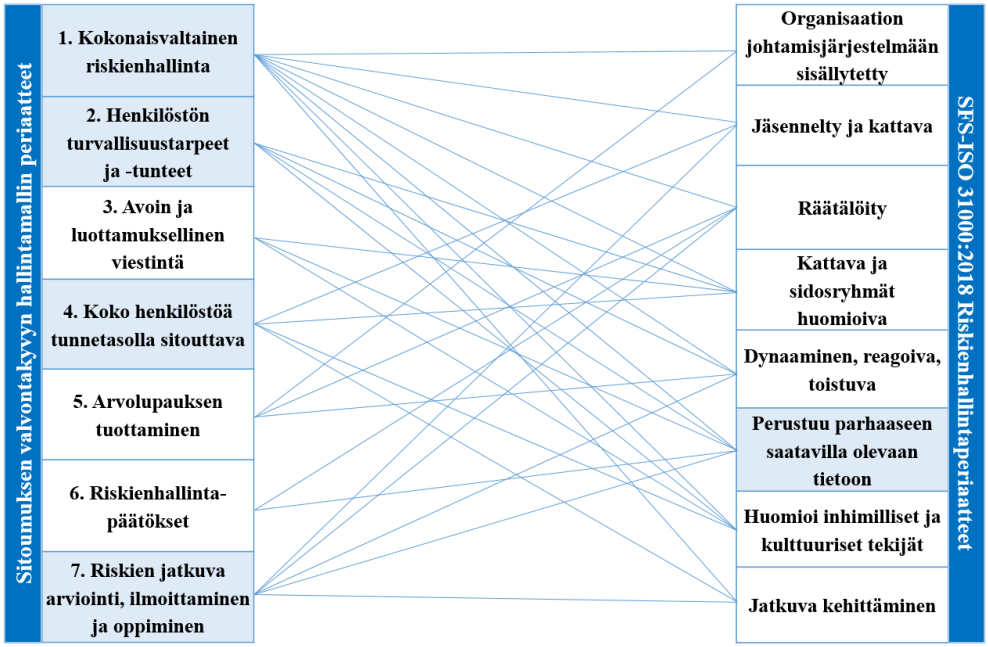
Tuloksissa korostui kolme periaatetta muita enemmän: 1. kokonaisvaltainen riskienhallinta ja 2. arvolupauksen tuottaminen sekä 3. riskien jatkuva arviointi, ilmoittaminen ja oppiminen. Kokonaisvaltainen riskienhallinta on sitoumuksen valvontakyvyn hallintamallin lähtökohta, jota toteutetaan arvolupauksella. Edellä mainittujen periaatteen mukaisesti toteutetaan kolmanneksi tärkeimmäksi arvioitua periaatetta: riskien jatkuva arviointi, ilmoittaminen ja oppiminen.

[62] Nykänen, R. ja Räsänen, I. Haastattelut 5.4.2023; Rajamäki, M. ja Nurminen, K. Haastattelut 24.4.2023; Korhonen, P. Haastattelu 1.11.2023; Rasila, T. Haastattelu 15.1.2024.

5.3 Periaatteiden vertailu

Asiantuntijat vertasivat sitoumuksen valvontakyvyn hallintamallin periaatteita ISO 31000 riskienhallinnan periaatteisiin[63].

TAULUKKO 4. Periaatteiden vertailun tulokset[63].



Tuloksissa korostuivat:

- 1. Kokonaisvaltainen riskienhallinta.
- 7. Riskien jatkuva arviointi, ilmoittaminen ja oppiminen.
- 2. Henkilöstön turvallisuustarpeet ja -tunteet.
- 4. Koko henkilöstöä tunnetasolla sitouttava.

Sitoumuksen valvontakyvyn hallintamallin vertaaminen ISO 31000 riskienhallintastandardiin korosti kokonaisvaltaisen riskienhallintaperiaatteen tärkeyttä. Toisena korostui riskien jatkuva arvioiminen, ilmoittaminen ja oppiminen. Kolmanneksi eniten yhtymäkohtia ISO 31000 riskienhallintaperiaatteisiin oli periaatteilla: 2. henkilöstön turvallisuustarpeet ja –tunteet sekä 4. koko henkilöstöä tunnetasolla sitouttava. Kaikilla seitsemällä periaatteilla oli kaksi tai useampi yhtymäkohtaa riskienhallintastandardiin.

[63] Nykänen, R. ja Räsänen, I. Haastattelut 5.4.2023; Rajamäki, M. ja Nurminen, K. Haastattelut 24.4.2023.

5.4 Asiantuntija-arvio

Asiantuntijat arvioivat sitoumuksen valvontakyvyn hallintamallin vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia[64].

TAULUKKO 5. Asiantuntijoiden yhdistetty SWOT-arvio[64].

Vahvuudet	Heikkoudet
- Tehokkuus on huomattava. - Henkilöstönäkökulman huomioiminen. - Prosessi on hyvin kuvattu. - Hallinnollisesti prosessin käynnistäminen vaatii vain vähän työtä. - Suunnitelmaa laadittaessa riskienhallinnan työpajan henkilövalinta tunnistettiin tärkeäksi asiaksi. - Riskienhallinnan työpajaan ei osallistunut johdon edustajaa. - Riskienhallinnan työpajan rakennetta pidettiin hyvänä ja keskusteluilmapiiri koettiin avoimeksi. - Riskienhallinnan työpajatyöskentelyssä erityisen hyvänä pidettiin asioiden läpikäyntiä yhdessä. - Kattava ja moniulotteinen.	- Toteutus vaatii organisaatiolta osaamista ja kypsyystasoa. - Kruunun tiedot tulee kuvata laajemmin ennen kyselyn ja riskienhallinnan työpajan toteutusta. - Toteutus ratkaisee sitoumuksen valvontakyvyn hallintamallin taloudellisuuden, tehokkuuden ja joustavuuden tason.
Mahdollisuudet	**Uhkat**
- Mahdollistaa poikkeamien havainnointikyvyn ja jatkossa trendien seurannan. - Henkilöstötasolla mahdollistaa oppimisen ja kyvykkyyden kehittymisen. - Sopeutettavuus suojattavaan tietoon. - Turvallisuuden kehittämiseksi tarvitaan organisaatiokohtaisten tavoitteiden asettamista ja mittareiden valitsemista. - Mahdollisuus nostaa turvallisuustasoa ulkopuolisen konsultin tuella. - Mahdollistaa laajemmin sisäisesti positiivisen turvallisuuskulttuurin kehittämisen. - Riskienhallinnan työtyhmän voi jakaa kahteen osaan ja vertailla tuloksia. - Yhdenmukainen näkemys työpajatyöskentelyn jälkeen.	- Uskaltaako kaikki henkilöt tuoda kyselyssä ja riskienhallinnan työpajatyöskentelyssä omia näkökulmia avoimesti esille? - Painotetaanko johdon esittelyssä riittävästi soveltamista ja PV-kontekstia? - Toteutus edellyttää osaamista ja samanlaista näkemystä asiaan. - Mitataanko oikeita asioita ja ymmärrämmekö turvallisuustapahtumien taustalla olevat syy-seuraussuhteet? - Toteutuuko olennaiset sitoumuksen valvontakyvyn turvallisuusvaatimukset? - Ovatko tulokset yhdenmukaisia? - Kattavuuden ja avoimuuden seurauksena selkeys voi kärsiä. - Tunnistetaanko kruunun tiedot?

[64] Nykänen, R. ja Räsänen, I. Haastattelut 5.4.2023; Rajamäki, M. ja Nurminen, K. Haastattelut 24.4.2023; Heinonen, H. Haastattelu 8.6.2023; Korhonen, P. Haastattelu 1.11.2023; Rasila, T. Haastattelu 15.1.2024.

Arvion mukaan sitoumuksen valvontakyvyn hallintamalli vaatii organisaatiolta kypsyystasoa ja fasilitoijalta osaamista. Esimerkiksi riskienhallinnan työpajaan osallistuneiden henkilöiden valinta on tärkeää, kuten myös prosessin alkuvaiheessa tarkemman kuvauksen laatiminen kruunun tiedoista. Lopulta toteutus ratkaisee mm. toiminnan taloudellisuuden, joustavuuden ja tehokkuuden. Sitoumuksen valvontakyvyn hallintamalli mahdollistaa laajemmin yrityksen sisäisen turvallisuuskulttuurin kehittämisen ja seurannan.

5.5 Yhteenveto evaluoinnista

Yhdistetyssä asiantuntia-arviossa sitoumuksen valvontakyvyn hallintamallia pidetään tarkoituksenmukaisena, tietoisuutta ja yhteistyötä lisäävänä. Periaatteiden vertailu korostaa kokonaisvaltaista riskienhallinnan tärkeyttä ja arvolupauksen tuottamista sekä riskien jatkuvaa arviointia, ilmoittamista ja oppimista. Periaatteiden vertaaminen ISO 310000 riskienhallintaperiaatteisiin korostaa myös kokonaisvaltaista riskienhallintaa ja koko henkilöstön sitouttamisen tärkeyttä tunnetasolla.

Evaluoinnissa hallintamallin tehokkuutta pidetään huomattavana ja prosessia hyvin kuvattuna. Riskienhallinnan työpajan keskusteluilmapiiri arvioidaan avoimeksi ja rakenteeltaan hyväksi. Toteutus edellyttää fasilitoijalta toimintamallin sisäistämistä ja osaamista. Sitoumuksen valvontakyvyn hallintamalli mahdollistaa esimerkiksi riskien havaitsemisen ja turvallisuuden kehittämisen niin yksilö- kuin organisaatiotasolla. Liitteenä 8 on turvallisuusmuotoilun Concept Sheet ja liitteenä 9 on Minimum ~~Viable~~ Lovable Product.

6 Johtopäätökset

Puolustusjärjestelmän suojaamiseksi lopputyön tavoitteena oli laatia sitoumuksen valvontakyvyn hallintamalli, mikä velvoittaa ja osallistaa PV:n sidosryhmät sitoumuksen valvontakyvyn hallintaan. Lopputyön pääkysymys: miten toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen tulisi osana puolustusjärjestelmän suojaamista, turvallisuusselvityslain (726/2014) 40 §:n mukaisesti valvoa yritykselle myönnetyn yritysturvallisuusselvitystodistuksen sitoumuksen hoitokykyä ja siinä tapahtuvia muutoksia? Laadittu sitoumuksen valvontakyvyn hallintamalli muodostuu seitsemästä johtamisperiaatteesta, viestintäsyklistä, henkilöstön sitouttamisesta ja käytännön ohjeesta. Sitoumuksen valvontakyvyn hallintamallin arvolupaus: lisäarvon tuottaminen yritysten liiketoimintaan, henkilöstön turvallisuustarpeeseen ja -tunteeseen, monitasoiseen luottamukseen, puolustusjärjestelmän suojaamiseen ja kansalliseen turvallisuuteen osana läntistä maailmaa. Arvolupauksen tuottamiseksi henkilöstön inhimilliset turvallisuustarpeet ja -tunteet ovat tärkeitä: tietoisuus, huolellisuus, kyvykkyys, asenne, motivaatio, ohjeet, työvälineet, työympäristö, kulttuuri ja johtaminen.

Lopputyön alakysymys: mitkä ovat PV:n sidosryhmien tavoitteet ja huolet laadittavaan sitoumuksen hoitokyvyn valvontamalliin liittyen? Näkökulmat kartoitettiin kyselyllä ja haastatteluilla erikseen valituilta PV:n sidosryhmiltä, EK:n yritysturvallisuuden johtavalta asiantuntijalta, Kansalliselta turvallisuusviranomaiselta NSA, PE:n valmiuspäälliköltä ja VNK:n johtavalta asiantuntijalta. Vastausten perusteella sitoumuksen valvontakyvyn hallintamallin tulee perustua PV:n sidosryhmien näkökulmien huomioimiseen, turvallisuustason tuottamiseen, kokonaisvaltaiseen riskienarviointiin, tarkoituksenmukaisuuteen, monitahoiseen luottamukseen ja arvon tuottamiseen puolustusjärjestelmän suojaamiseksi. PV:n sidosryhmien ennakkohuolet liittyvät liiketoiminnalle ongelmia ja aikatauluviiveitä aiheuttavaan toimintaan. Sitoumuksen valvontakyvyn hallintamalli laadittiin esille tuodut näkökulmat huomioiden.

Toinen alakysymys: miten evaluointiin osallistuneet PV:n sidosryhmien edustajat ja riskienhallinnan asiantuntijat suhtautuvat sitoumuksen hoitokyvyn valvontamalliin? Evaluointiin osallistuivat Telia Finland Oyj, Nokia Oyj, Huld Oy, Withsecure Cyber Security Services Oy ja EK. Sitoumuksen valvontakyvyn hallintamallin arvioidaan vaativan organisaatiolta osaamista ja kypsyystasoa. Eräs asiantuntija pitää sitoumuksen valvontakyvyn hallintamallin tehokkuutta huomattavana. Riskienhallinnan työpajan keskusteluilmapiiriä pidetään avoimena. Osa edustajista on jokseenkin eri mieltä, että hallintamalli olisi kannustava ja mahdollistaisi liiketoiminnan. Vastaajat ovat 90 prosenttisesti joko täysin tai jokseenkin samaa mieltä, että esille tuodut näkökulmat on huomioitu sitoumuksen valvontakyvyn hallintamallissa. Tulokset osoittavat, että näkökulmat huomioiva sitoumuksen valvontakyvyn hallintamalli mahdollistaa kruunun tietojen ja niihin kohdistuvien riskien sekä turvallisuustarpeiden ja -tunteiden tunnistamisen yksilön, yrityksen ja kansallisen resilienssin kehittämiseksi.

Teoreettisen viitekehyksen muodosti Aalto PRO 18. TJK ja turvallisuusmuotoiluprosessi auttoi sitoumuksen valvontakyvyn hallintamallin laatimista Puolustusvoimien sidosryhmille. TJK-kouluttajat ja vierailevat luennoitsijat korostivat muuttuvassa toimintaympäristössä inhimillisten turvallisuusnäkökulmien huomioimisen tärkeyttä. Henkilöstön turvallisuustarpeiden ja -tunteiden huomioiminen mahdollistaa sitoutumisen ja luottamuksen lisäämisen.

Sitoumuksen valvontakyvyn hallintamallin tavoitteet ja toteutus muistuttavat yrityksen kolmannen puolustuslinjan tavoitteita ja toteutusta: siinä pyritään objektiivisesti varmistumaan siitä, onko yritys huolehtinut riskienhallinnasta tehokkaasti yhteistyön tavoitteet ja vaatimukset huomioiden. Lopputyö osoittaa, että sitoumuksen valvontakyvyn hallintamalli osallistaa ja velvoittaa henkilöstön vastuulliseen turvallisuustyöhön mahdollistaen puolustusjärjestelmän suojaamisen kehittämällä yrityksen ja henkilöstön resilienssiä eli kyvykkyyttä toimia riskitilanteissa. Katakriin verrattuna sitoumuksen valvontakyvyn hallintamalli mahdollistaa henkilöstön turvallisuustarpeiden ja -tunteiden huomioimisen turvallisuustason säilyttämisessä. Hallintamallin käyttäminen lisää luottamusta ja henkilöstön sitoutumista yrityksen strategian ja visioiden saavuttamiseen. Liiketoiminnan kasvattamiseen tähtäävät PV:n sidosryhmät voivat hyödyntää sitoumuksen valvontakyvyn hallintamallia ja varmistaa liiketoiminnan jatkuminen ja kasvu PV:n ja muiden turvallisuutta

arvostavien asiakkaiden kanssa. Sitoumuksen valvontakyvyn hallintamallin käyttäminen helpottaa yritysturvallisuusselvitystodistuksen uusimista. Sitoumuksen valvontakyvyn hallintamalli soveltuu käytettäväksi yleisemmin organisaatioissa, joissa halutaan tunnistaa inhimilliset näkökulmat vastuullisen riskienhallintakulttuurin kehittämisessä.

Lopputyön laadinnan aikana tuli esille tarve päivittää yritysturvallisuusselvitysten laadintaohje PE:ssa, jotta sitoumuksen valvontakyvyn hallintamalli voitaisiin liittää yritysturvallisuusselvityssopimuksen liitteeseen. Ehdotus jatkotutkimukselle liittyy kyseisen asiakirjan päivittämiseen.

7 Liitteet

1: Turvallisuusmuotoilu, Business Objective and Context

Business Objective and Context

Create this together with the person funding this project.

Who needs to be involved?

(Stakeholders, people from parallel or related projects...)

Keskeisinä toimijoina ohjaamiseen osallistuvat erikseen määritellyt PV:n sidosryhmät ja Elinkeinoelämän keskusliiton yritysturvallisuuden ja riskienhallinnan johtava asiantuntija. Näkökulmia ja kantoja PV:n sitoumuksen valvontakyvyn hallintamallin tavoitteiden asetteluun, arvolupauksen tuottamiseen ja palautteen saamiseen antavat: valtioneuvoston johtava asiantuntija, PE:n valmius-päällikkö, kansallinen turvallisuusviranomainen NSA. Sitoumuksen valvontakyvyn hallintamal-lin evaluointiin osallistuvat erikseen määritetyt ja vapaaehtoiset PV:n sidosryhmät ja alihankkija.

ASK

WHY.

Social & environmental impact

(Based on our strategy & mission & values what are the positive societal and environmental impacts that we aim to boost and what are the impacts we aim to reduce.)

PV:n sidosryhmät osallistuvat omatoimisesti hyvässä hengessä sitoumuksen valvontakyvyn hallintaan.

Sitoumuksen valvontakyvyn hallintamallia voidaan hyödyntää yritysten ja heidän alihankkiioiden välisessä yhteistyössä. Sitoumuksen valvontakyvyn hallintamalli auttaa PV:n sidosryhmiä ja heidän alihankkijoita liiketoiminnallisten tavoitteiden saavuttamisessa ja tietoturvallisuuden kehittämisessä esim. hyvien käytänteiden ja tiedon jakamisessa. Sitoumuksen valvontakyvyn hallintamallia voidaan soveltaa myös viranomaisyhteistyössä esim. tietoturvallisuuskulttuurin kehittämisessä ja turvallisuustietoisuuden lisäämisessä.

Sitoumuksen valvontakyvyn hallintamalli ei edellytä keskeisten toimijoiden suurta koulutustarvetta ja toteutus voidaan jalkauttaa tämän asiakirjan muodossa. Arvion mukaan viiden vuoden päästä sitoumuksen valvontakyvyn hallintamallin toteuttaminen on kiinteä osa turvallisuustta samaan tapaan kuin yritysturvallisuustodistusten myöntä-minen. PV:n sitoumuksen valvontakyvyn hallintatyötä tehdään yhteistyössä sidosryhmi-en ja PE:n operatiivisen osaston kanssa. Toiminta on linjassaan toimivaltaiselle viranomaiselle ja määrätylle turvallisuusviranomaiselle annettujen tehtävien kanssa.

What is our business objective?

(What is the impact we are aiming to create? What is the business challenge we are trying to solve?)

Miten toimivaltaisen viranomaisen ja määrätyn turvallisuusviranomaisen tulisi osana puolustusjär-jestelmän suojaamista, turvallisuusselvityslain (726/2014) 40 §:n mukaisesti valvoa yritykselle myönnetyn yritysturvallisuusselvitystodistuksen sitoumuksen hoitokykyä ja siinnä tapahtuvia muutoksia?

How far are we aiming?

(Are we doing a incremental innovation, a breakthrough, or are we disrupting the market? When are we expected to have a viable business?)

Tavoitteena on laatia sitoumuksen valvontakyvyn hallintamalli, mikä velvoittaa ja osallistaa PV:n sidosryhmät sitoutumaan itsenäiseen riskienhallinnan kehittämiseen hyvässä yhteistyässä PE:n kanssa. Tavoitteena on lisäarvon tuottaminen puolustusjärjestelmän suojaamiseksi. Valvontatyön ja turvallisuuskontrollien merkitys on keskeinen puolustusjärjestelmän suojaamisessa motivoitunutta valtiollista toimijaa vastaan.

What is our strategic purpose?

(Are we an option to be invested in if need be? Are we the big bet that will change our company? Or are we a no-regret move that will be beneficial no matter what?)

Toimivaltainen viranomainen ja määrätty turvallisuusviranomainen tulee panostamaan antamiensa yritysturvallisuusselvitystodistusten sitoumuksen hoitokyvyn valvontaan. Valvonta koetaan perustavaa laatua olevaksi asiaksi ja tärkeäksi sitoumuksen hoitokyvyn arvioimiseksi tehtäväksi työksi. Valvontatyö on tärkeä puolustusjärjestelmän suojaamiseksi, jossa ei ole varaa epäonnistua.

How will we know that we've succeeded?

(After a month? After a year...? Write concrete goals.)

Lopullisen sitoumuksen valvontakyvyn hallintamallin arvioivat erikseen valitut PV:n sidosryhmien ja alihankkijoiden asiantuntijat.

Onnistuessaan PV:n sitoumuksen valvontakyvyn hallinta-malli velvoittaa ja osallistaa PV:n sidosryhmiä ja heidän alihankkijoita turvallisuuskulttuurin hehittämiseen myös ilman toimivaltaisen viranomaisen ja määrätyn turvallisuus-viranomaisen aktiivista roolia.

PV:n sidosryhmien sitouttamisen onnistumisen ratkaisee lopulta PV:n sidosryhmien tahtotila ja PV:n yritysturvallisuudesta vastaava Pääesikunta.

Muita mittareita ovat esim. laadittujen raporttien määrä vuodessa ja niiden perusteella laaditut suositukset.

Risks, restrictions and things we need to take into account?

(Budget, Schedule, Organization, Legal, Current business, ...)

Sitoumuksen valvontakyvyn hallintamallin laadinnassa on kartoitettava etukäteen erikseen määritettyjen PV:n sidosryhmien tavoitteet ja huolet.

Tavoiteasettelussa tulee hyödyntää keskeisten toimijoiden (PV:n sidosryhmät, EK, NSA, VNK ja PV) asiantuntijanäkemyksiä.

PV:n sidosryhmien huolet saattavat liittyä epävarmuuteen sitoumuksen valvontakyvyn hallintatyön merkityksellisyydestä liiketoiminnan jatkuvuuteen ja valvonnassa esille tuleviin asioihin, lisääntyvään byrokratiaan ja kasvaviin turvallisuuskustannuksiin.

2: Turvallisuusmuotoilu, Customer Grouping

Customer Grouping

Your best guess of who you aim to serve.

Identified customer need:

PV:n sidosryhmät toimivat liiketoiminnallisista lähtökohdista, joissa toiminnan tehokkuus ja yritysten liiketoiminnan kasvattaminen on tärkeää.

Sitoumuksen valvontakyvyn hallintamallin tulee mahdollistaa liiketoiminnan jatkuvuus PV:n kanssa.

Description:

PV:n sidosryhmiä ovat turvallisuushankkeissa ja -projekteissa työskenteleviä yrityksiä ja alihankkijoita sekä muita PV:n turvallisuusluokiteltuja asiakirjoja käsitteleviä organisaatioita.

Toimivaltainen viranomainen ja määrätty turvallisuusviranomainen on antanut PV:n sidosryhmille yritysturvallisuusselvitysto distuksia.

Group name:

PV:n sidosryhmät

PV:n sidosryhmät ja alihankkijat

Riskienhallinnan ammattilaiset

Hanke- ja projektipäälliköt

Hankehenkilöstö

Koko henkilöstö

Main Group: PV:n sidosryhmät

Identified customer need:

Lisäarvon tuottaminen puolustusjärjestelmän suojaamiseksi.

Description:

Kansallisen turvallisuusviranomaisen tehtävä on kansainvälisen tietoturvallisuusvelvoitelain mukaisesti ohjata ja valvoa, että Suomelle toimitettu kansainvälinen turvallisuusluokiteltu tieto suojataan ja sitä käsitellään asianmukaisesti

Puolustusministeriö, PE ja Supo toimivat määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA), joille on jaettu omat vastuualueet kansallisen turvallisuusviranomaisen kokonaisvastuukentästä.

Group name:

NSA ja PE DSA

Kansallinen turvallisuusviranomainen

PE, puolustusministeriö (PLM) ja Supo ovat määrättyjä turvallisuusviranomaisia

Traficom toimii määrättynä tietoliikenneturvallisuusviranomaisena

Main Group: **NSA ja PE DSA**

Identified customer need:

Puolustusjärjestelmän turvaaminen turvallisuusluokitelluissa hankkeissa ja projekteissa.

Description

PE:n operatiivinen osasto ylläpitää ja kehittää PV:n operatiivista johtamiskykyä ja valmiutta. PE:n valmiuspäällikkö on operatiivisen toimialan ja turvallisuustoimialan johtaja. PE:n operatiivinen osasto johtaa PV:n yritysturvallisuutta. PV:n turvallisuusarkastajat auditoivat yrityksiä PE:n operatiivisen osaston ohjauksessa. PV:n hankkeisiin osallistuvien yritysten sitoumuksen luotettavuutta auditoidaan kansallisella turvallisuuden auditointikriteeristöllä.

Group name:

PV

PE operatiivinen osasto

Puolustushaarat ja hallintoyksiköt

Asiantuntijat

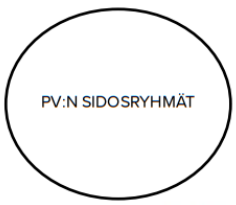
Hanke- ja projekti-henkilöstö

Main Group: **PE**

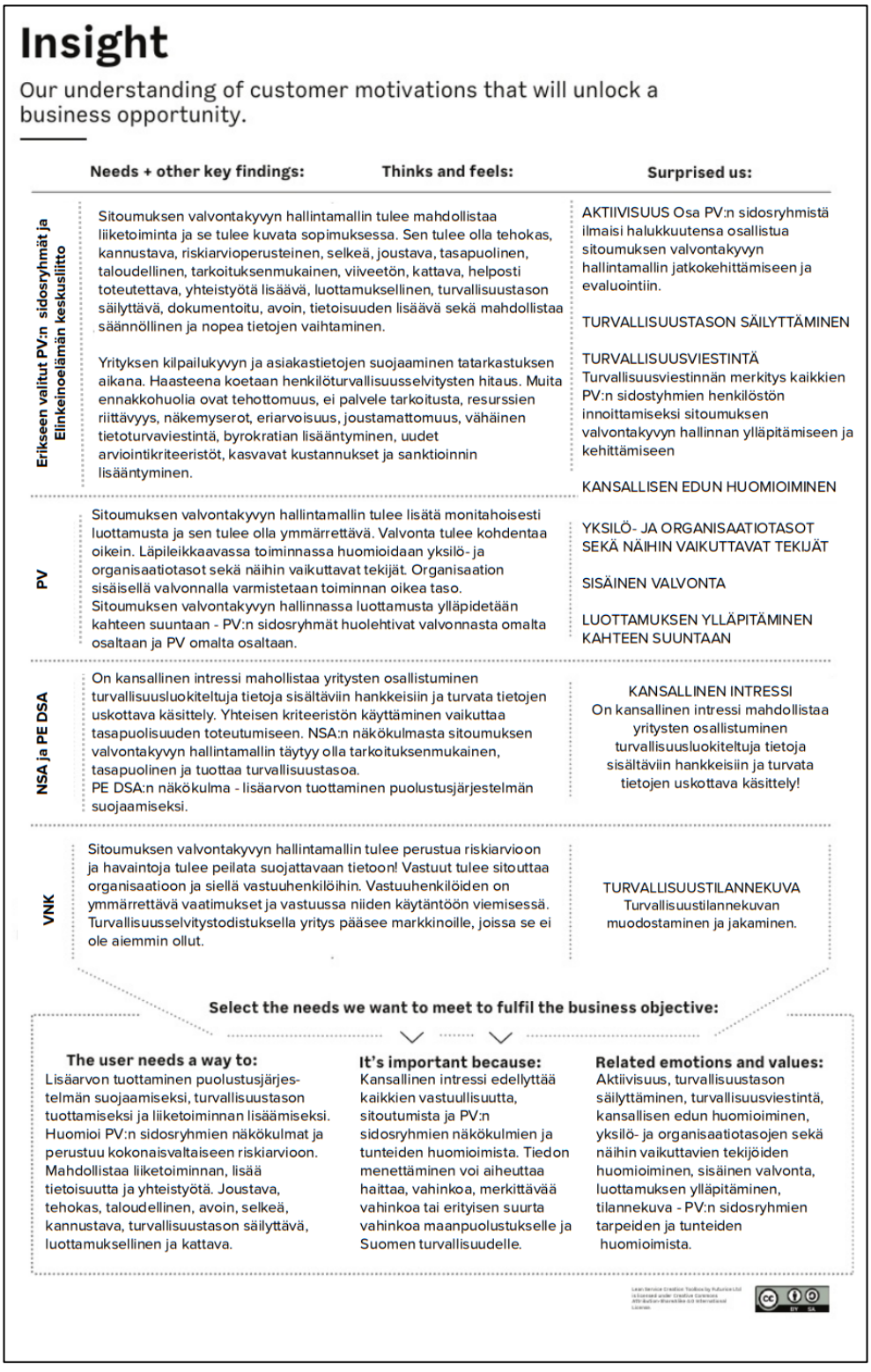
Common in all user segments:

- Yhteiset hankkeet ja -projektit, joissa käsitellään PV:n turvallisuusluokiteltuja asiakirjoja.
- Turvallisuusluokiteltujen asiakirjojen huolellinen säilyttäminen ja käsittely.
- Kokonaisvaltainen riskienhallinta turvallisuushankkeissa ja -projekteissa.
- Ennaltaehkäisevän riskienhallinta sekä resilienssin parantaminen yksilö- ja organisaatiotasolta aina valtiolliselle tasolle asti.
- Yhteisen arvopohjan, tavoitteiden ja visioiden jakaminen sekä aktiivinen yhteistyö eri tasoilla.
- Tietoturvallisuusvastuullisuus demokraattisessa yhteiskunnassa.

Keskeisin kohderyhmä



3: Turvallisuusmuotoilu, Insight



Insight

Our understanding of customer motivations that will unlock a business opportunity.

	Needs + other key findings:	Thinks and feels:	Surprised us:
Erikseen valitut PV:n sidosryhmät ja Elinkeinoelämän keskusliitto	Sitoumuksen valvontakyvyn hallintamallin tulee mahdollistaa liiketoiminta ja se tulee kuvata sopimuksessa. Sen tulee olla tehokas, kannustava, riskiarvioperusteinen, selkeä, joustava, tasapuolinen, taloudellinen, tarkoituksenmukainen, viiveetön, kattava, helposti toteutettava, yhteistyötä lisäävä, luottamuksellinen, turvallisuustason säilyttävä, dokumentoitu, avoin, tietoisuuden lisäävä sekä mahdollistaa säännöllinen ja nopea tietojen vaihtaminen. Yrityksen kilpailukyvyn ja asiakastietojen suojaaminen tatarkastuksen aikana. Haasteena koetaan henkilöturvallisuusselvitysten hitaus. Muita ennakkohuolia ovat tehottomuus, ei palvele tarkoitusta, resurssien riittävyys, näkemyserot, eriarvoisuus, joustamattomuus, vähäinen tietoturvaviestintä, byrokratian lisääntyminen, uudet arviointikriteeristöt, kasvavat kustannukset ja sanktioinnin lisääntyminen.		AKTIIVISUUS Osa PV:n sidosryhmistä ilmaisi halukkuutensa osallistua sitoumuksen valvontakyvyn hallintamallin jatkokehittämiseen ja evaluointiin. TURVALLISUUSTASON SÄILYTTÄMINEN TURVALLISUUSVIESTINTÄ Turvallisuusviestinnän merkitys kaikkien PV:n sidostyhmien henkilöstön innoittamiseksi sitoumuksen valvontakyvyn hallinnan ylläpitämiseen ja kehittämiseen KANSALLISEN EDUN HUOMIOIMINEN
PV	Sitoumuksen valvontakyvyn hallintamallin tulee lisätä monitahoisesti luottamusta ja sen tulee olla ymmärrettävä. Valvonta tulee kohdentaa oikein. Läpileikkaavassa toiminnassa huomioidaan yksilö- ja organisaatiotasot sekä näihin vaikuttavat tekijät. Organisaation sisäisellä valvonnalla varmistetaan toiminnan oikea taso. Sitoumuksen valvontakyvyn hallinnassa luottamusta ylläpidetään kahteen suuntaan - PV:n sidosryhmät huolehtivat valvonnasta omalta osaltaan ja PV omalta osaltaan.		YKSILÖ- JA ORGANISAATIOTASOT SEKÄ NÄIHIN VAIKUTTAVAT TEKIJÄT SISÄINEN VALVONTA LUOTTAMUKSEN YLLÄPITÄMINEN KAHTEEN SUUNTAAN
NSA ja PE DSA	On kansallinen intressi mahollistaa yritysten osallistuminen turvallisuusluokiteltuja tietoja sisältäviin hankkeisiin ja turvata tietojen uskottava käsittely. Yhteisen kriteeristön käyttäminen vaikuttaa tasapuolisuuden toteutumiseen. NSA:n näkökulmasta sitoumuksen valvontakyvyn hallintamallin täytyy olla tarkoituksenmukainen, tasapuolinen ja tuottaa turvallisuustasoa. PE DSA:n näkökulma - lisäarvon tuottaminen puolustusjärjestelmän suojaamiseksi.		KANSALLINEN INTRESSI On kansallinen intressi mahdollistaa yritysten osallistuminen turvallisuusluokiteltuja tietoja sisältäviin hankkeisiin ja turvata tietojen uskottava käsittely!
VNK	Sitoumuksen valvontakyvyn hallintamallin tulee perustua riskiarvioon ja havaintoja tulee peilata suojattavaan tietoon! Vastuut tulee sitouttaa organisaatioon ja siellä vastuuhenkilöihin. Vastuuhenkilöiden on ymmärrettävä vaatimukset ja vastuussa niiden käytäntöön viemisessä. Turvallisuusselvitystodistuksella yritys pääsee markkinoille, joissa se ei ole aiemmin ollut.		TURVALLISUUSTILANNEKUVA Turvallisuustilannekuvan muodostaminen ja jakaminen.

Select the needs we want to meet to fulfil the business objective:

The user needs a way to:
Lisäarvon tuottaminen puolustusjärjestelmän suojaamiseksi, turvallisuustason tuottamiseksi ja liiketoiminnan lisäämiseksi. Huomioi PV:n sidosryhmien näkökulmat ja perustuu kokonaisvaltaiseen riskiarvioon. Mahdollistaa liiketoiminnan, lisää tietoisuutta ja yhteistyötä. Joustava, tehokas, taloudellinen, avoin, selkeä, kannustava, turvallisuustason säilyttävä, luottamuksellinen ja kattava.

It's important because:
Kansallinen intressi edellyttää kaikkien vastuullisuutta, sitoutumista ja PV:n sidosryhmien näkökulmien ja tunteiden huomioimista. Tiedon menettäminen voi aiheuttaa haittaa, vahinkoa, merkittävää vahinkoa tai erityisen suurta vahinkoa maanpuolustukselle ja Suomen turvallisuudelle.

Related emotions and values:
Aktiivisuus, turvallisuustason säilyttäminen, turvallisuusviestintä, kansallisen edun huomioiminen, yksilö- ja organisaatiotasojen sekä näihin vaikuttavien tekijöiden huomioiminen, sisäinen valvonta, luottamuksen ylläpitäminen, tilannekuva - PV:n sidosryhmien tarpeiden ja tunteiden huomioimista.

4: Turvallisuusmuotoilu, Rational Concept Sheet

Rational Concept Sheet

Draft a concept out of your idea

Concept name? Sitoumuksen valvontakyvyn hallintamalli Puolustusvoimien sidosryhmissä

How does it work?

Sitoumuksen valvontakyvyn hallintamalli muodostuu kolemesta toistensa kanssa vuorovaikutuksessa olevasta osasta: seitsemästä toimintaperiaatteesta, viestäsyklistä ja tavoitteiden saavuttamiseen sitoutumisesta. PV:n turvallisuushankkeissa ja -projekteissa työskentelevällä henkilöstöllä on tärkeä rooli arvolupauksen tuottamisessa.

Sitoumuksen valvontakyvyn hallintaa ohjaa seitsemän periaatetta: 1. Kokonaisvaltainen riskienhallinta. 2. Henkilöstön turvallisuustarpeet ja -tunteet. 3. Avoin ja luottamuksellinen viestintä. 4. Koko henkilöstöä tunnetasolla sitouttava. 5. Arvolupauksen tuottaminen. 6. Riskienhallintapäätökset. 7. Riskien jatkuva arviointi, ilmoittaminen ja oppiminen.

Lisäarvon tuottamiseksi viestintä muodostuu neljästä loogisesti toisiinsa liittyvästä vaiheesta:
1) Yrityksen johdon ohjaus sitoumuksen valvontakyvyn hallintaan.
2) Sitoumuksen valvontakyvyn hallintasuunnitelman laatiminen.
3) Sitoumuksen valvontakyvyn hallintasuunnitelman toteuttaminen ja tarkentaminen.
4) Sitoumuksen valvontakyvyn hallinta-arvion laatiminen ja raportin esittely johdolle päätöksentekoa varten.

Sitoutumisen onnistumisen edellytys - koko henkilöstön sitoutuminen on linjassa yrityksen johdon riskinottohalun kanssa. Riskivastuiden osalta henkilöstön sitouttaminen tunnetasolla suunnitteluun ja päätöksentekoon. Sitouttamisperusteisessa johtamisessa selvitetään henkilöstön turvallisuustarpeet ja -tunteet, jotka ovat tietoisuus, huolellisuus, kyvykkyys, asenne, motivaatio, ohjeet, työvälineet, työympäristö, kulttuuri ja johtaminen.

Value to the end-user?

Tuottaa lisäarvoa liiketoiminnan mahdollistamiseksi ja puolustusjärjestelmän suojaamiseksi sekä lisätä monitasoisesti luottamusta.

Sitoumuksen valvontakyvyn hallintamalli sitouttaa vastuuhenkilöt ja organisaatiot liiketoiminnallisten tavoitteiden saavuttamiseen ja puolustusjärjestelmän suojaamiseen.

What differentiates it from other solutions to the same problem?

Sitoumuksen valvontakyvyn hallintamalli on laadittu erikseen valittujen PV:n sidosryhmien, EK:n, NSA:n, VNK:n, ja PV:n näkökulmien pohjalta.

Erona yleisiin riskienhallintastandardeihin verrattuna sitoumuksen valvontakyvyn hallintamallissa:

- henkilöstö asetetaan keskiöön arvolupauksen tuottamiseksi,
- vastuuhenkilöt pyritään tunnetasolla sitouttamaan lisäarvon tuottamiseen,
- henkilöstö sitoutetaan kartoituksessa
- valvonnan tasoa säädetään yrityksen johdon ohjauksessa ja
- yrityksen johdolle esitellään tilannekuva päätöksentekoa varten.

Value to our business?

- Varmista organisaation sitoutumisen hoitokyky ja liiketoiminnan jatkuminen ja kasvu PV:n kanssa.
- Varmista yrityksen tavoitteiden ja visioiden saavuttaminen tunnistamalla liiketoimintaan, puolustusjärjestelmään ja kansalliseen turvallisuuteen kohdistuvien riskien tunnistaminen.
- Uusi yritysturvallisuusselvitystodistus.
- Hallitse liiketoimintariskejä.

Social and environmental impact?

Sitoumuksen valvontakyvyn hallintamalli toteutetaan PV:n sidosryhmissä itsenäisesti ja toiminnan tasoa säädetään organisaation johdon ohjauksessa. Toiminta tuottaa johdolle analysoitua tietoa päätöksentekoa varten.

Tarvittaessa toimivaltainen viranomainen ja määrätty turvallisuusviranomainen tukee PV:n sidosryhmiä sitoumuksen valvontakyvyn hallinnassa. Asiantuntijatuki liittyy annetun yritysturvallisuusselvitystodistuksen uusimiseen ja/tai sitoumuksen hoitokyvyn toteuttamisen tai turvallisuuskulttuurin kehittämiseen.

Se miten valvonnasta puhutaan ja miten aktiivista yhteistyötä tehdään on positiivinen vaikutus organisaation turvallisuuskulttuurin kehittämisessä.

Rational value proposition:

END USER: Arvolupaus: lisäarvon tuottaminen yritysten liiketoimintaan, henkilöstön turvallisuustarpeeseen ja -tunteeseen, puolustusjärjestelmän suojaamiseen, monitasoisen luottamukseen ja Suomen turvallisuuteen osana läntistä maailmaa!

NEED:

- Liiketoiminnan mahdollistaminen ja lisääminen.
- Turvallisuustason säilyttäminen ja tuottaminen.
- Asiakkuuksien ja puolustusjärjestelmän suojaaminen.
- Kokonaisvaltaiseen riskiarvioon perustuva.
- PV:n sidosryhmien näkökulmat huomioiva.

SOLUTION: Sitoumuksen valvontakyvyn hallintamallin itsenäinen ja aktiivinen toteuttaminen yrityksissä ja alihankkijoissa lisäarvon tuottamiseksi.

5: Turvallisuustarpeiden ja -tunteiden kyselypohja

Päivämäärä: _____

Kartoitus koskee organisaatiota: _____

1. KRUUNUN TIEDOT

Kruunun tiedoilla tarkoitetaan kriittisiä tietoja ja turvallisuusluokiteltuja asiakirjoja, joiden joutuminen ulkopuolisten henkilöiden ja toimijoiden haltuun saattaa aiheuttaa joko haittaa, vahinkoa, merkittävää vahinkoa tai erityisen suurta vahinkoa yrityksen liiketoiminnalle, maanpuolustukselle ja Suomen turvallisuudelle.

Tarkennus ja rajaus kruunun tietoihin:

_____

_____

_____

_____

_____

2. KRUUNUN TIETOIHIN LIITTYVÄT RISKIT

ISO 31000:2018-riskienhallintastandardin mukaan riski on epävarmuuden vaikutus tavoitteisiin.

Minkälaisia riskejä mielestäsi kohdistuu kruunun tietoihin?
1. 2. 3. 4. 5.

3. HENKILÖSTÖN TURVALLISUUSTARPEET JA –TUNTEET

A. Sitoumuksen hoitokyvyn tietoisuuden taso on:

Tietoisuudella tarkoitetaan henkilöstön tietoisuutta kruunun tiedoista, haavoittuvuuksista ja uhkakuvista.

0. Olematon.
1. Erittäin alhainen.
2. Matala.
3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit tietoisuutta – mikä helpottaisi työtäsi?

B. Sitoumuksen hoitokyvyn huolellisuuden taso on:

Huolellisuudella tarkoitetaan kruunun tietojen huolellista ja ohjeiden mukaista käsittelyä ja säilytystä työkiireistä huolimatta.

0. Olematon.
1. Erittäin alhainen.
2. Matala.
3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit huolellisuutta – mikä helpottaisi työtäsi?

C. Sitoumuksen hoitokyvyn kyvykkyyden taso on:

Kyvykkyydellä tarkoitetaan riskienhallinnan toteuttamista osaavasti kruunun tietojen suojaamiseksi, esimerkiksi turvallisuuspoikkeamien tunnistaminen ja ilmoittaminen.

0. Olematon.
1. Erittäin alhainen.
2. Matala.
3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit kyvykkyyttä – mikä helpottaisi työtäsi?

D. Sitoumuksen hoitokyvyn asenteen taso on:

Henkilöstön asenne kruunun tietojen varovaiseen käsittelyyn ja säilytykseen voi olla joko positiivinen tai negatiivinen.

0. Olematon.
1. Erittäin alhainen.
2. Matala.
3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit asennetta – mikä helpottaisi työtäsi?

E. Sitoumuksen hoitokyvyn motivaation taso on:

Motivaatiolla tarkoitetaan sisäisiä ja ulkoisia motivaatiotekijöitä, jotka vaikuttavat kruunun tietojen turvalliseen käsittelyyn ja säilytykseen.

0. Olematon.
1. Erittäin alhainen.
2. Matala.
3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit motivaatiota – mikä helpottaisi työtäsi?

F. Sitoumuksen hoitokyvyn ohjeiden taso on:

Ohjeilla tarkoitetaan kruunun tietojen käsittelyyn ja säilytykseen liittyvien turvallisuusohjeiden selkeyttä, ymmärrettävyyttä ja helppoa saatavuutta.

0. Olematon.
1. Erittäin alhainen.
2. Matala.
3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit ohjeita – mikä helpottaisi työtäsi?

G. Sitoumuksen hoitokyvyn työvälineiden taso on:

Työvälineillä tarkoitetaan kruunun tietojen käsittelyyn ja säilytykseen tarkoitettuja teknisiä työvälineitä, jotka mahdollistavat henkilöstölle tarkoituksenmukaisen ja turvallisen työskentelyn.

0. Olematon.
1. Erittäin alhainen.
2. Matala.
3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit työvälineitä – mikä helpottaisi työtäsi?

H. Sitoumuksen hoitokyvyn työympäristön taso on:

Työympäristöllä tarkoitetaan kruunun tietojen fyysistä käsittely- ja säilytysympäristöä, mikä mahdollistaa henkilöstölle tarkoituksenmukaisen ja turvallisen käyttäytymisen.

0. Olematon.
1. Erittäin alhainen.
2. Matala.

3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit työympäristöä – mikä helpottaisi työtäsi?

I. Sitoumuksen hoitokyvyn kulttuurin taso on:

Kulttuurilla tarkoitetaan ajattelua ja käytänteitä sitä, kuinka avoimesti ja luottamuksellisesti kruunun tietoihin kohdistuvista riskeistä keskustellaan ja riskienhallintaa kehitetään yhdessä koko henkilöstön kanssa.

0. Olematon.
1. Erittäin alhainen.
2. Matala.
3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit kulttuuria – miten onnistuisit työssäsi turvallisemmin?

J. Sitoumuksen hoitokyvyn johtamisen taso on:

Johtamisella tarkoitetaan sitä, kuinka koko henkilöstö sitoutetaan tunnetasolla turvallisuusviestinnän ja -johtamisen keinoin sitoumuksen valvontakyvyn jatkuvaan seurantaan, suunnitteluun, toteutukseen, kehittämiseen, tietoisuuden lisäämiseen ja ylläpitoon.

0. Olematon.
1. Erittäin alhainen.
2. Matala.
3. Keskikokoinen.
4. Korkea.
5. Erittäin korkea.
6. En osaa sanoa.

Kerrotko esimerkin missä onnistuttiin?

Työn parhaana osaajana, miten arvioisit johtamista – miten onnistuisit työssäsi turvallisemmin?

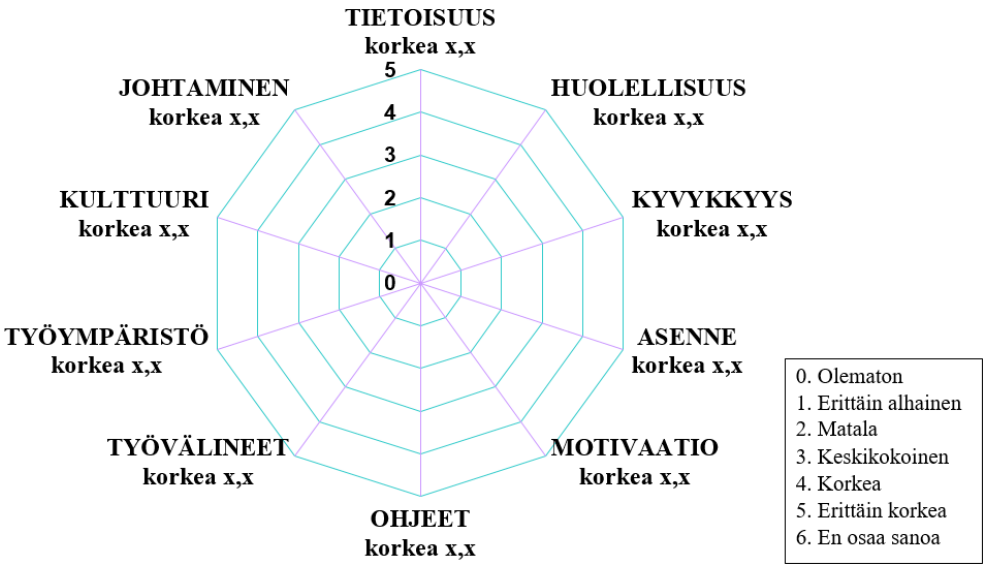
4. TURVALLISUUSKÄVELY

Turvallisuuskävelyn havainnot.

6: Turvallisuustarpeiden ja -tunteiden raportointipohja

Kruunun tiedot

Riskien ja haavoittuvuuksien luokittelu	
Hallinnollinen	Henkilöstö
Fyysinen	Tekninen



Turvallisuustarpeet ja –tunteiden mittaustulos			
Osa-alueet	Tulos	Esimerkkejä	Kehittämisnäkökulmia
A. Tietoisuus			
B. Huolellisuus			
C. Kyvykkyys			
D. Asenne			
E. Motivaatio			
F. Ohjeet			
G. Työvälineet			
H. Työympäristö			
I. Kulttuuri			
J. Johtaminen			

Turvallisuuskävelyn havainnot

7: Näkökulmien huomioimisen arviointikysely

1. Huomioi sidosryhmien näkökulmat.

   A. Täysin eri mieltä.
   B. Jossain määrin eri mieltä.
   C. Ei samaa mieltä eikä eri mieltä.
   D. Jossain määrin samaa mieltä.
   E. Täysin samaa mieltä.

2. Perustuu kokonaisvaltaiseen riskiarvioon.

   A. Täysin eri mieltä.
   B. Jossain määrin eri mieltä.
   C. Ei samaa mieltä eikä eri mieltä.
   D. Jossain määrin samaa mieltä.
   E. Täysin samaa mieltä.

3. Peilataan suojattavaan tietoon.

   A. Täysin eri mieltä.
   B. Jossain määrin eri mieltä.
   C. Ei samaa mieltä eikä eri mieltä.
   D. Jossain määrin samaa mieltä.
   E. Täysin samaa mieltä.

4. Tuottaa lisäarvoa puolustusjärjestelmän suojaamiseen.

   A. Täysin eri mieltä.
   B. Jossain määrin eri mieltä.
   C. Ei samaa mieltä eikä eri mieltä.
   D. Jossain määrin samaa mieltä.
   E. Täysin samaa mieltä.

5. Tarkoituksenmukainen.

   A. Täysin eri mieltä.
   B. Jossain määrin eri mieltä.
   C. Ei samaa mieltä eikä eri mieltä.
   D. Jossain määrin samaa mieltä.
   E. Täysin samaa mieltä.

6. Lisää tietoisuutta.

   A. Täysin eri mieltä.
   B. Jossain määrin eri mieltä.
   C. Ei samaa mieltä eikä eri mieltä.
   D. Jossain määrin samaa mieltä.
   E. Täysin samaa mieltä.

7. Joustava.

   A. Täysin eri mieltä.
   B. Jossain määrin eri mieltä.
   C. Ei samaa mieltä eikä eri mieltä.
   D. Jossain määrin samaa mieltä.
   E. Täysin samaa mieltä.

8. Tehokas.

   A. Täysin eri mieltä.
   B. Jossain määrin eri mieltä.
   C. Ei samaa mieltä eikä eri mieltä.
   D. Jossain määrin samaa mieltä.
   E. Täysin samaa mieltä.

9. Mahdollistaa liiketoiminnan.

   A. Täysin eri mieltä.
   B. Jossain määrin eri mieltä.
   C. Ei samaa mieltä eikä eri mieltä.
   D. Jossain määrin samaa mieltä.
   E. Täysin samaa mieltä.

10. Taloudellinen.

    A. Täysin eri mieltä.
    B. Jossain määrin eri mieltä.
    C. Ei samaa mieltä eikä eri mieltä.
    D. Jossain määrin samaa mieltä.
    E. Täysin samaa mieltä.

11. Yhteistyö.

    A. Täysin eri mieltä.
    B. Jossain määrin eri mieltä.
    C. Ei samaa mieltä eikä eri mieltä.
    D. Jossain määrin samaa mieltä.
    E. Täysin samaa mieltä.

12. Selkeä.

    A. Täysin eri mieltä.
    B. Jossain määrin eri mieltä.
    C. Ei samaa mieltä eikä eri mieltä.
    D. Jossain määrin samaa mieltä.
    E. Täysin samaa mieltä.

13. Avoin.

    A. Täysin eri mieltä.
    B. Jossain määrin eri mieltä.
    C. Ei samaa mieltä eikä eri mieltä.
    D. Jossain määrin samaa mieltä.
    E. Täysin samaa mieltä.

14. Tasapuolinen.

    A. Täysin eri mieltä.
    B. Jossain määrin eri mieltä.
    C. Ei samaa mieltä eikä eri mieltä.
    D. Jossain määrin samaa mieltä.
    E. Täysin samaa mieltä.

15. Kannustava.

    A. Täysin eri mieltä.
    B. Jossain määrin eri mieltä.
    C. Ei samaa mieltä eikä eri mieltä.
    D. Jossain määrin samaa mieltä.
    E. Täysin samaa mieltä.

16. Säilyttää turvallisuustason.

    A. Täysin eri mieltä.
    B. Jossain määrin eri mieltä.
    C. Ei samaa mieltä eikä eri mieltä.
    D. Jossain määrin samaa mieltä.
    E. Täysin samaa mieltä.

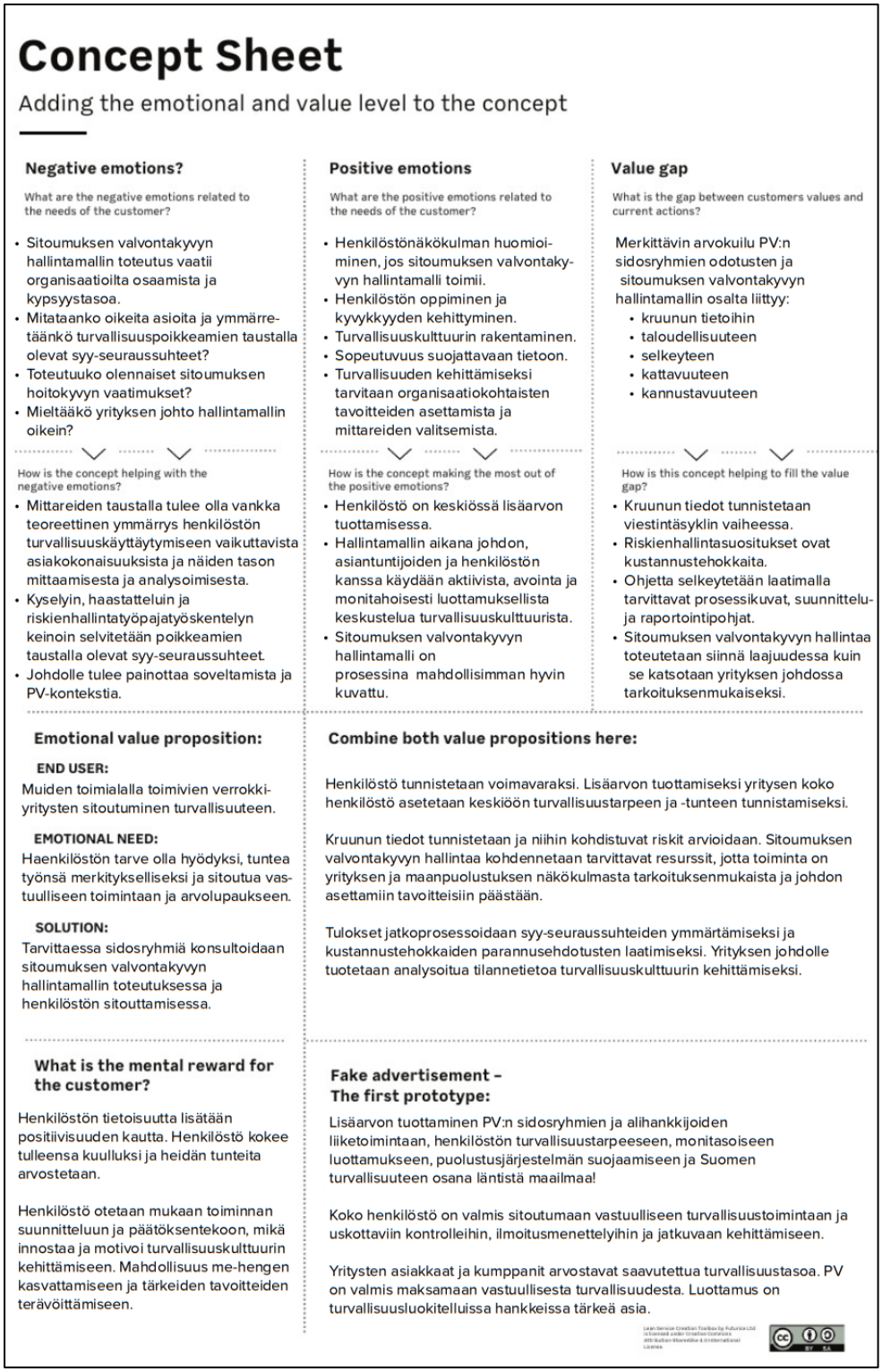
17. Luottamuksellinen.

    A. Täysin eri mieltä.
    B. Jossain määrin eri mieltä.
    C. Ei samaa mieltä eikä eri mieltä.
    D. Jossain määrin samaa mieltä.
    E. Täysin samaa mieltä.

18. Kattava.

    A. Täysin eri mieltä.
    B. Jossain määrin eri mieltä.
    C. Ei samaa mieltä eikä eri mieltä.
    D. Jossain määrin samaa mieltä.
    E. Täysin samaa mieltä.

8: Turvallisuusmuotoilu, Concept Sheet



Concept Sheet

Adding the emotional and value level to the concept

Negative emotions?

What are the negative emotions related to the needs of the customer?

- Sitoumuksen valvontakyvyn hallintamallin toteutus vaatii organisaatioilta osaamista ja kypsyystasoa.
- Mitataanko oikeita asioita ja ymmärretäänkö turvallisuuspoikkeamien taustalla olevat syy-seuraussuhteet?
- Toteutuuko olennaiset sitoumuksen hoitokyvyn vaatimukset?
- Mieltääkö yrityksen johto hallintamallin oikein?

How is the concept helping with the negative emotions?

- Mittareiden taustalla tulee olla vankka teoreettinen ymmärrys henkilöstön turvallisuuskäyttäytymiseen vaikuttavista asiakokonaisuuksista ja näiden tason mittaamisesta ja analysoimisesta.
- Kyselyin, haastatteluin ja riskienhallintatyöpajatyöskentelyn keinoin selvitetään poikkeamien taustalla olevat syy-seuraussuhteet.
- Johdolle tulee painottaa soveltamista ja PV-kontekstia.

Positive emotions

What are the positive emotions related to the needs of the customer?

- Henkilöstönäkökulman huomioiminen, jos sitoumuksen valvontakyvyn hallintamalli toimii.
- Henkilöstön oppiminen ja kyvykkyyden kehittyminen.
- Turvallisuuskulttuurin rakentaminen.
- Sopeutuvuus suojattavaan tietoon.
- Turvallisuuden kehittämiseksi tarvitaan organisaatiokohtaisten tavoitteiden asettamista ja mittareiden valitsemista.

How is the concept making the most out of the positive emotions?

- Henkilöstö on keskiössä lisäarvon tuottamisessa.
- Hallintamallin aikana johdon, asiantuntijoiden ja henkilöstön kanssa käydään aktiivista, avointa ja monitahoisesti luottamuksellista keskustelua turvallisuuskulttuurista.
- Sitoumuksen valvontakyvyn hallintamalli on prosessina mahdollisimman hyvin kuvattu.

Value gap

What is the gap between customers values and current actions?

Merkittävin arvokuilu PV:n sidosryhmien odotusten ja sitoumuksen valvontakyvyn hallintamallin osalta liittyy:

- kruunun tietoihin
- taloudellisuuteen
- selkeyteen
- kattavuuteen
- kannustavuuteen

How is this concept helping to fill the value gap?

- Kruunun tiedot tunnistetaan viestintäsyklin vaiheessa.
- Riskienhallintasuositukset ovat kustannustehokkaita.
- Ohjetta selkeytetään laatimalla tarvittavat prosessikuvat, suunnittelu- ja raportointipohjat.
- Sitoumuksen valvontakyvyn hallintaa toteutetaan siinnä laajuudessa kuin se katsotaan yrityksen johdossa tarkoituksenmukaiseksi.

Emotional value proposition:

END USER:

Muiden toimialalla toimivien verrokkiyritysten sitoutuminen turvallisuuteen.

EMOTIONAL NEED:

Haenkilöstön tarve olla hyödyksi, tuntea työnsä merkitykselliseksi ja sitoutua vastuulliseen toimintaan ja arvolupaukseen.

SOLUTION:

Tarvittaessa sidosryhmiä konsultoidaan sitoumuksen valvontakyvyn hallintamallin toteutuksessa ja henkilöstön sitouttamisessa.

Combine both value propositions here:

Henkilöstö tunnistetaan voimavaraksi. Lisäarvon tuottamiseksi yritysen koko henkilöstö asetetaan keskiöön turvallisuustarpeen ja -tunteen tunnistamiseksi.

Kruunun tiedot tunnistetaan ja niihin kohdistuvat riskit arvioidaan. Sitoumuksen valvontakyvyn hallintaa kohdennetaan tarvittavat resurssit, jotta toiminta on yrityksen ja maanpuolustuksen näkökulmasta tarkoituksenmukaista ja johdon asettamiin tavoitteisiin päästään.

Tulokset jatkoprosessoidaan syy-seuraussuhteiden ymmärtämiseksi ja kustannustehokkaiden parannusehdotusten laatimiseksi. Yrityksen johdolle tuotetaan analysoitua tilannetietoa turvallisuuskulttuurin kehittämiseksi.

What is the mental reward for the customer?

Henkilöstön tietoisuutta lisätään positiivisuuden kautta. Henkilöstö kokee tulleensa kuulluksi ja heidän tunteita arvostetaan.

Henkilöstö otetaan mukaan toiminnan suunnitteluun ja päätöksentekoon, mikä innostaa ja motivoi turvallisuuskulttuurin kehittämiseen. Mahdollisuus me-hengen kasvattamiseen ja tärkeiden tavoitteiden terävöittämiseen.

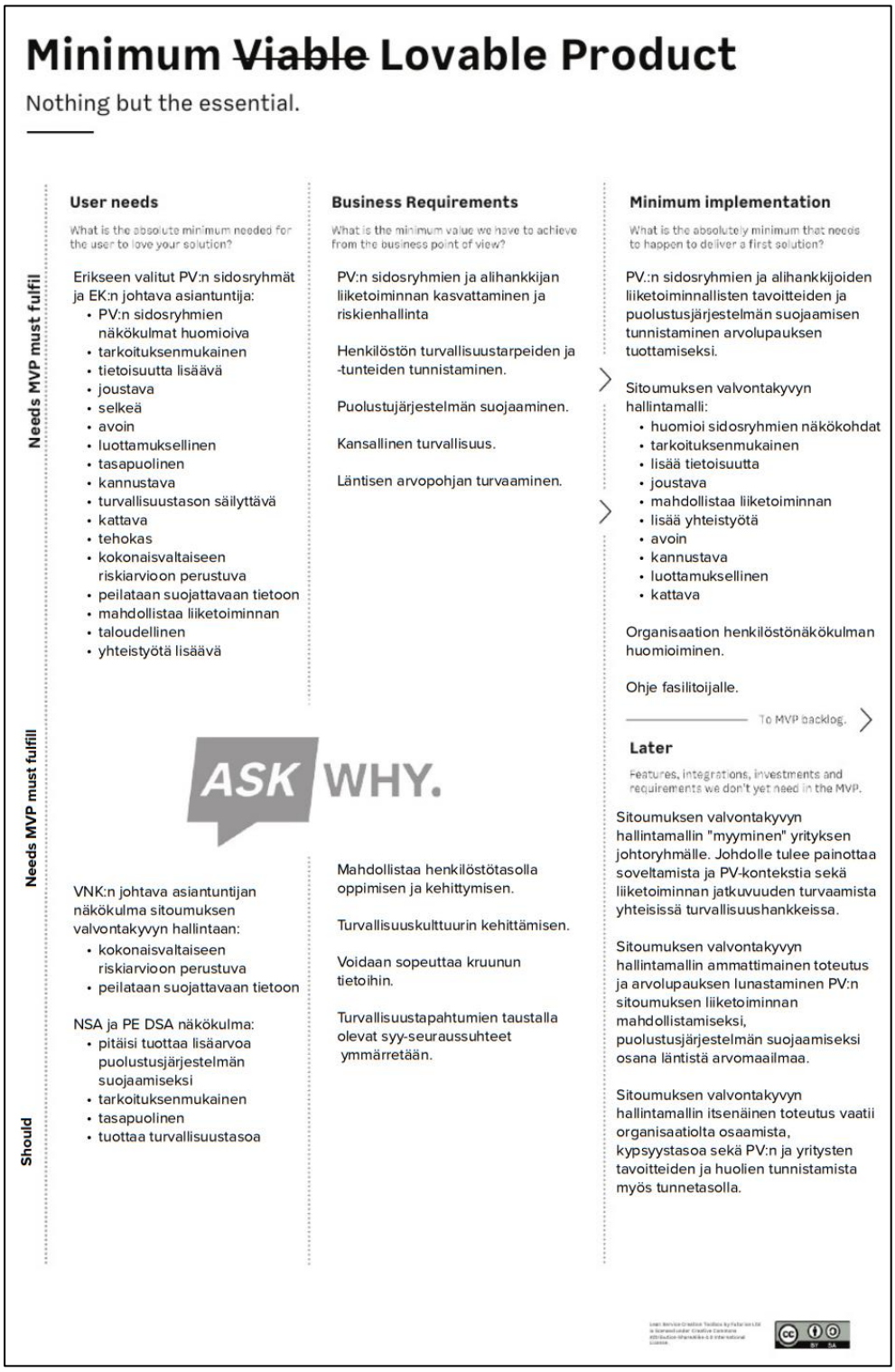
Fake advertisement – The first prototype:

Lisäarvon tuottaminen PV:n sidosryhmien ja alihankkijoiden liiketoimintaan, henkilöstön turvallisuustarpeeseen, monitasoiseen luottamukseen, puolustusjärjestelmän suojaamiseen ja Suomen turvallisuuteen osana läntistä maailmaa!

Koko henkilöstö on valmis sitoutumaan vastuulliseen turvallisuustoimintaan ja uskottaviin kontrolleihin, ilmoitusmenettelyihin ja jatkuvaan kehittämiseen.

Yritysten asiakkaat ja kumppanit arvostavat saavutettua turvallisuustasoa. PV on valmis maksamaan vastuullisesta turvallisuudesta. Luottamus on turvallisuusluokitelluissa hankkeissa tärkeä asia.

9: Turvallisuusmuotoilu, Minimun ~~Viable~~ Lovable Product



Minimum ~~Viable~~ Lovable Product

Nothing but the essential.

Needs MVP must fulfil

Needs MVP must fulfil

Should

User needs

What is the absolute minimum needed for the user to love your solution?

Erikseen valitut PV:n sidosryhmät ja EK:n johtava asiantuntija:

- PV:n sidosryhmien näkökulmat huomioiva
- tarkoituksenmukainen
- tietoisuutta lisäävä
- joustava
- selkeä
- avoin
- luottamuksellinen
- tasapuolinen
- kannustava
- turvallisuustason säilyttävä
- kattava
- tehokas
- kokonaisvaltaiseen riskiarvioon perustuva
- peilataan suojattavaan tietoon
- mahdollistaa liiketoiminnan
- taloudellinen
- yhteistyötä lisäävä

VNK:n johtava asiantuntijan näkökulma sitoumuksen valvontakyvyn hallintaan:

- kokonaisvaltaiseen riskiarvioon perustuva
- peilataan suojattavaan tietoon

NSA ja PE DSA näkökulma:

- pitäisi tuottaa lisäarvoa puolustusjärjestelmän suojaamiseksi
- tarkoituksenmukainen
- tasapuolinen
- tuottaa turvallisuustasoa

Business Requirements

What is the minimum value we have to achieve from the business point of view?

PV:n sidosryhmien ja alihankkijan liiketoiminnan kasvattaminen ja riskienhallinta

Henkilöstön turvallisuustarpeiden ja -tunteiden tunnistaminen.

Puolustujärjestelmän suojaaminen.

Kansallinen turvallisuus.

Läntisen arvopohjan turvaaminen.

Mahdollistaa henkilöstötasolla oppimisen ja kehittymisen.

Turvallisuuskulttuurin kehittämisen.

Voidaan sopeuttaa kruunun tietoihin.

Turvallisuustapahtumien taustalla olevat syy-seuraussuhteet ymmärretään.

Minimum implementation

What is the absolutely minimum that needs to happen to deliver a first solution?

PV.:n sidosryhmien ja alihankkijoiden liiketoiminnallisten tavoitteiden ja puolustusjärjestelmän suojaamisen tunnistaminen arvolupauksen tuottamiseksi.

Sitoumuksen valvontakyvyn hallintamalli:

- huomioi sidosryhmien näkökohdat
- tarkoituksenmukainen
- lisää tietoisuutta
- joustava
- mahdollistaa liiketoiminnan
- lisää yhteistyötä
- avoin
- kannustava
- luottamuksellinen
- kattava

Organisaation henkilöstönäkökulman huomioiminen.

Ohje fasilitoijalle.

To MVP backlog.

Later

Features, integrations, investments and requirements we don't yet need in the MVP.

Sitoumuksen valvontakyvyn hallintamallin "myyminen" yrityksen johtoryhmälle. Johdolle tulee painottaa soveltamista ja PV-kontekstia sekä liiketoiminnan jatkuvuuden turvaamista yhteisissä turvallisuushankkeissa.

Sitoumuksen valvontakyvyn hallintamallin ammattimainen toteutus ja arvolupauksen lunastaminen PV:n sitoumuksen liiketoiminnan mahdollistamiseksi, puolustusjärjestelmän suojaamiseksi osana läntistä arvomaailmaa.

Sitoumuksen valvontakyvyn hallintamallin itsenäinen toteutus vaatii organisaatiolta osaamista, kypsyystasoa sekä PV:n ja yritysten tavoitteiden ja huolien tunnistamista myös tunnetasolla.

ASK WHY.

8 Lyhenteet

ASIS	American Society for Industrial Security
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
COSO	Committee Of Sponsoring Organizations
EK	Elinkeinoelämän keskusliitto
ERM	Enterprise Risk Management
ESRM	Enterprise Security Risk Management
HF	Human Factor
ISO	International Organization for Standardization
Katakri	Kansallinen turvallisuusauditointikriteeristö
NSA	National Security Authority
DSA	Designated Security Authority
PE	Pääesikunta
PV	Puolustusvoimat
Supo	Suojelupoliisi
VNK	Valtioneuvoston kanslia

9 Lähteet

Haastattelut

Heinonen, H. 2023. Head of Information Security. Aktia Pankki Oyj. Helsinki, Arkadiankatu 4-6, 00100. Haastattelu 8.6.2023.

Huusko, J. 2023. Lippueamiraali. Pääesikunnan valmiuspäällikkö. Pääesikunta. Helsinki, Kasarmikatu 17, 00130. Haastattelu 26.5.2023.

Kaukoranta, P. 2023. Kansallinen turvallisuusviranomainen NSA. Ulkoministeriö. Helsinki, PL176, 00023. Haastattelu 28.2.2023.

Korhonen, P. 2023. Principal Consultant. Withsecure Cyber Security Services Oy. Helsinki, Tammasaarenkatu 7, 00180. Haastattelu 1.11.2023.

Nurminen, K. 2023. Senior Security and Preparedness Manager. Telia Finland Oyj. Helsinki, Pasilan asema-aukio 1, 00520. Haastattelu 24.4.2023.

Nykänen, R. 2023. Security Manager and Consultant. Huld Oy. Jyväskylä, Puistokatu 2 C, 40100. Haastattelu 5.4.2023.

Pallaspuro, J. 2023. Johtava asiantuntija. Valtioneuvoston kanslia. Helsinki, PL 23, 00023. Haastattelu 3.2.2023.

Pirhonen, J. 2023. Quality, Security & Privacy Lead (MTh, PhD, MSSc). Finland Tietoevry Oyj. Espoo, Keilalahdentie 2-4, 02150. Haastattelu 14.4.2023.

Rajamäki, M. 2023. Johtava asiantuntija. OTM. Varatuomari. RIMAP. Elinkeinoelämän keskusliitto. Helsinki, PL 30, 00131. Haastattelut 18.1.2023 ja 24.4.2023.

Rasila, T. 2024. Account Director. Nokia Oyj. Espoo, PL226, 00045. Haastattelu 15.1.2024.

Räsänen, I. 2023. Technical Manager. Huld Oy. Jyväskylä, Puistokatu 2 C, 40100. Haastattelu 5.4.2023.

Aalto PRO, 18. TJK-luennot

Alanko, M. 2024. Erityisasiantuntija. Oikeusministeriö (rikoksentorjuntaneuvosto). Aalto PRO, 18. TJK-luento 17.1.2024. Fyysinen turvallisuus osana kaupunkiturvallisuutta.

Dolk, L. 2024. Erityisasiantuntija. Liikenne- ja viestintäministeriö. Aalto PRO, 18 TJK-luento 13.3.2024. Tilannekuvan rakentaminen ja raportoiminen.

Haukkovaara, T. 2023. Kyndryl Alliance Leader. IBM Northern, Central, and Eastern Europe. Chairman of the Board. Aalto PRO, 18. TJK-luento 14.4.2023. Tietoturvallisuus osana organisaation strategiaa.

Heinonen, H. 2023. Director. Head of Information Security. CISO. Aktia Pankki Oyj. Aalto PRO, 18. TJK-luento 13.4.2023. Moderni tietoturvajohtaminen Case Aktia Pankki Oyj.

Korpiola, L. 2023. Toimitusjohtaja. Recado Oy. Aalto PRO, 18. TJK-luento 27.1.2023. Vaikuttaminen ja turvallisuusviestintä mediayhteiskunnassa.

Limnéll, J. 2022. Kansanedustaja ja Aalto-yliopiston kyberturvallisuuden työelämäprofessori (ST, sotatieteiden tohtori). Aalto PRO, 18. TJK-luento 10.11.2022. Turvallisuuden strategisen johtamisen merkitys organisaatiossa.

Maula, H. 2023. Viestintä- ja brändijohtaja (VTM, FL, KTT). UPM-Kymmene Oyj. Aalto PRO, 18. TJK-luento 26.1.2023. Turvallisuusviestinnän kivijalan rakentaminen.

Mikkonen, J. 2024. Toimitusjohtaja. Securitas Oy. Aalto PRO, 18. TJK-luento 17.1.2024. Fyysisen turvallisuuden muutosajurit ja niihin vastaaminen.

Mukkala, T. 2022. Head of Enterprise Risk Management and Insurances, Fortum Oyj. Aalto PRO, 18. TJK-luento 13.12.2022. Enterprise risk management (ERM) ja turvallisuus, järkiliitto vai valtataistelu?

Paavilainen, T. 2023. VP, Head of Global Risk Management. Kone Oyj. Aalto PRO, 18. TJK-luento 9.11.2023. Riskienhallinta, jatkuvuussuunnittelu ja toipuminen.

Pennanen, J. 2023. Tietoturvallisuuspäällikkö. Fingrid Oyj. Aalto PRO, 18. TJK-luento 14.4.2023. Tietoturvakriittisen järjestelmän suojaaminen – case Findgrid.

Pirhonen, J. 2023. Quality, Security & Privacy Lead (MTh, PhD, MSSc). Finland Tietoevry Oyj. Aalto PRO, 18. TJK-luento 12.-14.4.2023. Kumppaneiden tietoturvakyvykkyyden arvioiminen.

Raivio, T. 2023. Johtaja (TkT). Gaia Consulting Oy. Aalto PRO, 18. TJK-luento 24.5.2023. Vastuullisuusturvallisuus.

Rajamäki, M. 2023. Johtava asiantuntija (OTM, varatuomari, Turvallisuusjohdon koulutusohjelma, Johtamisen erikoisammattitutkinto, RIMAP). Elinkeinoelämän keskusliito. Aalto PRO, 18. TJK-luento 13.12.2022. Kokonaisvaltainen riskienhallinta.

Sallinen, S. 2023. Turvallisuuspäällikkö. LähiTapiola. Aalto PRO, 18. TJK-luento 16.3.2023. Uhkatilanteiden hallinta ja henkilöturvallisuuden ohjelma.

Sarvas, R. 2023. Työelämäprofessori. Aalto yliopisto. Aalto PRO, 18. TJK-luennot 12.12.2022 ja 24.5.2023. Turvallisuusmuotoilu.

Seppälä, T. 2023. Työelämäprofessori (TkT, KTM). Aalto PRO, 18. TJK-luento 12.4.2023. Digitaalinen murros tietoturvallisuuden kehyksenä.

Seppänen, A. 2023. Johtava lääkäri (MD, PhD, eMBA). Niuvanniemen sairaala. Aalto PRO, 18. TJK-luento 15.3.2023. Riskihenkilöt organisaatioissa.

Teperi, A-M. 2023. Tutkimusprofessori (FT). Työterveyslaitos. Aalto PRO, 18. TJK-luento 12.12.2023. Safety II ja inhimilliset tekijät turvallisuudessa.

Toimela, E. 2023. Johdon konsultti. Partneri, ICG Innotiimi Oy. Sopimusarvioija (DI) KIWA Inspecta. Aalto PRO, 18. TJK-luento 25.5.2023. Ympäristöriskien tunnistaminen, hallinta ja vaikutusten arviointi.

Waittinen, M. 2023. Erikoistutkija (FM, KM, Masterof Security). Turun yliopisto. Aalto PRO, 18. TJK-luento 5.10.2023. Organisaation turvallisuusosaaminen ja toistuvan harjoittelun merkitys.

Ylitalo, J. 2022 ja 2023. Yliopistonlehtori (TkT, tekniikan tohtori). Aaltoyliopisto. Aalto PRO, 18. TJK-luennot 11.11.2022. Minä turvallisuusvaikuttajana ja –johtajana. 26.1.2023 Vaikuttaminen, itsensä johtaminen ja voimavaraisuus. 8.11.2023 Jatkuva ammatillinen kehittyminen.

Tutkimukset

Buckingham, M. & Goodall, A. 2019. ADP Research Institute's Global Study of Engagement, The Power of Hidden Teams 2019. https://hbr.org/2019/05/the-power-of-hidden-teams Viitattu 18.12.2022.

Lopputyön kysely 2022. Valvontamalliin liittyvät tavoitteet? Valvontamalliin liittyvät huolet? Muuta huomioitavaa? Vastaajia 30. Aineisto on lopputyön laatijan hallussa. Helsinki.

Kirjallisuus

ASIS ESRM. 2019. ASIS International Enterprise Security Risk Management (ESRM) Guideline. Professional Standards Board ISBN 978-1934904-96-1. USA. 30 s.

Katakri 2020. Kansallinen turvallisuusauditointikriteeristö. Turvallisuuden auditointityökalu viranomaisille. Traficom ISBN 978-952-311-726-6. Helsinki. 115 s.

Teperi, A-M. 2023. Ihminen turvallisuuden tekijänä. Gaudeamus Oy ISBN 978-952-345-221-3. Helsinki. 413 s.

The Lean Service Creation Handbook. 2019. The Lean Way to Create: Loveable Services, Better Future, Sussessful Business, Future-Capable Organisation. Futurice Oy ISBN 978-952-69378-0-9. Estonia. 93 s.

Standardi

SFS-ISO 31000. 2018. Riskienhallinta. Ohjeet. Helsinki: Suomen standardisoimisliitto. 39 s.

Verkkosivustot

Verkkosivut on tarkastettu 3.2.2024.

Aalto PRO. Aalto University Professional Development. 2022. 18. Turvallisuusjohdon koulutusohjelma. https://aaltoee.fi/ohjemat/turvallisuusjohdon-koulutusohjelma-tjk

Allianz Global Corporate & Speciality. 2023-2024. Allianz Risk Barometer. https://commercial.allianz.com/news-and-insights/reports/allianz-risk-brmeter.html

COSO ERM. 2017. Committee of Sponsoring Organizations Enterprise Risk Management (ERM) Guideline. https://coso.org/ guidance-erm

Cybersecurity & Infrastructure Security Agency (CISA). 2023. Defining Insider Threats. https:/cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Ilta-Sanomat 28.12.2020. Niinistö sanoi presidentin kanslian sähköpostitse välittämässä kommentissaan STT:lle. https://is.fi/digitoday/tietoturva/art-2000007707896.html

Kaariste, R. 2017. Yritysturvallisuusselvitykset. Käsikirja turvallisuusselvityksen laatimisesta pääesikunnassa. Projektityö. Aalto PRO, 14. Turvallisuusjohdon koulutusohjelman lopputyö. https://aaltoee.fi/media/aalto-ee-publications/tjk/kaariste_reijo_14_tjk_kehitysprojekti.pdf

Puolustusvoimat. 2023. Pääesikunnan tiedusteluosasto. https://puolustusvoimat.fi/tietoa-meista/paaesikunta/tiedusteluosasto

Suojelupoliisi. 2022. Suojelupoliisin kansallisen turvallisuuden katsaus. https://supo.fi/documents/38197657/39761266/Kansallisen-turvallisuuden-katsaus_2022_FI.pdf/5d27d290-ed6c-d682-f122-5cff2d61e99e/Kansallisen-turvallisuuden-katsaus_2022_FI.pdf?t=1697008722 440

Suojelupoliisi. 2023. Sinäkin voit olla värväyksen kohde. https://supo.fi/varvays

Turvallisuusselvityslaki 19.9.2014/726. 5. luku Yritysturvallisuusselvitys, 40 § Yrityksen sitoumus. https://finlex.fi/fi/laki/ajatasa /2014/20140726

Työterveyslaitos. 2023. Työturvallisuus, ihmisen toiminta turvallisuudessa ja inhimilliset tekijät. https://ttl.fi/teemat/tyoturvallsuu s/ihmisen-toiminta-turvallisuudessa-ja-inhimilliset-tekijat

Ulkoministeriö. 2023. Kansallinen turvallisuusviranomainen (National Security Authority, NSA). https://um.fi/kansallinen-tur vallisuusviranomainen

Yleisradio 26.11.2022. Ykkösaamussa vieraana puolustusvoimain komentaja, kenraali Timo Kivinen. https://areena.yle.fi/1-50971025 Poistunut 26.11.2023.