

Kehdosta hautaan

Kokonaisturvallisuuden hallinta tietojärjestelmän elinkaaren eri vaiheissa

Turvallisuusjohdon koulutusohjelma

Lopputyöraportti

Flyktman, Jari

Puolustusvoimat

Brisbane 5.3.2024

Aalto University Executive Education and Professional Development

Tiivistelmä

Tässä lopputyössä tarkastellaan tietojärjestelmän elinkaaren aikaista turvallisuushallintaa. Erityisesti huomion kohteena ovat edellytykset vaatimukseenmukaisen tietojärjestelmän perustamiselle sekä turvallisuuden harkitulle ja suunnitelmalliselle ylläpidolle järjestelmän koko elinkaaren ajan alkaen suunnittelusta ja hankinnasta, päättyen järjestelmän käytöstä poistamiseen.

Tavoite on kirjallinen synteesi turvallisuusjohtamisen menetelmistä, jotka vaikuttavat tietojärjestelmien turvallisuuteen niiden elinkaaren eri vaiheissa. Näkökulman aiheeseen antavat erilaiset tunnustetut ICT-alan toimintakehykset ja hallintamallit, kuten ITIL ja liittyvät ISO-standardit sekä turvallisuuskriittisten organisaatioiden säännöt ja ohjeet.

Työn tarkoitus on osoittaa keskitetyn kokonaishallintamallin hyödyt ja tarpeellisuus palvelutoimittajan näkökulmasta.

Sisältö

1	Johdanto	8
2	Tutkimuksen esittely	10
3	Työn lähtökohdat ja tavoitteet.....	11
4	Elinkaaren määritelmät ja vaiheet	13
4.1	Elinkaaren määritelmä.....	13
4.2	Työssä käytettävä määritelmä	14
4.3	Elinkaaren ja vaatimuksenmukaisuuden merkitys turvallisuuden hallinnassa	14
4.4	Vaatimuksenmukaisuus.....	15
4.5	Elinkaaren konkretiaa tietojärjestelmän turvallisuuden näkökulmasta.....	16
5	Tietoturvan sekä hallintajärjestelmän määrittely ja suunnittelu.....	19
5.1	Tietoturvan suunnittelu	21
5.2	Henkilöturvallisuuden huomioiminen.....	22
5.3	Fyysisen turvallisuuden huomioiminen	22
5.4	Työkalut turvallisuuden suunnitteluun.....	24
6	Tietojärjestelmän elinkaaren turvallisuusvaatimusten hallinta	26
6.1	Hallintajärjestelmiä ja niiden eroja	27
7	Hallintamallit.....	31
7.1	Standardointimalli eli auditointi, akkreditointi ja sertifiointi.....	31
7.2	Hallintajärjestelmän sertifiointi.....	32
8	Turvallisuuden huomioiminen kilpailutuksen ja hankinnan suunnittelussa	35
8.1	Turvallisuustoimenpiteiden mitoitus.....	35
8.2	Suojattavan tiedon merkitys	36
8.3	Luottamuksellisuuden, eheyden ja saatavuuden tasapaino	38
8.4	Hankintalaki, julkisuusnäkökohdat ja turvallisuus.....	39
8.5	Tietojärjestelmän elinkaaren aikainen tuki	41
8.6	Palveluiden ulkoistamisen hankinta	42
9	Käyttöönotto.....	44
10	Ylläpito.....	45
11	Käytöstä poisto.....	46
12	Yhteenveto	48
13	Loppupäätelmät.....	50
14	Lähteet.....	52
15	Kuvaluettelo	58

1 Johdanto

Kybertoimintaympäristön ilmiöt monipuolistuvat ja kehittyvät jatkuvasti kiihtyvällä vauhdilla teknologisen kehityksen myötä. Esimerkiksi tekoälyjärjestelmien mahdollistama automaatio ja kvanttietokoneiden mukanaan tuoma merkittävä laskentatehon kasvu asettavat tietojärjestelmien ylläpidolle ja suojaamiselle kasvavia haasteita. Kyberympäristön toimijoiden resurssit ja kyvyt kasvavat saman aikaisesti, mutta eivät välttämättä yhtä nopeasti. Tämä asettaa haasteita tietojärjestelmien elinkaaren suunnitelmalliselle ylläpidolle ja kehittämiselle.

Tässä lopputyössä tarkastellaan tietojärjestelmän elinkaaren aikaista turvallisuushallintaa. Erityisesti huomion kohteena ovat edellytykset vaatimuksenmukaisen tietojärjestelmän turvallisuustyön perustamiselle sekä harkitulle ja suunnitelmalliselle ylläpidolle järjestelmän koko elinkaaren ajan alkaen suunnittelusta ja päättyen järjestelmän käytöstä poistamiseen.

Jotta turvallisuuden hallinnan onnistumista voitaisiin arvioida, turvallisuustyötä tulee voida hallita ja hallinnan eri näkökulmia toimintaa arvioida. Tämä koskee sekä yksittäisiä turvallisuuden osa-alueita että yritysturvallisuutta ylipäätään. Arvioinnin tulee perustua puolestaan mitattaviin määreisiin. Turvallisuustoiminnan mittareista on saatavilla kohtuullisen runsaasti tutkimustietoa ja kirjallisuusaineistoa, joten niihin perehtymistä ei nähdä tarpeelliseksi tässä yhteydessä.

Tässä työssä mielenkiinnon kohteena ovat erilaiset toimintamallit, -kehykset ja laatujärjestelmät. Tarkoitus ei ole kehittää uutta mittaustapaa tai kriteeristöä, vaan pyrkimys on löytää mahdollinen vastaus kysymykseen mitä tunnistettua turvallisuuskehystä, kriteeristöä tai laatujärjestelmää käyttäen voidaan huomioida turvallisuuden eri näkökulmien vaatimuksia riittävän kattavasti ja

tämän avulla hallita turvallisuustoiminnan kokonaisuutta rajallisilla resursseilla tietojärjestelmän elinkaaren aikana.

Suoraan kaikkeen soveltuva mallia ei uskota tämän selvityksen perusteella löydettävän, mutta todennäköistä on, että löydetään riittävän hyvä tai useampia riittävän hyviä malleja, joita yhdistämällä päästään toimivaan, laadukkaaseen lopputulokseen. Selkosuomella järjestelmän tulee tuottaa toimiva malli kohtuullisella määrällä resursseja.

Tarkoitus onkin hyödyntää työn tuloksia tietojärjestelmiin liittyvän turvallisuustyön hallinnassa erityisesti erilaisiin turvallisuustarkastuksiin liittyen sekä kansallisessa että kansainvälisessä kehityksessä. Työn tekijän lähtökohtainen näkemys on, että hallintajärjestelmät ensinnäkin parantavat kykyä vastata vaatimuksenmukaisuuden vaatimuksiin erilaisista vaatimuskriteeristöistä huolimatta, että toisekseen vähentävät pidemmällä aikavälillä arviointeihin kuluvien resurssien määrää.

2 Tutkimuksen esittely

Tutkimus tehdään laadullisena tutkimuksena analysoimalla julkisista lähteistä saatavilla olevaa lähdekirjallisuutta. Lähdekirjallisuudesta tärkeimmän osan tämän työn kannalta muodostavat erilaiset standardit ja direktiivit, joista esimerkkeinä voidaan mainita tietoturvallisuuden ja palveluiden hallintaan liittyvät SFS-ISO-standardit sekä NATO- ja EU-direktiivit. Tutkimuksia ja tietokirjallisuutta on hyödynnetty soveltuvilta osin avartamaan ymmärtämystä käsiteltävästä aiheesta

3 Työn lähtökohdat ja tavoitteet

Lopputyöraportin nimenä on ”Kehdosta hautaan”. Tämä nimi on kuvaava, vaikkakin lähtökohdaltaan virheellinen. Kattaahan se vain osan oppikirjojen mukaisesta tietojärjestelmän elinkaaresta. Kiitos kuitenkin Suomi-rokin klassikkoalbumeihin kuuluvalla Tuomari Nurmion ja Köyhien Ystävät ”Valo yössä” kappaleelle työn nimen inspiroimisesta, vaikkei kappaleen sanoitus tätä aihepiiriä kosketa edes kaukaisesti.

Otsikon virheellisyys johtuu siitä, että tietojärjestelmän syntymisen tulee olla harkittu ja suunnitelmallinen, vaatimuksiin perustuva päätös. Koska suunnitelmallisuus on tietojärjestelmän toteutumisen ehtona, tulee tämän osuuden alkaa jo ennen tietojärjestelmän ”syntymää”. Vastaavasti parhaat tulokset saavutetaan, kun muutkin tietojärjestelmän elinkaaren aikaiset toimenpiteet tehdään suunnitellusti.

Tietojärjestelmän elinkaaren eri vaiheiden suunnittelusta on julkaistu varsin kattavasti kirjallisuutta ja tutkimuksia sekä oma standardi ISO/IEC 15288:2023 (International Organization for Standardization, 2023). Tietojärjestelmäturvallisuus huomioidaan lähes kaikissa tavalla tai toisella, mutta näkökulma on usein varsin suppea ja kontekstisidonnainen. Esimerkiksi sovelluskehityksessä näkökulma on usein riippuvainen käytettävästä sovelluskehitysmallista; Digi- ja väestötietoviraston (DVV) ”Turvallinen sovelluskehitys” -oppaassa kohdassa Yleiset tietoturva-periaatteet todetaan ”Kussakin roolissa toimiva henkilö tutustuu itselleen olennaisiin periaatteisiin ja huolehtii niiden täyttymisestä oman työnsä kontekstissa” (Digi- ja väestötietovirasto DVV, 2020)”. Tällöin kokonaisuuden tietoturvan voidaan katsoa olevan yksittäisen kehittäjän vastuulla. Näkökulma on sinällään oikea kyseisessä kontekstissa, mutta kaukana holistisesta eikä ota riittävästi huomioon kokonaisuuden turvallisuuden varmistamista. Onko kokonaisuuden huomioiminen sitten edes mahdollista tai tarpeellista sovelluskehityksen osalta? Voidaan ajatella, että ei, sillä kaikkeen ei voida eikä kannata vaikuttaa kyseisessä tehtävässä. Eli

kokonaisturvallisuuteen vaikuttavien *tekijöiden* voidaan nähdä näin ollen olevan riippuvaista kontekstista, jolloin tämä riippuvuus tulee ottaa huomioon kokonaisturvallisuudessa.

Tässä työssä tarkastelukulma pyritään pitämään holistisena, mikä tarkoittaa määritelmän mukaan ”...kokonaisuuden näkökulmaan pyrkivää, että kokonaisuuden näkökulmasta määräytyvää...” (Tieteen termipankki, 2016). Apuvälineenä holistiseen lähestymistapaan toimii systeemiajattelu, joka yhden määritelmän mukaan ”on ymmärtämisen apuväline, jolla voidaan kuvata monimutkaisien järjestelmien vaikuttavia osia ja näiden toiminnan yhteistulosta. Toisin kuin perinteinen analyysi, se ei pyri jakamaan tutkittavaa kohdetta osiin, vaan pyrkii ymmärtämään, miten eri osaset vaikuttavat kokonaisturvallisuuteen. Systeemiajattelun avulla yritetään ymmärtää jonkin todellisen maailman osaa rakentamalla vuorovaikutusmalleja niistä asioista, jotka vaikuttavat tutkittavaan asiaan.” (Mielonen, ei pvm). Suomen Itsenäisyyden Juhlarahaston (SITRA) vieraileva tutkija Joss Colchester kuvasi systeemiajattelua puolestaan seuraavasti ”Systeemiajattelu on paradigma, joka auttaa meitä tarkastelemaan viheliäisten ongelmien keskinäisriippuvaista luonnetta – tarkastelemaan verkostoja ja muutoksen dynamiikkaa staattisten tilannekuvien sijaan. Systeemiajattelun avulla voimme havaita kompleksisten ilmiöiden taustalla olevat rakenteet. Tämä auttaa meitä hahmottamaan, mihin kohdistuvilla teoilla voidaan saada suuri vipuvaikutus ja mistä pieni. Systeemiajattelun avulla voimme löytää vipuvarsia aikamme vaikeimpiin haasteisiin.” (Colchester, 2019). Systeemiajattelun tarkoitus on siis auttaa ymmärtämään vaikuttavien tekijöiden välisiä yhteyksiä ja niiden yhteisvaikutusta kokonaisturvallisuuteen, kuten turvallisuuteen.

Holistisesta näkökulmasta haasteena on, että se hajottaa väistämättä fokuksen. Tämän vuoksi tässä työssä on rajauksia, jotka ovat edellytys edes jonkinlaisen polttopisteen tai kohdennuksen säilyttämiseksi työn kirjoittamisen aikana. Olen rajannut käsiteltävän Sanastokeskuksen määritelmän mukaan siten, että termi ”Tietojärjestelmä” on ”Tietojärjestelmän muodostavat tiedot ja niiden käsittelysäännöt, käsittelyn henkilö- ja laiteresurssit sekä tiedonsiirtolaitteet ja toimintaohjeet.” (Sanastokeskus, 1993; Sanastokeskus, 2023; Sanastokeskus, 2023)

4 Elinkaaren määritelmät ja vaiheet

Laki julkisen hallinnon tiedonhallinnasta 13§ määrää, että ”Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan” (Oikeusministeriö Finlex, 2019).

4.1 Elinkaaren määritelmä

Elinkaari kuvataan normaalisti toisiaan seuraavina vaiheina. ”Suosituskokoelma tiettyjen tietoturvaluussäännösten soveltamisesta” mukaan ”Tietojärjestelmän elinkaari alkaa siihen liittyvästä tarvekartoituksesta ja päättyy tietojärjestelmän käytöstä poistoon”. Tietojärjestelmän elinkaari kattaa siis kaikki tällä välillä olevat vaiheet, jotka ovat määrittely ja suunnittelu, kilpailutus ja hankinta, toteutus ja kehitys, käyttöönotto, ylläpito sekä käytöstä poisto (Valtiovarainministeriö, 2020).

Toisaalla ja toisissa konteksteissa edellä käytettyä elinkaaren käsitettä kuvataan termillä ”elinjakso”. Esimerkiksi ympäristötieteissä käytetty elinkaaren käsite on laajempi ja se kattaa tuotteen vaiheet raaka-aineiden hankinnasta tuotteesta syntyvien jätteiden loppukäsittelyyn asti. Koneen, laitteen tai järjestelmän elinjakso muodostuu yleisesti ottaen suunnittelun ja rakentamisen vaatimasta ajasta, sekä eliniästä, jonka aikana kohde on missä tahansa käytössä kenellä tahansa. Elinjakso päättyy käytöstä poistoon, jonka jälkeen tuote poistuu käytöstä (Kortelainen, et al., 2021). Määritelmät eivät varsinaisesti ole ristiriitaisia, mutta eivät yksiselitteisiä tai täydellisiääkään. Systemiajattelun perspektiivistä molemmat määritelmät sisältävät oleellisia asioita, mutta tämä riippuu käsittelijän perspektiivistä. Poliittisstrategisesta kokonaisturvallisuuden näkökulmasta käytettävien raaka-aineiden alkuperä on hyvinkin tarpeellinen tieto mahdollisten uhkien tunnistamiseksi, mutta yksittäisen yrityksen tai valtion viraston kannalta vaikuttaminen siihen on mahdollista. Esimerkkinä tästä on riippuvuus kiinalaisesta alkutuotannosta, raaka-aineiden jalostuksesta sekä tuotannosta.

4.2 Työssä käytettävä määritelmä

Yhteenvedona voitaneen todeta, että kokonaisen tietojärjestelmän elinkaari on pidempi kuin useimpien sen yksittäisten komponenttien elinjakso pois lukien kiinteät rakenteet ja rakennelmat. Koska elinjakson määritelmä ei sovellu tietojärjestelmäkäyttöön ainakaan turvallisuusluokitellun tiedon käsittelyssä, käytän selkeyden vuoksi tässä työssä Valtiovarainministeriön julkaisun mukaista elinkaaren määritelmää, jonka taustalla on lain määritelmä: ”Tietojärjestelmän elinkaari alkaa siihen liittyvästä tarvekartoituksesta ja päättyy tietojärjestelmän käytöstä poistoon” (Valtiovarainministeriö, 2020). Järjestelmän elinkaari ei siis tässä työssä sisällä kiinteitä tietoverkkoja (media), tiloja tai LVIS- tai muita vastaavia järjestelmiä, vaikka niiden vaikutus tietojärjestelmän turvallisuuteen onkin merkittävä, erityisesti kyberturvallisuuden kontekstissa.

Holistisessa lähestymistavassa tulisi kuitenkin ottaa huomioon kokonaisuus, esimerkiksi toimitusketjut, että raaka-aineiden hankintaan tai käytettyjen laitteiden hävitykseen liittyvät ympäristönäkökulmat, vaikka ne eivät varsinaisesti määritelmän mukaiseen elinkaareen kuulu. Nämä ovat kuitenkin merkittävä osa kestäväen kehityksen mallin mukaista avointa toimintaa ja liittyvät myös turvallisuuteen, joten niitä ei voida jättää täysin huomiotta. Työssä pyritäänkin rajatusti huomioimaan tämä turvallisuuden laajempi konteksti kirjattun määritelmän ohella. Osaltaan tämä rajausta ja sen laajentaminen kertovat siitä, että oppikirjamaiset määritelmät ovat väistämättä vajaita toisesta tarkastelukulmasta katsoen.

4.3 Elinkaaren ja vaatimuksenmukaisuuden merkitys turvallisuuden hallinnassa

Miksi järjestelmän elinkaarella ja sen turvallisuuden hallinnalla on merkitystä?

Tietojärjestelmäkokonaisuudet muodostuvat useista komponenteista ja osajärjestelmistä, joiden elinjaksot ovat hyvinkin eri mittaisia ja joiden turvallisuuden suunnittelu tapahtuu siten eri aikoina ja eri viitekehyksiä, lakeja sekä turvallisuusmääräyksiä noudattaen. Kun edellä mainittuja asioita noudatetaan, kutsutaan sitä vaatimuksenmukaisuuden noudattamiseksi. Eri aikoina vaatimuksenmukaisuuden vaatimus voi siis olla erilainen. Jokaisen tarkastuksen yhteydessä järjestelmän toteutus pitää kuitenkin huolehtia viimeisimpien,

hyväksyttävissä olevien vaatimusten mukaiseksi. Tämä ei ole mahdollista, jos ei tunneta sitä, miten asia on toteutettu ja mitä pitäisi tehdä vaatimuksenmukaisuuden täyttämiseksi nykyisten vaatimusten mukaan.

4.4 Vaatimuksenmukaisuus

Vaatimuksenmukaisuus määritellään seuraavasti: ”toiminnan ominaisuus, joka ilmentää sitä, noudatetaanko toiminnassa sekä sille asetettuja erityisiä että sitä koskevia yleisiä ehtoja, sääntöjä, säädöksiä tai eettisiä normeja” (Sanastokeskus, 2023). Englannin kielellä vaatimuksenmukaisuus vastaa tässä asiayhteydessä lähinnä sanaa *compliance* (määräysten mukaisuus), joka on ennen kaikkea tekniseen toteutukseen liittyvä. Joissakin yhteyksissä käytetään myös englanninkielistä sanaa *confirmity*, esimerkiksi vaatimuksen mukaisuuden vahvistaminen on *confirmity assessment* (Sanastokeskus, 2023). Vaatimuksenmukaisuuteen ja standardointiin liittyvät termit ovat määritelty laajemmin asiakirjassa SFS-EN 45020 Standardization and related activities. General vocabulary (Suomen Standardisoimisliitto SFS ry, 2012). Tässä yhteydessä on kuitenkin huomattava, että vaikka suomen kielen sana vaatimuksenmukaisuus kääntyykin sekä *compliance* että *confirmity*, tulee termien käytössä olla varovainen, sillä muilla kielillä merkitys saattaa vaihdella.

Vaatimuksenmukaisuuden seuranta ja sen merkitys on tärkeää, koska vaatimuksenmukaisuutta todistetusti osoittamalla voidaan näyttää se, että noudatamme lakeja, määräyksiä, ohjeita ja parhaita käytäntöjä siten, kuten olemme joko velvoitettuja tekemään tai olemme itse luvanneet tehdä. Yrityksellä tähän johtavat asiakkaiden vaatimukset esim. standardin kuten ISO-SFS 27001 tai 20000-1 noudattamisesta. Näitä sopimuksessa vaatimalla asiakas voi puolestaan osoittaa omalta osaltaan edellyttävänsä hyväksytyjen käytäntöjen noudattamista sekä noudattavansa itse lain edellyttämää varovaisuutta toimittajiensa suhteen. Vaatimuksenmukaisuuden noudattamisella osoitetaan yrityksen tai yhteisön olevan vaaditun luottamuksen arvoisia sille osoitetussa tehtävässä. Luottamuksella on tässä yhteydessä suuri merkitys, sillä ilman luottamusta yhteiskunta ei voi tai kykene toimimaan sujuvasti. Vaatimuksenmukaisuuden osoittaminen ja suunniteltu hallinta onkin merkittävä asia liiketoiminnan sekä koko yhteiskunnan luotettavuuden ja toimivuuden kannalta.

ISO Standardi 37301 toteaa “Organizations that aim to be successful in the long term need to establish and maintain a culture of compliance, considering the needs and expectations of interested parties. Compliance is therefore not

only the basis, but also an opportunity, for a successful and sustainable organization” (International Organization for Standardization, 2021). Suomen nettuna lainauksen keskeinen sisältö on, että “Organisaatiot, jotka tähtäävät menestykseen pitkällä tähtäimellä, täytyy perustaa vaatimuksenmukaisuuden kulttuuri huomioiden kiinnostuneiden osapuolten tarpeet ja odotukset. Vaatimuksenmukaisuus ei siis ole vain perusta, vaan myös mahdollisuus menestyksekkäälle ja kestäväälle organisaatiolle” (käännös kirjoittajan).

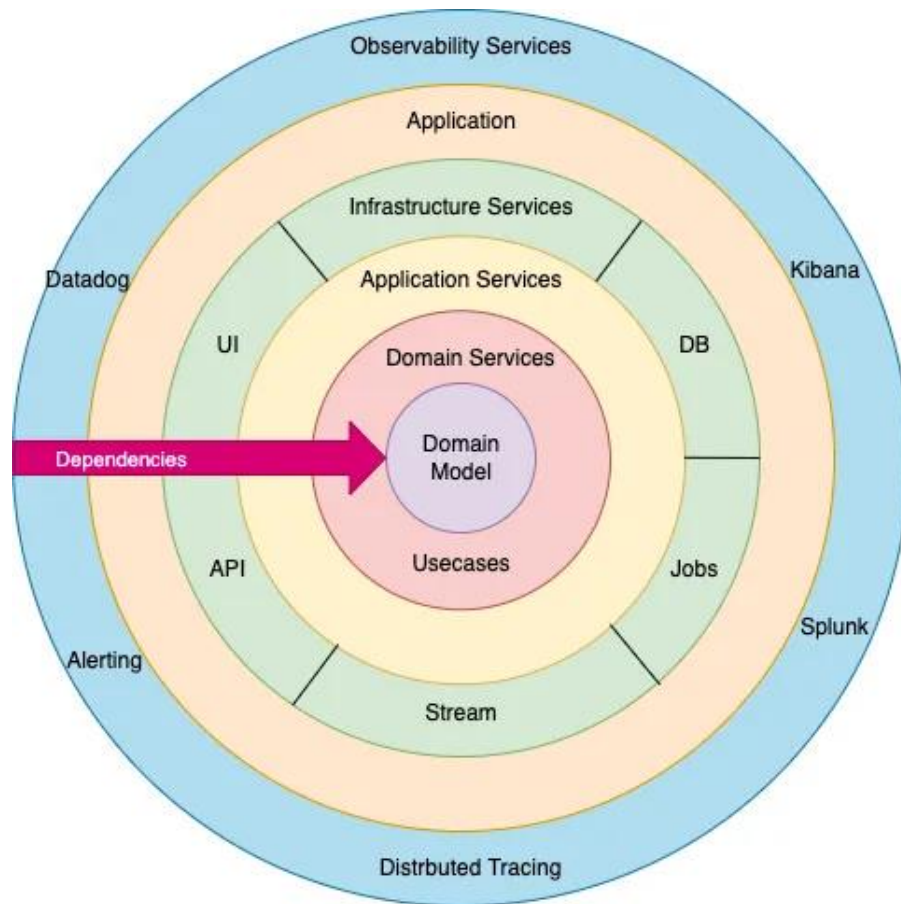
4.5 Elinkaaren konkretiaa tietojärjestelmän turvallisuuden näkökulmasta

Kun puhutaan tietojärjestelmän elinkaaresta, mitä se tarkoittaa konkreettisesti tasolla?

Lyhin elinkaari tietojärjestelmissä on raudalla (hardware), esim. työasemilla ja palvelinlaitteilla, noin 3-5 vuotta. Verkkolaitteiden, kuten kytkimien, reitittimien, palomuurien ja kuormantasainten elinkaari vaihtelee keskimäärin 3-8 vuoden välillä. Laitteiden turvallisuuteen sekä elinkaareen vaikuttavat lisäksi laiteohjelmistojen lisenssit, joiden eri versioiden elinkaari on vielä laitteidenkin elinkaarta lyhyempi muutamasta kuukaudesta muutamaan vuoteen. Laitteissa käytettävissä olevat ominaisuudet määräytyvät sekä laitteen komponenttien suorituskyvyn että laitesovellusten (firmware jne.) mukaan, vaatimukset suorituskyvylle puolestaan kasvavat tekniikan ja ominaisuuksien kehittyessä. Lisäksi tulee huomioida eri sovelluskomponenteista löytyvät haavoittuvuudet sekä niiden korjaukset, jotka tulee vaatimuksenmukaisuuden hallitsemiseksi tehdä, vaikka uusia ominaisuuksia ei päivitysten yhteydessä tulisikaan. Tämä edellyttää luotettavia toimittajia kautta koko toimitusketjun sekä palvelu-, ylläpito- ja lisenssisopimuksia, jotta vaatimuksenmukaisuus ylipäätään kyetään säilyttämään.

Laitteita pidempi elinkaari voi olla käytettävillä ohjelmistoilla. Tässä yhteydessä on huomioitava se, että sovellukset yleensä päivittyvät ja kehittyvät monta kertaa elinkaarensa aikana. Yhdessä laitteessa toimii useita eri ohjelmistoja eri tasoilla. Lähimpänä käyttäjää ovat sovelluspalvelut tai loppukäyttäjäpalvelut, kuten käytettävät sovellukset, niiden alla käyttöjärjestelmä, jonka alla virtualisointikerroksia (1..n), jonka alla on laitteiston toimintaa ohjaavia sovelluksia. Tätä arkkitehtuurimallia kutsutaan sipulimalliksi, jonka kaikki kerrokset ovat riippuvaisia toisistaan ja siten edellyttävät eri

kerrosten saumatonta yhteistyötä ja yhteensopivuutta. Esimerkki tästä arkkitehtuurimallista on esitetty alla.



Kuva 1 Esimerkki kerroksittaisesta arkkitehtuurista (Onion-architecture)
(Lähde: <https://medium.com/expedia-group-tech/onion-architecture-deed8a554423>)

Pidempää elinkaarta edustavat kiinteät rakenteet, esim. tietoliikenneverkot, tai saatavuuden ja jatkuvuuden kannalta kriittiset LVIS- tai varavoimajärjestelmät. Toisaalta kiinteät tilat, joissa järjestelmien palvelutuotanto on ja missä niitä ylläpidetään, tulee ottaa huomioon järjestelmän turvallisuutta suunniteltaessa. Tilat ja rakenteet ovat muita järjestelmän osia pitkäikäisempiä ja todennäköisimmin niitä hyödynnetään muiden järjestelmien käytössä aiempien järjestelmien muiden komponenttien elinjakson jo päätyttyä.

Yhdessä edellä kerrotut osat muodostavat järjestelmäinfrastruktuurin, järjestelmän johon toiset järjestelmät nojautuvat ja joka muodostaa laajan, verrattain monimutkaiset kokonaisuuden. Pöyhösen mukaan ”Tästä näkökulmasta katsottuna on merkittävää mallintaa ja analysoida jokainen infrastruktuurin osa osana monimutkaista verkkoa, joka muodostaa yleisen infrastruktuurin” (Pöyhönen, 2020).

Jotta kaikki yleiseen infrastruktuuriin ja sen turvallisuuteen liittyvä saadaan hallittua, vaaditaan niin elinkaaren hallintaa kuin turvallisuuden hallintaa, jotka tätä kautta liittyvät toisiinsa. Elinkaaren hallinta edellyttää sopimuksia, jotka ovat kaupallista toimintaa, jotka edellyttävät sopimusten hallintaa. Näin tätä ketjua purkamalla voidaan edellä kuvattu monimutkainen verkko purkaa systeemiin, tunnistettaviin ja huomioitaviin osiin.

Kuuluvatko sitten sopimukset järjestelmän elinkaareen? Kyllä, sillä sopimukset määrittävät järjestelmän elinkaaren aikaisia kustannuksia, lisäksi ilman sopimusten hallintaa ei vaatimuksenmukaisuus mielestäni täyty esimerkiksi riskienhallinnan näkökulmasta katsottuna. Erityisen tärkeää tämä on, jos käytetään palveluntuottajan palveluita, joiden tietoturvallisesta ja vaatimuksenmukaisesta toteutuksesta tulee palvelun ostajan varmistua. Ensimmäiseksi mieleen tulevia esimerkkejä ulkoistetuista palveluista ovat eri tarjoajien pilvipalvelut, valtionhallinnon lailla määrätyt palveluntuottajat Suomen Erillisverkot (ERVE) ja Valtion tieto- ja viestintätekniikkakeskus Valtori. Tietyin varauksin lakisääteistä palvelua ja sopimuksia tarjoavat myös julkishallinnon yhteishankintayksikkö Hansel sekä Valtion talous- ja henkilöstöhallinnon palvelukeskus Palkeet. Viranomaisen tulee suunnitella ja ylläpitää digitaaliset palvelunsa siten, että tietoturvallisuudesta, tietosuojasta, löydettävyydestä ja helppokäyttöisyydestä on varmistuttu (Oikeusministeriö, 2019). Kaikissa tapauksissa ostajan tulee siis varmistua palvelun vaatimuksenmukaisuudesta, mutta muistaa se, että tämä on vain puolet kokonaisuudesta. Vaatimuksenmukaisuudesta tulee huolehtia myös omassa toiminnassa ja huolehtia siitä, että palvelun tuottajan vaatimuksenmukaisuuden täyttymistä seurataan sopimuksien mahdollistamalla tavalla ja tuodaan tämä tieto mukaan omaan vaatimuksenmukaisuuden hallintaan.

Kun kyse on näin laajasta ja monimutkaisesta kokonaisuudesta, mikä olisi oikea tapa hallita sitä? Todennäköisesti kaikilla turvallisuuteen ja elinkaaren hallintaan vaikuttavilla osa-alueilla on omat vaatimuksensa ja standardinsa vaatimuksenmukaisuutensa osoittamiseksi, esimerkkeinä jo aiemmin mainitut ISO-SFS 27001 ja 20000–1.

5 Tietoturvan sekä hallintajärjestelmän määrittely ja suunnittelu

Mikä olisi järkevä tapa lähteä määrittelemään ja suunnittelemaan tietoturvan hallintajärjestelmää? Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista määrää, että ”Palvelutuottajan on tarkoituksenmukaisin keinoin varmistettava, että sen tukipalvelun tuottamiseen käytettävä tietojärjestelmä on suunniteltu, valmistettu ja toimii tietoturvasuutta ja tietosuojaa koskevien lakien ja niiden nojalla annettujen säännösten sekä yhteentoimivuutta koskevien kansallisten määritysten mukaisesti” (Oikeusministeriö, 2016). Lain määräyksestä voi johtaa vaatimuksen siitä, että hallintajärjestelmälle asetettavat vaatimukset otetaan mukaan jo tietojärjestelmän suunnitteluvaiheessa ja erityisesti suunniteltaessa tietoturvaa.

Kysyttäessä ChatGPT:ltä, joka on ”AI-chatbot eli tekoälyyn perustuva vuorovaikutusohjelmisto” (Keystone Education Group Oy, 2023) ”Mitä tulee huomioida tietojärjestelmän tietoturvan määrittelyssä?” saadaan seuraava vastaus:

”Tietojärjestelmän tietoturvan määrittelyssä on tärkeää huomioida useita keskeisiä tekijöitä. Tässä on joitakin keskeisiä seikkoja, jotka tulisi ottaa huomioon:

1. Riskinarviointi: Arvioi tietojärjestelmän riskejä tunnistamalla mahdolliset uhkat, haavoittuvuudet ja hyökkäyspisteet. Tunnista myös tietojärjestelmän arvokkaat resurssit, kuten asiakastiedot, yrityssalaisuudet tai muut arkaluonteiset tiedot.
2. Tietojen luokittelu: Luokittele tiedot niiden arkaluonteisuuden ja luotamuksellisuuden perusteella. Määrittele eri tietoturvatason vaatimukset eri tiedostoluokille.

3. Pääsynhallinta: Määrittele käyttäjien ja järjestelmänvalvojien oikeudet ja vastuut. Varmista, että käyttäjät saavat vain tarvitsemansa oikeudet ja että pääsy arkaluontoisiin tietoihin on rajoitettu tarvittaviin henkilöihin.
4. Vahva tunnistautuminen: Käytä vahvoja tunnistusmenetelmiä, kuten monivaiheista tunnistautumista (esim. salasana ja tekstiviestivahvistus), varmistaaksesi käyttäjien henkilöllisyyden.
5. Salaus: Käytä salausta tiedonsiirrossa ja tallennuksessa varmistaaksesi, että tiedot eivät ole luettavissa tai ymmärrettävissä ulkopuolisille.
6. Haittaohjelmien torjunta: Asenna ja päivitä haittaohjelmien torjuntaohjelmisto (esim. virustorjunta) suojaamaan järjestelmää haittaohjelmilta, kuten viruksilta, matoilta ja troijalaisilta.
7. Tietojen varmuuskopiointi: Luo säännöllisesti varmuuskopioita tietojärjestelmästä varmistaaksesi, että tiedot voidaan palauttaa mahdollisen tietoturvaloukkauksen tai tietojen menetyksen tapauksessa.
8. Jatkuvuuden varmistaminen: Suunnittele ja toteuta jatkuvuuden varmistamistoimenpiteitä, kuten varajärjestelmät ja suunnitelmat, jotka mahdollistavat tietojärjestelmän toiminnan jatkumisen häiriötilanteissa.
9. Tietoturvakoulutus: Järjestä koulutusta käyttäjille ja henkilökunnalle tietoturvaohjeiden noudattamisesta, tietojen luottamuksellisuudesta ja vastuullisesta tietojenkäsittelystä.
10. Seuranta ja auditointi: Aseta järjestelmä, joka seuraa tietojärjestelmän toimintaa ja valvoo poikkeamia. Tee säännöllisiä tarkastuksia ja auditointeja tietoturvan tehokkuuden varmistamiseksi.

On myös tärkeää huomioda, että tietoturvan määrittely on jatkuvaa prosessia, jota on tarkistettava ja päivitettävä säännöllisesti vastaamaan uusia uhkia ja haasteita, joita tietojärjestelmä voi kohdata”.

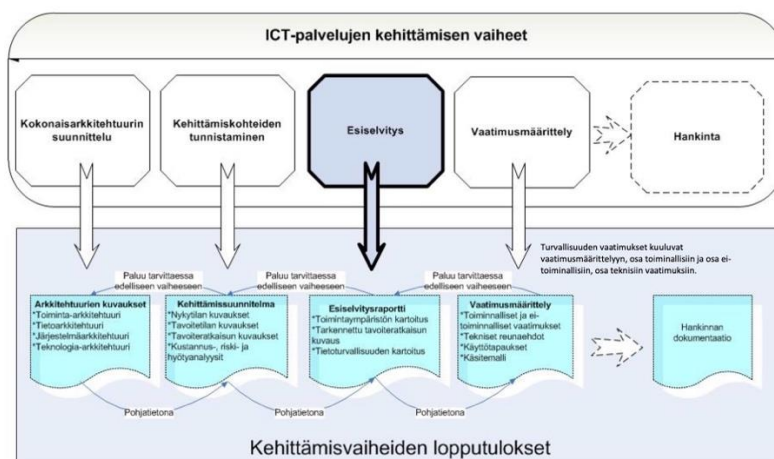
ChatGPT:n vastaus ei ole laisinkaan huono ja sitä noudattamalla pääsee turvallisuuden puolesta jo varsin pitkälle. Edelleen joiltakin osin vastaus on kuitenkin vajavainen. Rajoittuneisuuden syy selviää, kun kysyy ChatGPT:n määrittelyä tietojärjestelmästä ”Tietojärjestelmä on organisaation tai yrityksen käyttämä järjestelmä, joka käsittää tiedon tallentamisen, käsittelyn ja jakamisen tietotekniikan avulla. Se koostuu laitteistoista, ohjelmistoista, tietokannoista, verkoista ja ihmisistä, jotka yhdessä toimivat tiedon hallinnassa ja

liiketoiminnan tukemisessa”. Tämän mukaan ChatGPT tuottaa järkevän, annetun kysymyksen kontekstiin sopivan vastauksen. Itse korostaisin ChatGPT:n vastauksesta erityisesti ensimmäistä kohtaa, jonka nimeäisin kuitenkin riskiarvion sijasta uhka-arvioksi, sekä viimeistä kohtaa seuranta ja auditointi, erityisesti huomioiden jälkikaneetti jatkuvasta prosessista, joka puolestaan toimiakseen edellyttää hallintajärjestelmää. Vastauksesta selviää hyvin se, kuinka laajasti erilaisia asioita on huomioitava, vaikka vuorovaikutusohjelmiston näkökulmaa moitinkin rajoittuneeksi.

5.1 Tietoturvan suunnittelu

Joka tapauksessa tietoturvan suunnittelu kuuluu osana projektin tai hankkeen kokonaisuuden suunnitteluun, jota ohjaavat organisaation operatiivinen johto ja muut sidosryhmät.

Esimerkiksi Julkisen hallinnon tietohallinnon neuvottelukunta JUHTA toteaa jo vanhentuneessa ohjeessaan JHS 172 ICT-palvelujen kehittäminen: Esiselvitys, että ”Organisaation korkean tason vaatimukset (kuten TTS, lain-säädäntö, kehittämisohjelma) toimivat pohjana esiselvityksen kohteena olevalle tietojärjestelmälle.” (Julkisen hallinnon tietohallinnon neuvottelukunta, 2010). Turvallisuudelle asetettavat vaatimukset eivät siis poikkea muista vaatimuksista, ja ne on otettava huomioon toiminallisissa, ei-toiminallisissa kuin teknisissäkin vaatimuksissa.



Kuva 2 ICT-palvelujen kehittämisen vaiheet mukailien lähde (Julkisen hallinnon tietohallinnon neuvottelukunta, 2010)

5.2 Henkilöturvallisuuden huomioiminen

Henkilöriskeillä tarkoitetaan henkilöstöstä aiheutuvia riskejä yrityksen toiminnalle ja riskejä, joita yrityksen henkilöstöön voi kohdistua. (Suomen Riskienhallintayhdistys, 2012 - 2024). Tässä työssä ei tarkastella niinkään henkilöstöön kohdistuvia riskejä, vaan riskejä, joita henkilöstöstä voi koitua yritykselle tai yhteisölle.

Perustan turvallisuuden toteuttamiselle tietojärjestelmän elinkaaren aikana antaa henkilöturvallisuuden huomioiminen. Jos henkilöturvallisuutta ei ole otettu huomioon, on jätetty huomioimatta todennäköisin turvallisuusriski. Esimerkiksi Seppälän mukaan ”Huolimattomasti toimivat ihmiset ovat suurin riski yrityksen tietoturvallisuudelle” (Seppänen, 2012) ja Ncubezin tutkimuksen mukaan inhimilliset virheet ovat ”kyberturvallisuuden huolenaihe ja heikoin lenkki” (Ncubezi, 2022).

Henkilöturvallisuus on jo itsessään monitahoinen ja kompleksinen asia. Mistä sitten saadaan eväitä turvallisuuden suunnitteluun koskien henkilöturvallisuutta? Kansallisen turvallisuusviranomaisen KATAKRI 2020 arviointikriteeristön osat T09-T13 käsittelevät henkilöturvallisuutta (Kansallinen turvallisuusviranomainen, 2021). KATAKRI 2020 noudattaa kansallista lainsäädäntöä, joka on pitkälti yhtenäinen Euroopan Unionin neuvoston luokiteltavan tiedon suojaamista koskevan päätöksen 2013/488/EU kanssa (Official Journal of the European Union, 2013). Toinen tiedon lähde on julkisesti saatavilla oleva NATO:n direktiivi DIRECTIVE ON PERSONNEL SECURITY, AC/35-D/2000-REV8 (NATO North Atlantic Treaty Organization, 2020).

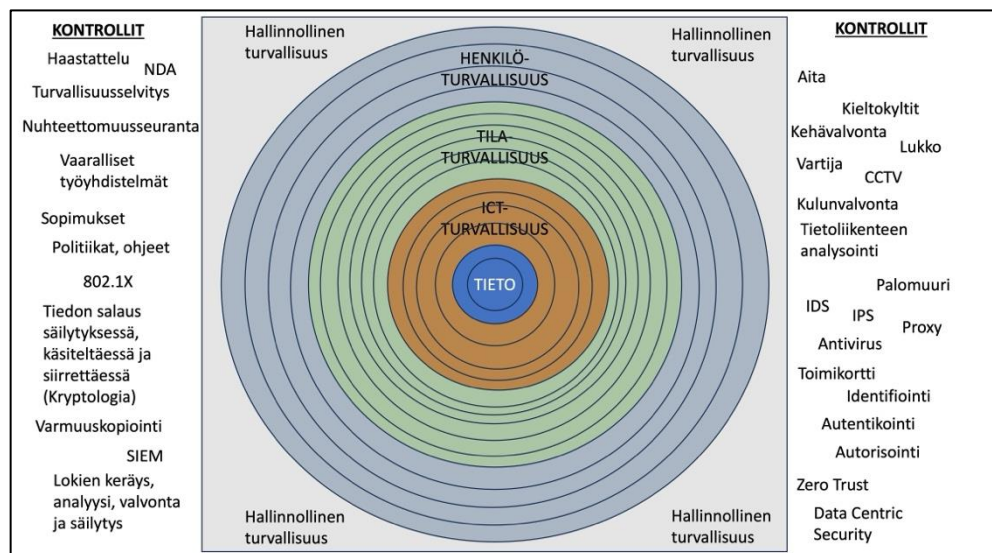
Edellä mainitut asiakirjat ohjeistavat kuitenkin vasta henkilöturvallisuuteen liittyvät peruseriaatteet. Henkilöturvallisuuden näkökulmat tulee ottaa huomioon kaikessa turvallisuuteen liittyvissä asioissa alkaen turvallisuuspolitiikoista, ohjeista ja etenkin koulutuksessa.

5.3 Fyysisen turvallisuuden huomioiminen

Yksi selkeä puute ChatGPT:n vastauksessa on tilaturvallisuuden täydellinen huomioimatta jättäminen. Tietojärjestelmä on aina sijoitettava sellaiseen tilaan, joka täyttää vaatimuksenmukaisuuden tilaturvallisuuden, valvonnan ja vartiointin, lukituksen sekä näiden ohjauksen ja jatkuvan seurannan osalta.

Lisäksi suunnittelussa on huomioitava jatkuvuuden hallinnan kannalta tärkeät asiat, kuten esimerkiksi monennettu sähkönsyöttö, varavoiman ja lämmönhallinnan saatavuus myös häiriötilanteissa sekä näihin liittyvät kyber turvallisuuden vaikuttavat seikat, vaikkapa sivukanavaohyökkäysten estäminen. ”Uusien toimitilojen osalta fyysisten turvallisuusvaatimusten ja niiden toiminnallisten eritelmien määrittely on oltava osa toimitilojen suunnittelua ja rakenteita. Jo olemassa olevien toimitilojen osalta fyysiset turvallisuusvaatimukset on pantava täytäntöön mahdollisimman täydellisesti”. (Kansallinen turvallisuusviranomainen, 2021).

Ilman fyysisen turvallisuuden huomiointia ei siis ole mahdollista määrittellä tai rakentaa turvallista tietojärjestelmää vaatimuksenmukaisella tavalla. Vähimmilläänkin muun tietojärjestelmän suojauksen vaatimukset nousevat huomattavasti ilman fyysisen turvallisuuden vaatimusten huomiointia, eikä tulos voi olla käytännössä auditointikelpoinen. Tämä johtuu siitä, että käytännössä tarkastellut arviointikriteeristöt vaativat fyysisen turvallisuuden huomioimista niin datakeskuksissa kuin loppukäyttäjän käyttöpaikoilla arvioidessa järjestelmän kokonaisturvallisuutta. Esimerkkinä tästä on kotimaisessa kontekstissa ehkä tunnetuin arviointikriteeristö KATAKRI 2020, jossa fyysiselle turvallisuuden vaatimuksia on yksi osio koko arviointikriteeristöstä (Kansallinen turvallisuusviranomainen, 2021).



Kuva 3 Esimerkki turvallisuuden kontrolleista sipulimallina. Kuvan reunalla esitetyt turvallisuuskontrollit sijoittuvat keskellä sijaitsevan ”sipulin” eri kerroksille muodostaen kokonaisturvallisuuden vaikuttavat kontrollit.

Turvallisuutta rakennettaessa ei siis ole olemassa yhtä ”hopealuotia”, vaan asiat vaikuttavat toisiinsa monimutkaisessa systeemissä, joista kaikki olisi

huomioitava ja kontrolloitava. Jos hallintajärjestelmän tarve elinkaaren myöhemmissä vaiheissa otetaan huomioon alusta alkaen, helpottaa se nähdäkseni myös tietoturvan suunnittelua ja seurantaan jatkossa. Tältä osin olen huomannut varsin hyväksi lähtökohdaksi NATO:n julkisesti saatavilla olevan direktiivin Directive on Physical Security AC/35-D/2001-REV3 (NATO North Atlantic Treaty Organization, 2020).

5.4 Työkalut turvallisuuden suunnitteluun

Mikä sitten olisi mahdollisesti paras työkalu kuin turvallisuutta suunniteltaessa? Arviointikriteeristön hyödyntäminen tässä tarkoituksessa on mahdollista, huomioiksi tarvittavat turvallisuustekijät varsin laajalti ja tällöin sen käyttö palvelisi itseauditointia ja mahdollisesti tulevia auditointitarpeita. Ongelmana on se, että kriteeristö asettaa vaatimukset varsin löyhästi, esim. KATAKRI 2020, mikä johtaa väärin tulkinnan mahdollisuuteen. Lisähaasteena on, että kriteeristöön perustuvaan työkalu saattaa olla rajattu tiettyyn tarkastelunäkökulmaan tai tietyn valtiollisen viranomaisen käyttöön. Tällöin ei välttämättä huomioida vaikuttavia asioita laajemmassa kontekstissa kriteeristön ulkopuolelta. Edelleen on huomattava se, että arviointikriteeristöt ovat aikansa tuotteita eivätkä välttämättä ole kaikilta osin ajan tasalla.

Esimerkiksi KATAKRI 2020 tai SFS-ISO27001 turvallisuuden vaatimukset on yhdistetty yhteen dokumenttiin tai dokumenttikokoelmaan, joka uusiutuu omalla aikataulullaan. Nopeasti muuttuvassa tilanteessa vaatimukset voivat vanhentua kuitenkin nopeasti ilman, että kriteeristössä tai standardissa tätä huomioidaan riittävästi. Esimerkkeinä nousevat tällä hetkellä esiin generatiivisen tekoälyn tai kvanttitietojenkäsittelyn mahdollisesti aiheuttamat uhat. Tärkeää onkin systemaattinen, jatkuva työ huomioiden kriteeristöjen ajantasaisuuden mahdolliset puutteet. Näin siksi, että orastaviin, nopeasti ilmaantuviin uhkatekijöihin, mustiin joutseniin ja harmaisiin sarvikuonoihin, kyetään varautumaan ennakkoon ja reagoimaan heti kun aika on. Ei siis pidä jäykistyä paikalleen, vaan tarkastella muuttuvaa maailmaa mahdolliset, kaukaiseltakin tuntuvat uhkatekijät tunnistaen.

Puolustusvoimallisessa kontekstissa, joka yleensä on kykeneväinen normittamaan asioita laajasti huomioiden monia yksityiskohtia, yksi mahdollinen suunnittelutyökalu voisi olla esimerkiksi North Atlantic Treaty Organization (NATO) käyttämä Comprehensive Operations Planning Directive (COPD) (NATO North Atlantic Treaty Organization, 2010). Vaikka COPD ei ole

tarkoitettu tietojärjestelmäprojektien suunnitteluun, soveltuu siinä esitelty DOTMLPF-I (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities ja Interoperability) suunnittelumalli nähdäkseni varsin hyvin tietojärjestelmähankkeiden ja -projektienkin suunnitteluun. Tällöin tulee tunnistaa se, että termit ja käsitteet voivat olla erilaiset sotilaskielenkäytössä ja tietojärjestelmätieteessä. Esimerkkinä käytetty tilaturvallisuus sisältyy materiaaliosioon ja että ”Facilities” (something that facilitates, or makes possible an action or process), joka helposti suomennetaan laitteistoksi, laitteeksi tai laitokseksi (Sanakirja.org Solutions Oy, 2024), tarkoittaa tässä kontekstissa yhteistyökumppaneita, esim. toimintaa tukevaa teollisuutta tai palveluntarjoajia eikä esimerkiksi toiminnan mahdollistavaa tilaa tai rakennusta.

COPD mukainen suunnitteluprosessi on tarkoitettu puolustusvoimien yhteisoperaatioiden suunnitteluun ja siten huomioimaan monien erilaisten toimijoiden erilaiset tarpeet. COPD on yleinen malli ja siksi tarjoaa vain karkeat puitteet suunnitteluprosessille, joita voi ja tulee tarkentaa yksityiskohteisemmilla suunnitteluohjeilla tietoturvallisuuden tarpeisiin, jos se koetaan hyödylliseksi.

COPD edellyttääkin toimintakontekstin ja suunnitteluprosessin yksityiskohtaista osaamista – aivan kuten voi odottaa kokonaisturvallisuuden suunnittelua tekevilta. COPD ei kuitenkaan ole hallintaan, vaan suunnitteluun tarkoitettu prosessityöohje. COPD voisi siten olla mahdollinen hyvä suunnitteluvaiheen työkalu, joka antaa suunnittelumallin, mutta ei palvele hallintajärjestelmänä, joka puolestaan on tarkoitettu suunnitteluvaihetta seuraavan elinkaaren aikaisen vaatimuksenmukaisuuden seurantaan. Vähintäänkin COPD:n mukaista suunnitteluprosessia käyttäessä tulee huolehtia siitä, että turvallisuudelle asetettuja vaatimuksia seurataan. Tässä kontekstissa lähtökohta, joka on todettu toimivaksi myös kansallista kriteeristöä noudatettaessa, voisi olla ohjedokumentti Security Within The North Atlantic Treaty Organization (NATO) C-M(2002)49-REV1 liitedokumentteineen (NATO North Atlantic Treaty Organization, 2020).

6 Tietojärjestelmän elinkaaren turvallisuusvaatimusten hallinta

Mitä muita mahdollisia vaihtoehtoja sitten järjestelmähanketta vetävälle toimijalle mahdollisesti olisi tarjolla tietojärjestelmän elinkaaren aikaisen turvallisuustoiminnan hallintaan?

Kysytäänpä taasen kaikkitietävältä taholta, eli hyödynnetään toistamiseen ChatGPT:n ”älykkyyttä”.

Kysymys: Mitä kokonaisturvallisuuden laatujärjestelmää tai kriteeristöä suositellaan käytettäväksi tietojärjestelmän elinkaaren aikaisen turvallisuustoiminnan hallintaan?

”Tietojärjestelmän elinkaaren aikaisen turvallisuustoiminnan hallintaan suositellaan useita erilaisia kokonaisturvallisuuden laatujärjestelmiä tai kriteeristöjä. Tässä on muutamia suosittuja:

1. ISO 27001: ISO/IEC 27001 on kansainvälinen standardi, joka määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset. Se tarjoaa kehyksen tietojärjestelmän tietoturvallisuuden hallintaan, joka sisältää riskienhallinnan, toimintapolitiikat, ohjeet ja toimenpiteet tietoturvallisuuden ylläpitämiseksi.

2. NIST Cybersecurity Framework: National Institute of Standards and Technology (NIST) on kehittänyt kyberturvallisuuden kehyksen organisaatioille. Tämä kehys auttaa organisaatioita tunnistamaan, suojelemaan, havaitsemaan, vastaamaan ja toipumaan kyberuhkista. NIST-kehys tarjoaa joukon suosituksia, käytäntöjä ja ohjeita tietoturvallisuuden parantamiseksi.

3. ITIL (Information Technology Infrastructure Library): ITIL on kokoelma parhaita käytäntöjä IT-palvelunhallintaan. Vaikka ITIL ei ole suoranaisesti tietoturvallisuuden kehys, se tarjoaa hyödyllisiä suosituksia ja prosesseja tietojärjestelmän hallintaan, mukaan lukien tietoturvallisuusprosessit.

4. *CIS Controls: Center for Internet Security (CIS) on määritellyt 20 kriittistä tietoturvallisuuskontrollia, jotka tarjoavat ohjeita ja toimenpiteitä tietojärjestelmän suojaamiseksi yleisiltä tietoturvariskeiltä. CIS-kontrolleja voidaan soveltaa tietojärjestelmän elinkaaren eri vaiheissa.*

Nämä ovat vain joitain esimerkkejä kokonaisturvallisuuden laatujärjestelmistä tai kriteeristöistä. On tärkeää valita järjestelmä tai kriteeristö, joka sopii parhaiten organisaation tarpeisiin ja noudattaa alan parhaita käytäntöjä”.

6.1 Hallintajärjestelmiä ja niiden eroja

ChatGPT:n vastaus ei taaskaan ole keho, mutta kuitenkin kaukana täydellisestä. Näyttää siltä, että ChatGPT:tä vaivaa vahvistusharha – eli sille ei ole annettu prosessoitavaksi riittävän laajaa materiaalia tai ei ole opetettu tietoturvan, henkilöturvallisuuden ja fyysisen turvallisuuden välistä riippuvuutta. Kun ChatGPT:n tuottamaa vastausta analysoidaan, voitaisiin todeta, että tila- ja henkilöturvallisuutta ei edelleenkään välttämättä tunnisteta olennaiseksi osaksi tietoturvallisuutta mainittujen laatujärjestelmien tai kriteeristöjen toimesta.

Esim. edellä mainituista hallintamalleista Center for Internet Security, Inc®. (CIS) tunnistaa kriittiseksi omaisuuseräksi (eng. asset) ainoastaan seuraavat:

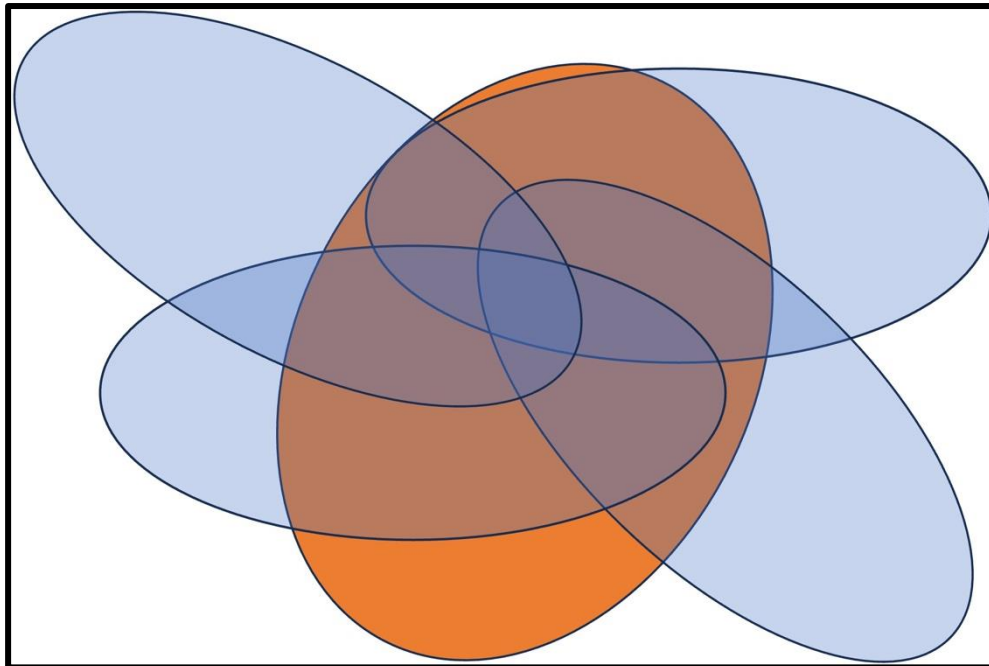
- *Network*
- *Devices*
- *Data*
- *Applications*
- *Users*

(Center for Internet Security, Inc®. (CIS), 2023)

Tässä luettelossa käyttäjät on huomioitu, mutta lähinnä päätelaitteen käyttöön liittyvissä asioissa (salasanaturvallisuus, käyttövaltuudet jne.), ei siis henkilöturvallisuuteen tai esim. henkilön rekrytoinnin aikaisiin prosesseihin, kuten taustaselvityksiin, liittyviä asioita. Tilaturvallisuutta ei tunnisteta lainkaan, eikä siten tunnisteta puutteellisen tilaturvallisuuden merkitystä esimerkiksi verkko-, laite- tai käyttäjäturvallisuudelle ja toimintojen suojaamiselle.

ITIL taasen on parhaita käytäntöjä sisältävä palvelujohtamisen malli, joka kyllä osaltaan huomioi ja tunnistaa tietoturvallisuuden, mutta tietojärjestelmän elinkaaren kannalta katsottuna vain osan. Näin ollen ITIL-mallin parhaiden käytänteiden noudattaminen ei ole yksistään ratkaisu pulmaan.

ITIL noudattaa kuitenkin pitkälti käytäntöjä, joita edellytetään ISO standardeissa, esim. SFS/ISO20000-1 ja SFS/ISO27001. Kyseiset standardit huomioivat myös tilaturvallisuuden ja henkilöturvallisuuden näkökulmat, ainakin jossakin määrin. Täydellisesti turvallisuuden eri osa-alueet kattava hallintamalli edellyttääkin eri standardien käyttämistä, jolloin standardointityö, eri standardien vaatimuksenmukaisen laadun varmistaminen ja kontrollointi sekä ylläpitoon liittyvät parhaat käytännöt työllistävät merkittävästi. Tämä työ ja sen määrä voivatkin tulla yllätyksenä, etenkin kun vaatimuksenmukaisuutta pitää osoittaa jatkuvasti akkreditoinnin ylläpitämiseksi.



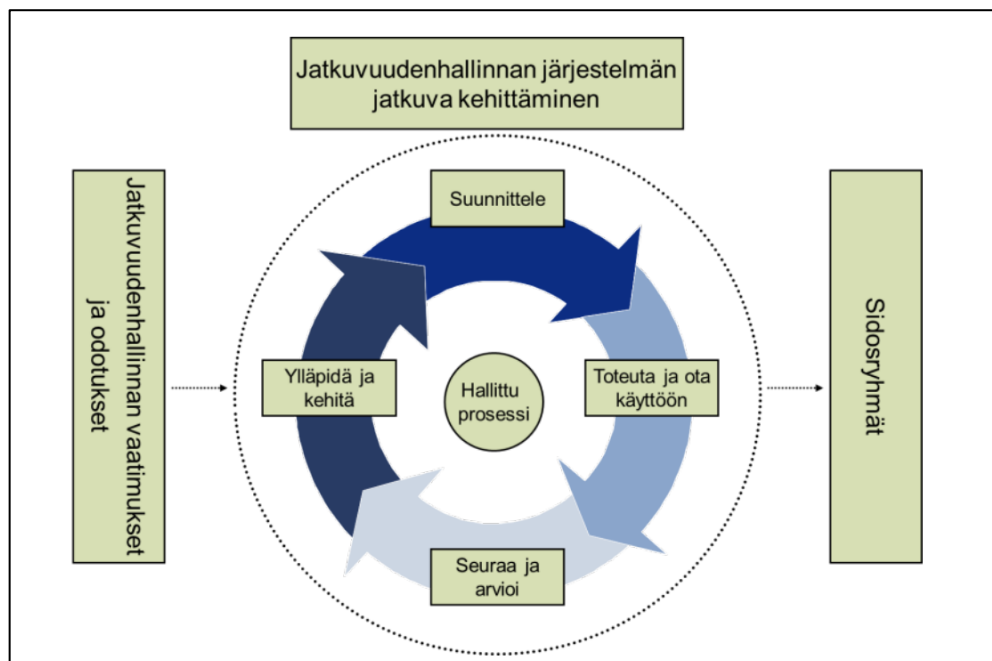
Kuva 4 Standardit tarkastelevat samaa asiaa hieman eri näkökulmista. Näin ne muodostavat osittain toistensa yli käyvän kokonaisuuden.

Yhdysvalloista lähtöisin oleva NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF) on kansainvälisesti laajasti tunnettu ja tunnustettu viitekehys turvallisuuden kehittämiseksi (NIST The National Institute of Standards and Technology, 2024). Tämä viitekehys on pohjana mm. Digi- ja väestötietoviraston DVV:n Digitaalisen turvallisuuden arkkitehtuurin viitekehykselle. Viitekehys kokoaa käytäntöjä useasta eri stan-

dardista ja se koostuu viidestä avaintoiminnosta: tunnistaminen, suojauminen, havainnointi, reagointi ja palautuminen. (Digi- ja väestötietovirasto DVV, 2023).

Edellisistä NIST ohjaa enemmän riskien tunnistamiseen ja hallintaan riskianalyysin kautta. Ainakin teoriassa NIST:in CSF ohjaa välillisesti myös fyysisen turvallisuuden hallintaan. Sen sijaan kansallinen DVV:n versio tunnistaa, että suojaamisen kannalta on olennaista ottaa huomioon erilaiset vaatimukset ja tietoturvaratkaisut tietojärjestelmien, palveluiden sekä näitä tukevan infrastruktuurin elinkaaren kaikissa vaiheissa aina kehityksestä ylläpitoon ja elinkaaren päättämiseen. Viitekehyksessä esitellyt suojaustoimenpiteet ovat kansainvälisistä tietoturvallisuuden, kyberturvallisuuden ja digitaalisen turvallisuuden standardeista johdettuja toimenpiteitä, joiden avulla organisaation on mahdollista rakentaa suojaustaan kokonaisuutena erillisten ratkaisujen sijaan (Digi- ja väestötietovirasto DVV, 2023).

Viitekehyksenä DVV:n kehys mielestäni välttää tiukkaa määrittelyä ja toimintatapojen ohjausta, jättäen siten valinnanvaraa ja vapautta toteuttajalle. Toisaalta auditoinnin ja akkreditoinnin näkökulmasta vapausastetta toteutukselle voi olla liikaakin. Tämä on syytä tunnistaa ja toimia siten, että kriteeristöjen vaatimukset ja auditoijan tulkinta siitä täytetään.



Kuva 5 Jatkuvuudenhallinnan järjestelmän jatkuva kehittäminen (Valtiovarainministeriö, 2016)

DVV:n viitekehys ohjaa myös jatkuvuudenhallinnan hallintajärjestelmän jatkuvaan kehittämiseen valtionhallinnon VAHTI-ohjeistuksen mukaisesti, jota kuvataan yllä olevassa kuvassa. Kyseinen malli noudattaa PDCA-sykliä (Plan-Do-Check-Act), joka tunnetaan myös OODA-silmukkana (OODA-loop, Observe-Orient-Decide-Act) etenkin sotilaskäytössä. Riippumatta nimestä, kyseinen malli on keskeinen puhuttaessa laadusta ja standardien hallintamalleista. Kuva 5 Jatkuvuudenhallinnan järjestelmän jatkuva kehittäminen

7 Hallintamallit

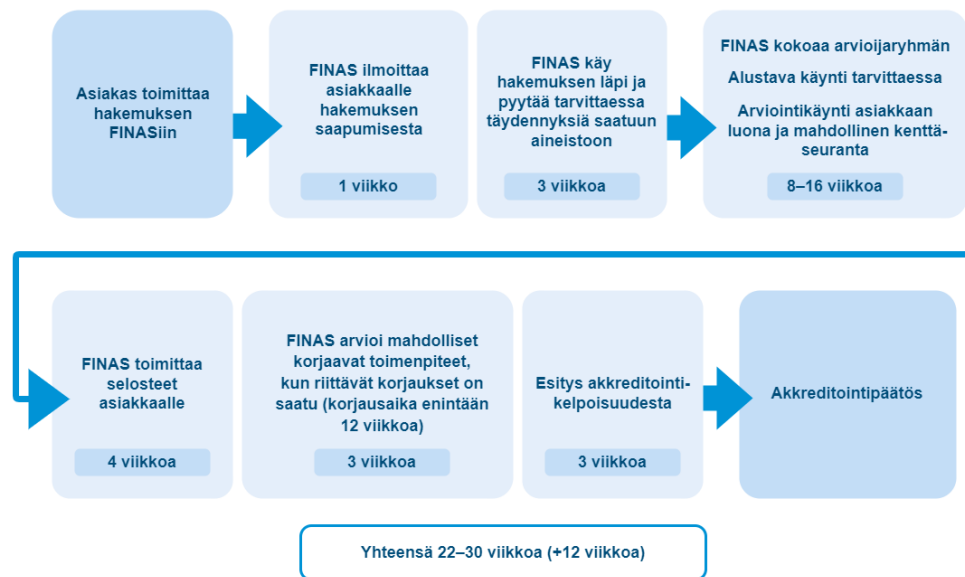
Yksi ISO-standardien akkreditoinnin edellytyksistä onkin hallintamalli ja sen dokumentoitu noudattaminen, joka todennetaan puolueettoman toimijan säännöllisin tarkastuksin joka vuosi ja auditoinnein kolmen vuoden välein. Vaatimukset akkreditoinnille ja sen määräaikaishyväksynnöille on kuvattu omassa standardissaan SFS-EN ISO/IEC 17011: 2017 Conformity assessment. Requirements for accreditation bodies accrediting conformity assessment bodies (European committee for standardization CEN, 2017).

7.1 Standardointimalli eli auditointi, akkreditointi ja sertifiointi

Edellä mainitut puolueettomat toimijat ovat standardointimallin noudattamiseen sitoutuneita ja sitoumuksensa osoittaneita organisaatioita. Standardointimallissa toimijat ovatkin eriytettyjä, eli standardointiorganisaatio, keskusliittona Suomen Standardisoimisliitto ry (SFS), julkaisee ja ylläpitää standardointidokumentteja suomeksi. Suomen kansallinen akkreditointielin (FINAS) puolestaan ”akkreditoi eli toteaa päteväksi laboratorioita, sertifiointielimiä, tarkastuslaitoksia, vertailumittausten järjestäjiä sekä ympäristö- ja päästökauppatodentajia” (FINAS Finnish Accreditation Service, 2023). FINAS:in toimintaa puolestaan ohjaa työ- ja elinkeinoministeriön nimittämä akkreditointiasiain valtuuskunta. Akkreditointielimen toimintaan ja sen riippumattomuuteen ja tasapuolisuuteen ottaa kantaa Vaatimustenmukaisuuden arviointiasioita käsittelevä neuvottelukunta ja sen pätevyys toteamistojen jaosto (FINAS Finnish Accreditation Service, 2023).

Akkreditointiprosessi – uusi hakija

Ajat ovat tavoiteaikoja, ja niihin vaikuttavat hakemuksen sisältö, laajuus sekä asiakkaan valmius akkreditointiin sekä mahdollisten korjaavien toimenpiteiden toteuttaminen ajallaan.



Kuva 6 Kuva uuden hakijan akkreditointiprosessista. (Lähde: <https://www.finas.fi/akkreditointi/Akkreditointiprosessi/Sivut/default.aspx>)

Kolmannen lenkin tässä kokonaisuudessa muodostavat sertifiointiorganisaatiot, jotka voivat olla kaupallisia toimijoita (esim. Nixu Sertifiointi, KIWA Sertifiointi, Huld Sertifiointi, KPMG IT Sertifiointi) tai viranomaisia. Sertifiointiorganisaatio on akkreditoitu, eli todetusti pätevä testaamaan ja sertifioidaan kolmansia osapuolia, se toimii eettisesti ja käyttää soveltuvaa laadunvarmistusta. FINAS Akkreditointipalvelu pitää yllä ajantasaista, kerran vuorokaudessa päivittyvää luetteloa akkreditoimistaan sertifiointiorganisaatioista (FINAS Finnish Accreditation Service, 2024).

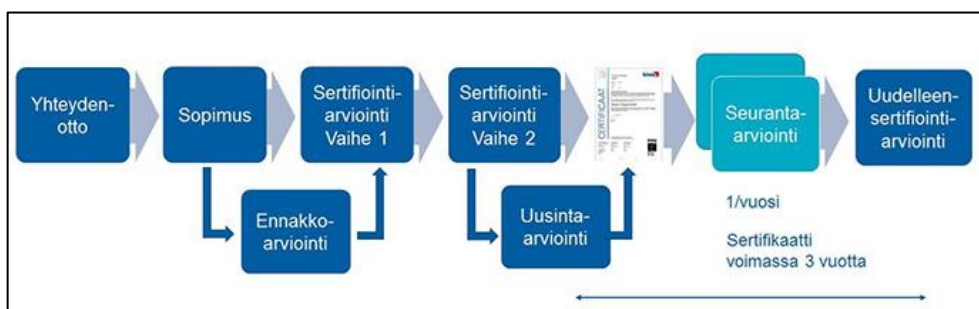
7.2 Hallintajärjestelmän sertifiointi

Sertifiointi on määritelmän mukaan arviointiin perustuvaa vaatimustenmukaisuuden arviointia. Vaatimukset on useimmiten esitetty standardeissa. Standardit voivat olla kansainvälisiä ISO, eurooppalaisia EN tai kansallisia SFS-standardeja (FINAS Finnish Accreditation Service, 2024)

Sertifiointiprosessi käynnistetään yleensä hakemuksesta vapaasti valittavan, akkreditoitun auditointiorganisaation kanssa, joista on mainittu esimerkkejä edellisessä kappaleessa 7.1 tai lakisäätöisenä auditoivan viranomaisen, eli Traficommin kanssa. Traficom toimii Suomen kansallisen turvallisuusviran-

omaisen (NSA), jona toimii ulkoministeriö, määräämänä turvallisuusviranomaisena ja kansallisena tietoturvaviranomaisena (NCSA, National Communications Security Authority), vastaten turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista (Liikenne- ja viestintävirasto kyberturvallisuuskeskus, 2023)

Auditoijasta riippumatta prosessit noudattavat pääpiirteittäin samaa kaavaa, mikä on esitetty alla olevissa kuvassa sekä taulukossa.



Kuva 7 Auditointiprosessi (Lähde: <https://www.kiwa.com/fi/fi/palvelutyypit/sertifiointi-ja-arviointi/johtamisjarjestelmat/auditointiprosessi/>)

Auditoinnissa on tärkeää huomioida suunnitelmallisuus, pitkäjänteisyys ja auditointiin kuuluva aika, mikä saattaa olla huomattavan pitkä. Auditointiin menevä aika riippuu auditoitavan organisaation olemassa olevasta toiminta- ja hallintaprosessien kypsyystasosta sekä auditoitavan kohteen tai palvelun laajuudesta.

Taulukko 1 Auditointiprosessin pääpiirteinen kulku esimerkin omaisesti

1.	informaatiotilaisuus	vapaaehtoinen
2.	hakemus auditoinnista	pakollinen, ennen sopimuksen solmimista ja auditoinnin aloittamista
3.	ennakoarviointi	vapaaehtoinen, arvioidaan auditoitavan kypsyystaso
4.	sertifiointiarviointi vaihe 1	pakollinen
5.	sertifiointiarviointi vaihe 2	pakollinen
6.	uusintaarviointi	tarvittaessa
7.	seuranta-arvioinnit	pakollisia 1 a. välein
8.	uudelleensertifiointiarviointi	pakollinen määrävälein (3 a.)
9.	arvioinnin kohdentaminen	vapaaehtoinen

Viranomaishyväksyntää vaativat järjestelmäauditoinnit ovat puolestaan riippuvaisia tarkastettavan tietojärjestelmän (vast.) tietoturvaluokasta. TLIV järjestelmät uudelleen arvioidaan 5 a. välein, TLII puolestaan enintään 3 a. vä-

lein. Itse tarkastuksen voi suorittaa tietoturvaluokasta riippuen joko tietoturvaluokkaan akkreditoitu, NCSA:n (National Communications Security Authority) hyväksymä kaupallinen toimija (turvallisuusluokat IV ja III) tai toimivaltainen viranomais (TLII).

Tietoturvallisuuden arviointilaitosten toimintaa säädellään valtiovallan toimesta lailla (Oikeusministeriö, 2011). Mainituista auditoijista Liikenne- ja viestintävirasto Traficom toimii määrättyinä tietoliikenneturvallisuusviranomaisena (National Communication Security Authority, NCSA) niissä tapauksissa, joissa on kyse kansainvälisiä sitoumuksia edellyttävästä teknisestä tietoturvallisuudesta ja tietoliikenteen turvallisuudesta. Määräyksen tehtävään on antanut Suomen kansallinen turvallisuusviranomais (NSA, National Security Authority), jona toimii Ulkoasianministeriö (Ulkoministeriö, 2023). Oman mausteensa asiaan tuo lisäksi se, että Traficom ei ole ainoa määrätty turvallisuusviranomais (DSA, Designated Security Authority), vaan esimerkiksi Suojelupoliisilla, Puolustusministeriöllä ja pääesikunnalla on omia määrättyjä, lakisääteisiä vastuitaan.

Määrätyt turvallisuusviranomaiset huolehtivatkin niille laissa kansainvälisistä tietoturvallisuusvelvoitteista (2004/588) (Oikeusministeriö, 2004) säädetyistä ja muista niille kansainvälisistä tietoturvallisuusvelvoitteista johtuvista tehtävistä. Puolustusministeriö, pääesikunta ja suojelupoliisi toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa. Tämä tarkoittaa turvallisuuden hallinnan kannalta sitä, että kokonaisturvallisuudessa tulee huomioida usean eri viranomaisen ja tarkastuslaitoksen tulkinnat ja vaatimukset, mikä puolestaan saattaa aiheuttaa tarkastustilanteessa haasteita. Soikkelin analyysin perusteella vaatimuksenmukaisuus vaikuttaa kansallisen tietoturvallisuuden osalta veteen piirretyltä viivalta, koska laki jättää varsin paljon vapausasteita sen osalta, mitä kriteereitä vasten arviointi toteutetaan (Soikkeli, 2021). Toisaalta toimivaltaisuuden jakaantuminen eri tahoille edellyttää sitä, että tarkastettavan näkökulmasta tulee hallita kokonaisturvallisuutta, ei vain yhtä (näkö)kulmaa kokonaisuudesta. Tämä korostaa kokonaisuuden hallinnan ymmärtämisen ja osaamisen tärkeyttä.

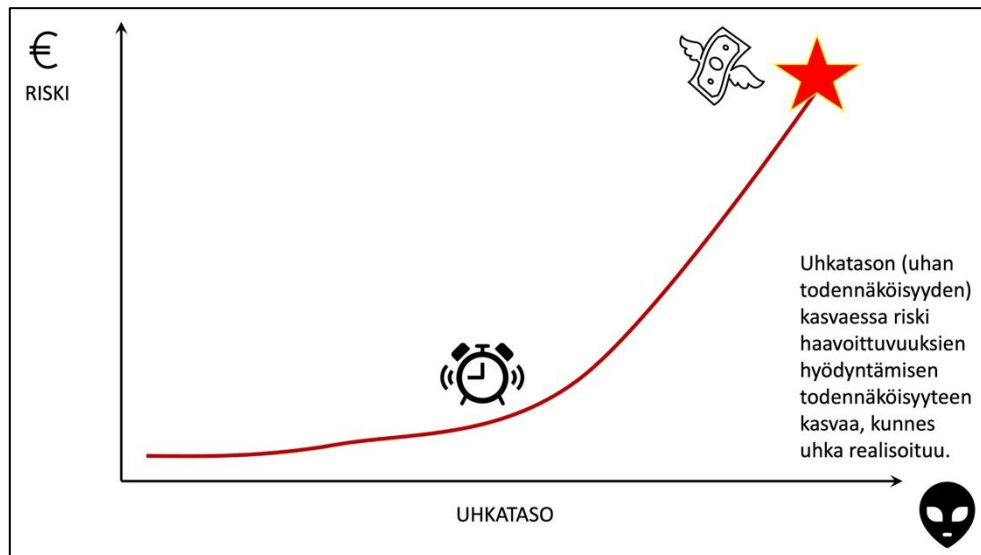
8 Turvallisuuden huomioiminen kilpailutuksen ja hankinnan suunnittelussa

Kilpailutettaessa ja hankittaessa työsuorituksia, palveluita tai materiaalia tulee alusta asti huomioida turvallisuuden vaatimukset. Haasteena usein on, että turvallisuuden huomioimisen vaade sinällään tunnistetaan, mutta miten määrittellä hankittavan palvelun tai järjestelmän turvallisuudelle asetettavat vaatimukset? Mikä on tavoiteltava vaatimus, etenkin kun tiedetään, että vaatimustason nostaminen nostaa myös kustannuksia?

Valtioneuvoston asetuksessa 681/2010 Tietoturvallisuudesta valtionhallinnossa todettiin seuraavaa ”Valtionhallinnon viranomaisen on pidettävä huolta, että tietoturvallisuuden suunnittelu hyvän tiedonhallintatavan mukaisesti perustuu viranomaisen selvityksiin ja arvioihin sen hallussa olevista asiakirjoista sekä niihin talletettujen tietojen merkityksestä ja että suunnittelussa otetaan huomioon vaatimus hyvän julkisuus- ja salassapitorakenteen toteuttamisesta tietojärjestelmissä ja että tietoturvaluustoimenpiteet mitoitetaan ottamalla huomioon suojattavien tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvaluustoimenpiteistä aiheutuvat kustannukset.” (Oikeusministeriö, 2010). Edellä oleva vaatimus tietoturvaluustoimenpiteiden oikeasta mitoitukselta voi todeta olevan oikea, vaikka aikaa asetuksen voimaantulosta on jo kulunutkin.

8.1 Turvaluustoimenpiteiden mitoitus

Avainsanoja turvallisuustason määrittelyssä ovatkin mielestäni uhkatekijät, suojattavan tiedon merkitys ja käyttötarkoitus, kustannusten ja siedettävissä olevan riskitason ollessa optimoinnin kohteena (suhteellisuusperiaate).



Kuva 8 Esimerkki suhteellisuusperiaatteesta. Uhkatason noustessa kasvaa uhan torjuntaan tarvittavien resurssien määrä, jonka suhteen tulisi löytää optimi; kohtuulliset kustannukset – siedettävä riski.

Jotta uhkatasoon käytettävät resurssit pysyisivät kohtuullisina ja riskit siedettävänä, tulee järjestelmän omistajan hyväksyä molemmat suunnitteluperusteiksi. Korkean riskin ja uhkataso tilanteissa resurssien käyttö on tätä vastaavaa, eli resurssien käyttö kasvaa. Samoin matalan riskin ja uhkataso tilanteissa resurssien käyttöä tulee tarkastella uhkatasoa vastaavasti.

8.2 Suojattavan tiedon merkitys

Suojattavan tiedon merkitystä, tai toisin sanoen tiedon paljastumisen aiheuttamia vaikutuksia voi arvioida puolestaan Valtioneuvoston asetuksen asiakirjojen turvallisuusluokittelusta valtionhallinnossa mukaisesti. Tämä tehdään arvioimalla tiedon paljastumisen aiheuttamia mahdollisia vahinkoja suojattavalle edulle seuraavalla asteikolla: lievää vahinkoa, vahinkoa, merkittävää vahinkoa, erityisen merkittävää vahinkoa aiheuttava (Oikeusministeriö, 2019).

Asteikko on osin vertailukelpoinen yhdysvaltalaisen NIST:in (National Institute of Standards and Technology) julkaiseman ”Standards for Security Categorization of Federal Information and Information Systems” (NIST The National Institute of Standards and Technology, 2004) kanssa, mutta merkittäviä eroavaisuuksiakin on. Yhdysvaltalaisessa standardissa vahinko saattaa koskea tiedon luottamuksellisuutta (Confidentiality), tiedon eheyttä (Integrity) tai tiedon saatavuutta (Availability) pelkän suojattavan edun paljastumisen (vrt. Confidentiality) ja oikeudettoman käytön lisäksi. Lisäksi tulee huo-

Turvallisuuden huomioiminen kilpailutuksen ja hankinnan suunnittelussa mata yhdysvaltalaisen standardin ”suojattavaa etua” ja ”oikeudetonta käyttöä” konkreettisemmat käsitteet, eli operaatiot, omaisuus, ja henkilöt voivat olla suojattava etu, kun suomalaisessa lainsäädännössä ei ole ”suojattavaa etua” tai ”oikeudetonta käyttöä” määritelty. Eroavaisuuksia ja samankaltaisuutta on pyritty selventämään alla olevassa taulukossa: Taulukko 2 Asetus 1101/2029 ja NIST FIPS 199 eroavaisuudet.

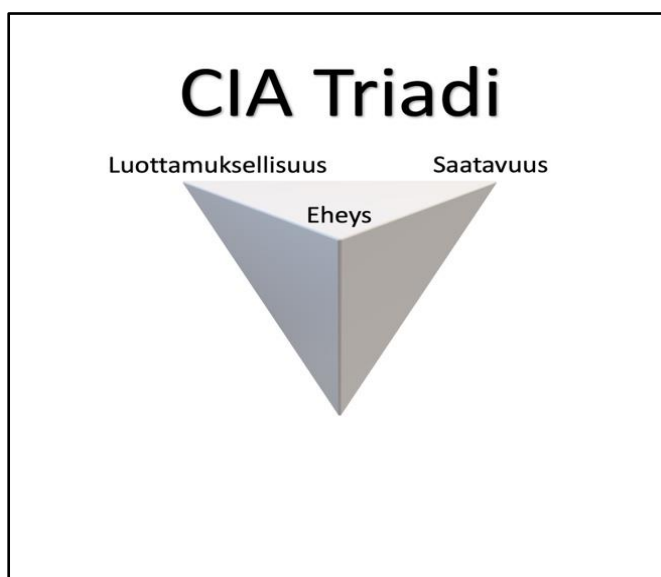
Taulukko 2 Asetus 1101/2029 ja NIST FIPS 199 eroavaisuudet

Asetus 1101/2019 (Oikeusministeriö, 2019)	NIST FIPS 199 (NIST The National Institute of Standards and Technology, 2004)	Selite
”...salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa...”	“The potential impact is...”	“The loss of confidentiality, integrity, or availability could be expected to have...”
...lievää vahinkoa...	...low...	a limited adverse
...vahinkoa...	...moderate...	a serious adverse
...merkittävä vahinkoa...	...high...	a severe or catastrophic
...erityisen suurta vahinkoa...	N/A	N/A
“...tiedonhallintalain 18 §:n 1 momentissa tarkoitettulle suojattavalle edulle”	“... effect on organizational operations, organizational assets, or individuals.”	N/A

Mielestäni lievästi parempi lähtökohta suunniteltavan tietojärjestelmän turvallisuusluokitukselle on NIST:in standardi sen konkreettisemmän määrittelyn vuoksi. Tämän käyttö ei sulje pois kansallisen asetuksen määritelmiä, vaan täsmentää niitä ja huomioi mielestäni paremmin muita vartenotettavia asioita kuten tiedon saatavuuden ja eheyden merkityksen.

8.3 Luottamuksellisuuden, eheyden ja saatavuuden tasapaino

Suomalainen asetuksen mukainen luokittelu korostaakin tiedon luottamuksellisuuden (Confidentiality) säilyttämistä tiedon eheyden (Integrity) ja saatavuuden (Availability) jäädessä huomiotta, vaikka kaikista näistä olisi tärkeää pitää kiinni. Luottamuksellisuus, eli tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, on tärkeä peruseriaate. Toisaalta tiedolla, joka ei ole tarvittaessa saatavilla, ei ole merkitystä ja edelleen tieto, jota on päästy oikeudettomasti muokkaamaan, on menettänyt arvonsa tai on pahimmassa arvoltaan jopa negatiivinen (haitallinen).



Kuva 9 Tiedon luottamuksellisuus, eheys ja saatavuus muodostavat kokonaisuuden, jossa tulee huolehtia osien tasapainosta.

Pahimmillaan luottamuksellisuuden korostaminen johtaa siihen, että eri tietoturvaluokkien järjestelmät eivät keskustele keskenään. Tämä johtaa tietojärjestelmien ja tietojen siiloutumiseen ja estää näin esimerkiksi digitalisaation hyödyntämisen siinä laajuudessa, kuin se muutoin olisi mahdollista. Luottamuksellisuuden korostaminen voi johtaa myös tiedon ylikuokittelun kaltaisiin ei-toivottaviin ilmiöihin haluttaessa pelata ”varman päälle”. Esimerkiksi Puhakaisen mukaan ”Tiedon ylikuokittelu hankaloittaa tiedon käsittelyä ja heikentää saatavuutta” (Puhakainen, 2021). Tiedon luokittelun tuleekin perustua poikkeuksetta kokonaisarviointiin.

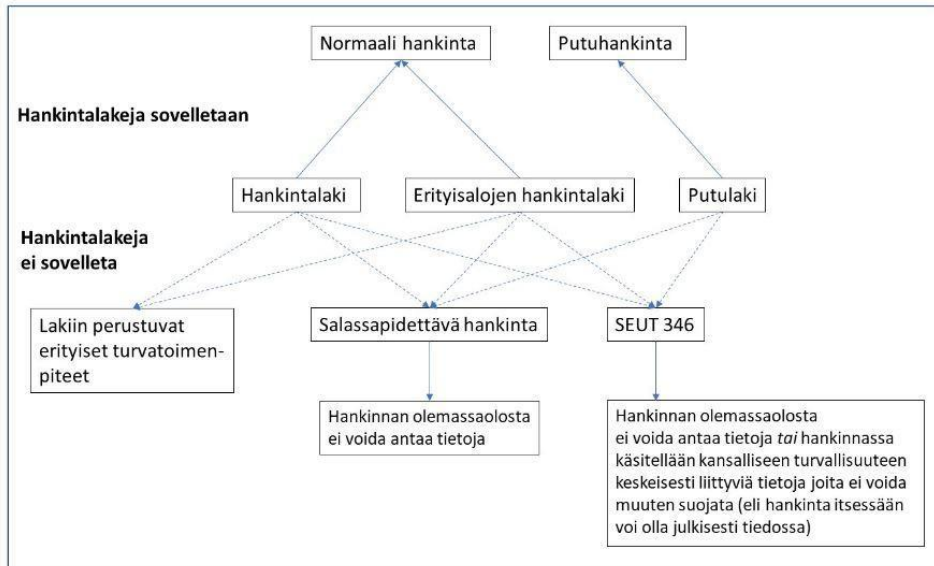
Huomioiden tosielämän kokemukset luottamuksellisuuden korostumisesta tietoa suojaattaessa, on sinällään on erikoista, että Laki sähköisen viestinnän

palveluista 917/2014 toteaa 3§:ssa tietoturvan määritelmäksi ”...*hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä*” (Oikeusministeriö, 2014). Tämän mukaan toimittaessa tietojärjestelmän suunnittelussa, toteutuksessa ja hankinnassa huomioidaan tiedon luottamuksellisuuden lisäksi eheys ja saatavuus. Vaikka tämä ei suoraan vaikutakaan vaatimukseen tietojärjestelmässä käsiteltävän tiedon tietoturvaluokasta, sillä saattaa olla välillistä vaikutusta esim. eri tietoturvaluokkien välisen tiedonvaihdon tai tiedon suojaamisen toteutuksen vuoksi. Tämän vuoksi tulee käyttää harkintaa ja ottaa eheyden sekä saatavuuden vaatimukset osaksi järjestelmän tietoturva-vaatimuksia eikä ylikorostaa luottamuksellisuutta niin kuin se olisi ainoa tapa toteuttaa asia vaatimuksenmukaisesti.

8.4 Hankintalaki, julkisuusnäkökohdat ja turvallisuus

Julkisia hankintoja säätelee Laki julkisista hankinnoista ja käyttöoikeussopimuksista, joka edellyttää hankintatietojen julkistamista laissa määritellyllä tavalla (Oikeusministeriö, 2016). Puolustus- ja turvallisuushankintoja koskevat puolestaan ”Laki julkisista puolustus- ja turvallisuushankinnoista (1531/2011)”, eli PUTU-laki, joka rajaa tietojen julkisuutta jossakin määrin sekä Sopimus Euroopan Unionin toiminnasta (SEUT) artikla 346. Artiklan 346 mukaisesti EU jäsenvaltioilla on oikeus vapauttaa tiettyjä sopimuksia tästä direktiivistä, jos tämä on välttämätöntä EU-maiden keskeisten turvallisuussetujen suojaamiseksi (Euroopan Unioni, 2016).

Suunniteltaessa hankintaa ja kilpailutusta tulee miettiä, hankitaanko tarvittava palvelu tai materiaali hankintalakia vai PUTU-lakia noudattaen. Kumpaa noudattaen hankinta tehdään, riippuu hankintayksikön näkemyksestä siitä, liittyykö hankintaan *erityisiä suojattavia tietoja*. Lain tulkitsijasta ja tulkinnaasta riippuen lain julkisuusvaatimukset saattavatkin olla turvallisuuden näkökulmasta tarkasteltuna (vähintäänkin osin) ristiriidassa turvallisuusnäkökohtien kanssa. Lisäksi hankinnan suunnittelua saattaa hankaloittaa, jos hankintayksikkö ja hankintaa valmisteleva organisaatio ovat eri.



Kuva 10 Hankintalakien soveltaminen (Lähde: <https://ptcs.fi/lainsaadannon-soveltaminen-turvallisuusorientoituneisiin-hankintoihin/>)

Suunnittelun hankaloituminen johtuu siitä, että organisaation sisälläkin eri yksiköillä saattaa olla eri näkemys siitä, mitkä ovat mahdolliset uhat, riskit ja niistä aiheutuvat haavoittuvuudet kokonaisuuden kannalta, jos hankittavan järjestelmäkokonaisuuden tietoja julkistetaan. Hankintayksikkö korostaa tehtävänsä kannalta tärkeää hankintalain noudattamista ja hankintaa tarvitseva organisaatioyksikkö puolestaan hankittavan kokonaisuuden tietojen luottamuksellisuutta, sekä hankinnan käyttökelpoisuutta, nopeutta ja ketteryyttä. Käytännön kokemukset vaihtelevatkin suuresti ja kilpailu eri yksiköiden toimivallasta ja sen rajoista saattaa tällöin haastaa turvallisuuden.

Usein nämä eroavaisuudet näkemyksissä ovat soviteltavissa, joskin tärkeää on huomata hyödyntää alan erityisosaajien (Subject Matter Expert, SME) substanssia mahdollisesti turvallisuuskriittisiä hankintoja tehtäessä eikä pitäytyä pelkästään hankinta-ammattilaisten näkökulmassa. Esimerkiksi tietojärjestelmäpalveluiden tuottamisessa käytettävät laitteistot tai ohjelmistot eivät ole vain Atk:ta tai ITC:tä. Hankinnan aikana sekä jälki-ilmoituksissa paljastettavat tiedot saattavat sisältää oleellisia asioita hankittavasta kokonaisuudesta ja hankkivan organisaation kriittisistä suorituskyvystä, jotka tiukan hankintalain tulkinnan vuoksi paljastuvat tahattomasti jättäen turvallisuusnäkökohdat huomiotta. Tämän vuoksi hankintaa suunniteltaessa tulee käyttää erityistä harkintaa tietojen julkisuudesta mahdollisesti aiheutuvien riskien pienentämiseksi ja vahinkojen estämiseksi sekä hyödyntää ne mahdollisuudet tiedon suojaamiseen, mitkä laintulkinta mahdollistaa.

8.5 Tietojärjestelmän elinkaaren aikainen tuki

Hankintaa suunniteltaessa on otettava huomioon järjestelmän elinkaaren aikaisen tuen vaatimukset. Onko laitteistolla, sovelluksella tai palvelulla saatavilla tukipalveluita Suomesta, vai tuotetaanko ne muualta Euroopasta, Afrikasta, Pohjois-Amerikasta tai Aasiasta? Tässä usein ei ole ratkaisevaa tuen laatu ja siihen liittyvät kriteerit, vaan lakien ja asetusten määräykset esimerkiksi henkilötietojen käsittelystä ja säilytyksestä. Vaikka tietojärjestelmässä ei lähtökohtaisesti käsiteltäisikään henkilöiden nimiä tai muuta vastaavaa tietoa, yleisen tietosuojasetuksen (General Data Protection Regulation, GDPR) mukaan ”Luonnolliset henkilöt voidaan yhdistää heidän käyttämiensä laitteiden, sovellusten, työkalujen ja protokollien verkkotunnistietoihin, kuten IP-osoitteisiin, evästeisiin tai muihin tunnistisiin, esimerkiksi radiotaajuustunnisteisiin. Näin käyttäjästä voi jäädä jälkiä, joita voidaan käyttää luonnollisten henkilöiden profilointiin ja tunnistamiseen etenkin, kun niitä yhdistetään yksilöllisiin tunnistisiin ja muihin palvelimille toimitettuihin tietoihin.” (Euroopan Unioni, 2016). Lähtökohtaisesti Euroopan Unionin alueella tietojen käsittely ja säilyttäminen ovat hyväksyttäviä, mutta eri maiden lainsäädännön poikkeamien takia Yhdysvalloissa tai Kiinassa tapahtuva Suomen kansalaisten henkilötietojen käsittely vaatii joko luvan tai valtionhallinnon järjestelmistä puhuttaessa edes ole sallittua.

Mikä on oikea tukipalveluiden taso hankittavalle järjestelmälle, riippuu järjestelmän kriittisyydestä ja omistajan (Business Owner) vaatimuksista tukitasolle. Usein nämä asiat jätetään tietojärjestelmästä vastaavan vastuulle, mikä ei ole suositeltava menettelytapa, vaan järjestelmän omistajan tulee vastata päätöksestä ja siitä aiheutuvista seuraamuksista. Tämä johtuu siitä syystä, että se taho, jolla on liiketoiminta- tai operatiivinen vastuu, vastaa tällöin myös liiketoiminnan menestymisestä sekä kuluista, joita vaatimukset aiheuttavat. Lisäksi tälle taholle kuuluu vastuu tietoturvan kokonaisturvallisuudesta tavalla, jota edellytetään esim. laissa julkisen hallinnon tiedonhallinnan 4 luvussa, 13 §:ssa ”Tietoaineistojen ja tietojärjestelmien tietoturvasuus” (Oikeusministeriö, 2019).

Hankintaa suunniteltaessa tukipalveluiden saatavuus vaikuttaa lisäksi sekä yritys- että henkilöturvallisuuteen. Ostajan on siis varmistuttava, että taho jolta hankinta tehdään, on huolehtinut omista turvallisuusvelvoitteistaan vaa-

timuksenmukaisella tavalla ja kykenee sekä haluaa tehdä tämän myös jatkossa. Tämä vaatimus tulee ja usein kyetäänkin hoitamaan jo tarjouspyyntövaiheessa ottamalla tarjouspyyntöön mukaan hyväksyntäkriteeristön edellyttämiä vaatimuksia. Vaatimuksen täyttymisen toteamista helpottaa se, jos vaatimukseen on otettu esimerkiksi mukaan vaade akkreditoinnista palvelun- tai tietoturvallisuuden hallinnassa.

Järjestelmän elinkaaren kannalta oleellinen seikka on hankinnan yhteydessä tehtävä tukisopimusten pituus. Usein laitevalmistajat tarjoavat 1-3 a. tukisopimuksia hankittaville laitteille, saatavilla on myös 5 a. sopimuksia. Yleensä tukisopimukset ovat merkittävästi edullisempia laitteita ostettaessa kuin myöhemmin hankittaessa.

Sovelluslisenssien suhteen tilanne on eri, riippuen erityisesti toimittajan tarjoamista lisenssimalleista. Usein yrityksellä on Enterprise License Agreement (ELA) sopimus, joka on elinkaaren kannalta monissa tapauksissa sekä taloudellisesti että toiminnallisesti järkevin. Vaihtoehtoja ovat perpetual (jatkuva /pysyvä) tai subscriber (tilaaja) -lisenssit. Perpetual-lisenssit ovat hankittaessa kalliimpia, mutta niissä ei tule vuosittaisia tukimaksuja, jolloin mahdollisuutta päivittää sovellusversiota ilman lisäkustannusta ei ole. Perpetual-lisenssit eivät sisällä myöskään laajempia tukipalveluita. Subscriber-lisenssit ovat hankittaessa edullisempia, mutta niistä on maksettava vuosittainen tilausmaksu, mikä sisältää tukipalvelut ja oikeuden päivittää sovellusta (Partanen, 2009). Tärkeää on kuitenkin lisensoida oikein lisenssiehdot ja asetetut vaatimukset tuelle sekä päivitettävyydelle huomioiden.

8.6 Palveluiden ulkoistamisen hankinta

Jos palvelu hankitaan joko kokonaan tai osittain ulkoistettuna, kasvavat hankinnan tarjouspyynnölle asetettavat vaatimukset. Toisaalta ulkoistus helpottaa turvallisuusvaatimusten toteuttamista niiden ollessa pois omalta kontolta, toisaalta ulkoistus asettaa vaatimuksia sekä palveluostamisen että sopimustekniselle osaamiselle ja ulkoistettujen palveluiden turvallisuuden hallinnalle. Erityisen tarkkana tulee olla määriteltäessä ulkoistuksen vastuurajoja, jotta hankalassa paikassa ei pääse käymään siten, että kukaan ei häiriötilanteessa sopimuksen mukaan vastaa juuri siitä huomiota vaativasta osasta palvelua. Palvelun ”palastelu” ja vastuurajojen määrittely ja selventäminen voidaan toteuttaa helposti esimerkiksi RACI- tms. muun matriisin avulla, mutta tämä

vastuurajojen tunnistaminen vaatii jo aiemminkin korostettua SME-osaimista.

Onkin kaikkien sopimusosapuolten etu, että vastuut ovat selkeät. Huomionarvoista on myös se, että palveluntarjoajien palvelukuvauksia ja niiden ehtoja sekä rajoituksia kannattaisi noudattaa sopimuksenteon helpottamiseksi. Lyhytnäköinen oman organisaation edun tavoittelu vaatimalla muokkauksia juuri omaan tarpeeseen sopivaksi palvelutoimittajan palvelukuvauksia räätälöimällä voi osoittautua vääräksi tavoitteeksi molempien osapuolten kannalta. Kun palvelua toimittava organisaatio on tottunut toimimaan palvelukuvauksen mukaisesti, poikkeamat normaalipalvelusta saattavat aiheuttaa ongelmia häiriötilanteissa, mikä ei ole koskaan tavoiteltavaa.

Valtionhallinnon toimijan ollessa kyseessä, tulee ottaa huomioon myös strategiset ja poliittiset tavoitteet, kuten esimerkiksi Yhteiskunnan turvallisuusstrategia (Valtioneuvosto, 2017). Jos poliittinen tavoite on, että halutaan rakentaa maailman turvallisimaa maa tai esimerkiksi vähentää riippuvuutta aasialaisista tuotteista, kuten puolijohteista, tulee tämä huomioida sekä ohjauksessa että turvallisuustoiminnan vaatimuksissa. Ilman riittävän korkealta tasolta ohjattuja tai saatuja vaatimuksia poliittisluonteisten vaatimusten huomioiminen ei ole välttämättä mahdollista. Valtioneuvoston toimenpidesuosituksen johtopäätöksissä todetaankin strategisen tavoitetilan määrittelyn tarpeellisuus huomioiden muutokset turvallisuusympäristössä (Kyberselvityshankkeen työryhmä, 2023).

9 Käyttöönotto

Palvelua käyttöönotettaessa on turvallisuuden kannalta tärkeää huolehtia siitä, että toteutukseen ja hallintaan tarvittavat resurssit ovat saatavilla ja lähtökohdat vaatimuksenmukaisuudelle, esim. henkilöturvallisuus tai turvallisuussopimukset, täyttyvät dokumentoidusti ennen käyttöönoton aloittamista. Lisäksi tulee huolehtia siitä, että vaatimuksenmukaisuuden ylläpitämiseen tarvittavat edellytykset ovat olemassa, ylläpidon prosessit ovat kunnossa, prosessien toimintaa seurataan esimerkiksi mittareiden avulla ja tuotettuja mitta-
reita arvioidaan toiminnan laadun ylläpitämiseksi ja parantamiseksi. Käyttöönotto-
vaiheessa parhaat käytännöt ja mallit, kuten ITIL ja eri standardit, ovat avuksi valmiuden toteamisessa.

Yleisin tapa edellä kuvatun kaltaiseen seurantaan on hyödyntää jotakin sovitua hallintajärjestelmää, joka antaa toiminnalle viitekehyksen. Tietoteknisten palveluiden osalta yleisin palvelunhallintajärjestelmä Suomessa lienee SFS-ISO 20001 ja tietoturvan osalta SFS-ISO 27001 mukainen. Palvelunhallintajärjestelmän ylläpitämistä varten tarjoavat tukea eri tietojärjestelmät, esimerkiksi voidaan mainita ServiceNow ja BMC Helix, jotka tukevat ITIL (Information Technology Infrastructure Library) parhaita käytäntöjä laadukkaana palvelunhallinnan tukena.

Yleisesti voidaan todeta, että käyttöönotto on varsin suoraviivainen tapahtuma, edellyttäen että aiemmat kohdat on huolehdittu ja että käyttöönotossa edetään suunnitelmallisesti ilman mutkien oikomista.

10 Ylläpito

Tietojärjestelmän ylläpitovaiheen aikana ylläpidetään sekä tietojärjestelmää, siihen liittyviä komponentteja ja niiden lisäksi hallintajärjestelmää. Jotta ylläpidon aikaisten muutosten vaatimuksenmukaisuus voidaan osoittaa, tulee niin tietojärjestelmän kuin hallintajärjestelmän prosessien olla hyvin suunniteltuja ja dokumentoituja. Anu Lampisen Pro Gradu tutkielman mukaan ”Dokumenttien tärkein tehtävä oli toimia ylläpidon aikaisten muutosten lähtökohdina. Dokumentteja hyödynnettiin myös tietojärjestelmän opettelussa ja tiedon lähteenä” (Lampinen , 2020).

Dokumentointia hyödynnetään siis koulutuksessa ja tietojärjestelmän opettelussa ja sen avulla osoitetaan myös tietojärjestelmän vaatimuksenmukaisuus ja sen ylläpito. Ylläpidon osoittaminen tapahtuu kuvattun ja mitatun prosessin mukaisesti, jota seurataan hallintaprosessin kuvaamalla, auditoinnissa todetulla sertifioidulla tavalla. Tämä on kohta, jossa parhaat käytännöt ja niissä kuvatut prosessit, kuten ITIL ja standardissa kuvatut hallintajärjestelmät kohtaavat. Eroksi näiden kahden välillä on, että esimerkiksi ITIL-prosessit ovat tekemistä parhaiksi oletettujen käytäntöjen mukaan tarkoituksena sujuvoittaa laadukasta, tehokasta ja mitattavaa tekemistä. Standardin prosessit, esimerkiksi ISO-SFS 20000-1, prosessit ovat hallintajärjestelmään kuuluvia, jotka hyödyntävät ITIL-prosessien tuloksia sekä toimintatapaa. Standardien prosesseihin kuuluvat oleellisesti mittarit (KPI, Key Point Indicators), joiden avulla osoitetaan vaatimuksenmukaisuutta ja sen täyttymistä tai täyttymättä jäämistä.

11 Käytöstä poisto

Käsiteltäessä turvallisuusluokiteltua materiaalia tietojärjestelmän elinkaari ei pääty siihen, että suoritetaan tietohuolto ja tiedon tallennusvälineiden sanitointi ennen kuin laitteista katkaistaan virta. Käytöstä poistettuja laitteita ja materiaalia tulee edelleen käsitellä kuten tietosuojattavaa aineistoa tietojärjestelmän aiemman elinkaaren aikana. Tämän vuoksi myös hallintajärjestelmässä tulee huomioida järjestelmän elinkaaren päättymiseen liittyvät toimenpiteet. Käsitellyn tiedon turvallisuusluokitukseen perustuen voi olla mahdollista hyödyntää laitteistoa muussa tarkoituksessa, kunhan vain huolehditaan vaatimuksenmukaisesta tiedon sanitoinnista esimerkiksi sertifioidun tiedon tyhjennys- tai ylikirjoitusohjelmiston avulla, joita on tarjolla usealta toimittajalta. Toimittajaa tai ohjelmistoa valittaessa on syytä huomioida käytettävän ratkaisun vaatimustenmukaisuus, jotta omalta osalta tätä ei epähuomioissa rikkottaisi. Esimerkiksi ISO/IEC 15408:2022 Information security, cybersecurity and privacy protection standardin mukainen sertifiointi on käytettävältä ratkaisulta hyvä löytyä (korvaava, tekeillä oleva standardi ISO/IEC AWI 15408-1) (International Organization for Standardization, 2022).

Korkeampien turvallisuusluokkien laitteistojen kanssa tämä ei ole mahdollista, vaan laitteiden käytöstä poistamisen jälkeen ne tulee varastoida ja hävittää määritellyllä, tietoturvaluokkaan hyväksytyllä tavalla. Ohjeita hävitykseen eri tietoturvaluokille löytyy edellä mainitun ISO-standardin lisäksi esim. NIST Special Publication 800-88 Guidelines for Media Sanitization julkaisusta (NIST The National Institute of Standards and Technology, 2014) ja kansallisesta KATAKRI 2020 -kriteeristöstä ja sen NATO-liitteestä (Kansallinen turvallisuusviranomainen, 2021).

Tietosuojamateriaalin hävittämisessä on lisäksi edelleen huomioitava dokumentointi ja tiettyjen tietoturvaluokkien käsittelyvaatimuksissa oleva hävittämisen dokumentointivaatimus (hävitystodistus), joka on kirjattava ja säilytet-

tävä määrätyn ajan. Koska vaatimukset tämän osalta vaihtelevat, tulee ne tarkastaa asianmukaisista lähteistä tietosuojamateriaalin hävittämisen ollessa ajankohtaista. Esimerkiksi NATO CONFIDENTIAL tiedon tuhoamisesta ei tarvitse tehdä erikseen ilmoitusta (Kansallinen turvallisuusviranomainen, 2023).

Jos materiaali on toisen osapuolen materiaalia, tai jos tietojärjestelmä on sisältänyt ko. materiaalia, tulee tiedon sanitoinnista ja tietovälineiden sekä materiaalin tuhoamisesta ilmoittaa tiedon omistavalle osapuolelle (Kansallinen turvallisuusviranomainen, 2021). Lisäksi on huomioitava järjestelmän tarkastanut viranomainen, jolle tuhoamistieto on toimitettava.

12 Yhteenveto

Tutkimuksen havaintojen ja lähdemateriaalin perusteella voidaan todeta, että tietojärjestelmän turvallisuuden vaatimuksenmukaisuuden määrittäminen, määritysten mukaisen tietojärjestelmän suunnittelu, hankinta ja ylläpito kaikki turvallisuuteen kuuluva huomioiden on varsin laaja, systemistä osaa- mista ja monipuolista asiantuntemusta vaativa tehtävä.

Tietojärjestelmän vaatimuksenmukaisuus, vaatimuksenmukaisuuden hallinta ja seuranta vaativat tuekseen suunnitelmallisen lähestymistavan, jota ilman menestyksekkäs, todistettava toiminta on käytännössä mahdotonta. Tätä lähes- tymistapaa kuvataan alla.



Kuva 11 PDCA-mallin mukainen lähestymistapa vaatimuksenmukaisuuden hallintaan (Lähde: ISO 37301:2021)

Kuvaustapa on hieman erilainen kansallisiin VAHTI-suosituksiin verrattuna, mutta pääosin ajatusmalli ja johtopäätös on sama – Vaatimuksenmukaisuuden seuranta vaatii hallintajärjestelmän.

Prosessi on jatkuva ja edellyttää sitoutunutta toimintaa usealta eri toimijalta, organisaation osalta ja viranomaistaholta. Tästä voidaan päätellä, että mitä enemmän vastuita hajautetaan, sitä vaativampi on vaatimuksenmukaisuuden seurannan prosessi ja sen toteuttaminen. Vähintäänkin vastuuprosessien ja roolien kuvaukseen tulee kiinnittää erityistä huomiota jo suunnitteluvaiheessa ja sitouttaa organisaation osat ja erityisesti johto tukemaan prosessien tarkoituksenmukaista suorittamista. Tämä tarve todetaan myös Kansallisen turvallisuusviranomaisen arviointikriteeristön liitteessä IV (Kansallinen turvallisuusviranomainen, 2023). Johdon sitoutumista korostetaan myös eri standardien vaatimuksissa, joissa edelleen edellytetään sitoutumisen osoittamista (Suomen Standardoimisliitto SFS ry, 2022).

Mikä hallintamalli puolestaan on oikea, siihen on mahdotonta vastata. Tutkimuksessa käytetyn materiaalin perusteella paras malli muodostuu usean eri standardin mukaisesta hallintamallista, jotka tarkastelevat asiaa hieman eri näkökulmasta. Nämä hallintamallit edellyttävät asiantuntijaosaamista ja sen täysimittaista hyödyntämistä. Huomattavana riskinä tällöin on kuitenkin hallintajärjestelmien vaatiman työn määrän merkittävä kasvu.

Järkevintä lienee on todeta, että hallintamalli tai hallintamallit ovat tarpeellisia, mutta ne edellyttävät myös toimivia, tarpeeseen soveltuvia suunnittelu- ja ylläpitomalleja. Mikä on kulloiseenkin tarpeeseen sopivin, riippuu viime kädessä organisaation tarpeesta ja käytettävissä olevista resursseista.

13 Loppupäätelmät

Tietojärjestelmän elinkaaren aikaisen kokonaisturvallisuuden hallinta on jo aiemmin todetun mukaisesti laaja, vaativa ja kokonaisvaltaista näkemystä tarvitseva tehtävä. Tarkastellun materiaalin perusteella hallintajärjestelmän suunnitteluun ei löydy suoraa mallia, joskin parhaan tuloksen voidaan arvioida syntyvän suunnitelmallisesti ja harkiten kokonaisturvallisuutta eri näkökulmista tarkastelemalla hyödyntäen esim. turvallisuuskriteeristöä suunnittelutyön tukena.

Tarkastellut standardoidut hallintajärjestelmät puolestaan ovat enemmän tai vähemmän asiaa tietyltä, yhdeltä rajoitetulta näkökulmalta tarkastelevia, kattaen kuitenkin asioita varsin laajasti. Tarjontaa standardoiduista hallintajärjestelmistä on paljon ja isolta osalta niiden vaatimukset ovat päällekkäisiä. Tästä voidaan tulla johtopäätökseen, että tarkoituksenmukaisesti yrityksen tarpeeseen valitulla standardoidulla hallintajärjestelmällä kyetään kattamaan valtaosa tietojärjestelmän elinkaaren aikaisista kokonaisturvallisuuden tarpeista. Erityistä huomiota tulee kuitenkin kiinnittää kevyemmin ohjattuihin elinkaaren alkupään asioihin, eli hankintaprosessiin, toimittajavalintoihin ja tarjottaviin tukipalveluihin sekä sopimushallintaan. Tämä koskee erityisesti saatavuuden sekä jatkuvuudenhallinnan näkökulmia. Turvallisuuden näkökulma tulee huomioida myös hankintatietoja julkisuudesta päätettäessä, erityisesti turvallisuuskriittisten valtionhallinnon toimijoiden ollessa kyseessä. Mainitut asiat on toki tiedetty tärkeiksi, mutta toisesta, kaupallisesta, näkökulmasta. Turvallisuuden näkökulmasta niiden käsittely on jäänyt erillisen ohjauksen ja johtamisen alle, eikä niihin ole välttämättä kiinnitetty turvallisuuden edellyttämää huomiota.

Hallintajärjestelmää ylläpidettäessä huomio kiinnittyy väistämättä siihen, että organisaatioissa tieto- ja fyysisen turvallisuuden johtaminen ovat usein eriytetty eri tahoille ja todennäköisesti eri hallintamalliin. Tarkastelun perusteella on kuitenkin järkevää yhdistää hallintamallit vähintäänkin siten, että ohjaus

ja seuranta tapahtuvat yhdestä paikasta keskitetysti. Tällöin päästäneen kokonaisvaltaisempaan ja kattavampaan, systeemimallin mukaiseen lopputulokseen kuin hallintamalleja erillisenä seuraten ja ohjaten.

Tutkituista ja tarkastelluista asioista on tehty paljon tieteellistä tutkimusta ja materiaalia tutustuttavaksi oli runsaasti. Tehdyn tutkimuksen määrän takia yksittäiset työssä esitetyt havainnot eivät sinällään ole ainutlaatuisia. Kuitenkin tästä huolimatta ja opinnäytetyöraportin laajasta tutkimusnäkökulmasta johtuen, työn tuloksena tehty synteesi sisältää uutta, pohtimisen ja tutustumisen arvoista asiaa tietojärjestelmän elinkaaren aikaisen kokonaisturvallisuuden hallinnan kannalta.

14 Lähteet

Center for Internet Security, Inc®. (CIS), 2023. *The Center for Internet Security*. [Online]

Available at: <https://cissecurity.org>
[Haettu 16 loka 2023].

Colchester, J., 2019. *SITRA*. [Online]

Available at: <https://www.sitra.fi/blogit/viheliaiset-ongelmat-systeemiajattelu/>
[Haettu 7. tammikuu 2024].

Digi- ja väestötietovirasto DVV, 2020. *Turvallisen sovelluskehityksen käsikirja*. [Online]

Available at: <https://www.suomidigi.fi/sites/default/files/2020-05/Turvallisen%20sovelluskehityksen%20k%C3%A4sikirja.pdf>
[Haettu 30. toukokuu 2023].

Digi- ja väestötietovirasto DVV, 2023. *Digitaalisen turvallisuuden arkkitehtuurin julkinen dokumentaatio*. [Online]

Available at: <https://wiki.dvv.fi/display/DTARK/Viitekehys>
[Haettu 27. helmikuu 2024].

Euroopan Unioni, 2016. *EUR-Lex*. [Online]

Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0008.01/DOC_1&format=PDF
[Haettu 4. tammikuu 2024].

Euroopan Unioni, 2016. *EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679*. [Online]

Available at: <https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679>
[Haettu 3. tammikuu 2024].

European committee for standardization CEN, 2017. *Conformity assessment. Requirements for accreditation bodies accrediting conformity assessment bodies (ISO/IEC17011:2017)*, Brussels: Finnish Standards Association SFS.

FINAS Finnish Accreditation Service, 2023. *FINAS Finnish Accreditation Service*. [Online]

Available at: <https://www.finas.fi/Sivut/default.aspx>

FINAS Finnish Accreditation Service, 2023. *FINAS Toiminnan ohjaus*. [Online]

Available at: <https://www.finas.fi/Tietoa/Sivut/Toiminnan-ohjaus.aspx>
[Haettu 7. tammikuu 2024].

FINAS Finnish Accreditation Service, 2024. *Akkreditoitut toimijat*.
[Online]

Available at: <https://www.finas.fi/toimijat/Sivut/default.aspx>
[Haettu 17. helmikuu 2024].

FINAS Finnish Accreditation Service, 2024. *Sertifiointiorganisaatiot*.
[Online]

Available at:
<https://www.finas.fi/akkreditointi/Akkreditointialueet/Sivut/Sertifiointiorganisaatiot.aspx>

[Haettu 17. helmikuu 2024].

International Organization for Standardization, 2023. *ISO/IEC/IEEE 15288:2023(en) Systems and software engineering — System life cycle processes*. [Online]

Available at: <https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:15288:ed-2:v1:en>

[Accessed 28. helmikuu 2024].

International Organization for Standardization, 2021. *ISO 37301:2021 Compliance management systems - requirements with guidance for use*, Geneva: ISO Copyright office.

International Organization for Standardization, 2022. *ISO/IEC 15408-1:2022*. [Online]

Available at: <https://www.iso.org/standard/72891.html>

[Accessed 18. helmikuu 2024].

Julkisen hallinnon tietohallinnon neuvottelukunta, 2010. *Suomidigi.fi*.
[Online]

Available at: <https://www.suomidigi.fi/ohjeet-ja-tuki/jhs-suositukset/jhs-172-ict-palvelujen-kehittaminen-esiselvitys-vanhentunut>

[Haettu 3. tammikuu 2024].

Kansallinen turvallisuusviranomainen, 2021. *Katakri 2020*. Ensimmäinen painos toim. Helsinki: Traficom.

Kansallinen turvallisuusviranomainen, 2023. *KATAKRI 2020 Liite IV: Naton turvallisuusluokitellun tiedon suojaaminen*, Helsinki : Ulkoministeriö - Kansallinen turvallisuusviranomainen.

Keystone Education Group Oy, 2023. <https://www.koulutus.fi>. [Online]

Available at: <https://www.koulutus.fi/artikkelit/mika-on-chatgpt-ja-mitaisiita-pitaisi-tietaa-23286>

[Haettu 16 10 2023].

Kortelainen, H. ym., 2021. *VTT's Research Information Portal*. [Online]

Available at: <https://cris.vtt.fi/ws/portalfiles/portal/44305471/>

[Haettu 30. toukokuu 2023].

Kyberselvityshankkeen työryhmä, 2023. *Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa*, Helsinki: Valtioneuvosto.

Lampinen , A., 2020. *Tietojärjestelmädokumenttien hyödyntäminen ylläpidossa: Tapaustutkimus*, Jyväskylä: Jyväskylän Yliopisto, Tietojenkäsittelytieteiden laitos.

Liikenne- ja viestintävirasto kyberturvallisuuskeskus, 2023. *Toimintamme - NCSA*. [Online]

Available at: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa> [Haettu 17. helmikuu 2024].

Mielonen , S., ei pvm *Systeemiajattelu*. [Online]

Available at:

https://mlab.taik.fi/polut/Yhteiskunnalliset/tyokalu_systeemiajattelu.html [Haettu 27. joulukuuta 2023].

NATO North Atlantic Treaty Organization, 2010. *Allied Command Operations Comprehensive Operations Planning Directive (COPD) Interim Version 1.0*, Mons: Supreme Headquarters Allied Powers Europe .

NATO North Atlantic Treaty Organization, 2020. *Directive on personnel security AC/35-D/2000-REV8*, Bryssel: NATO Security Committee.

NATO North Atlantic Treaty Organization, 2020. *Directive on Physical Security AC/35-D/2001-REV3* , Bryssel: NATO Security Council.

NATO North Atlantic Treaty Organization, 2020. *Security within The North Atlantic Treaty Organization C-M(2002)49-REV1*, Bryssel: NATO Security Committee.

Ncubukezi, T., 2022. *Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses*, Cape Town: Information Technology Department, Faculty of Informatics and Design, Cape Peninsula University of Technology,.

NIST The National Institute of Standards and Technology, 2004. *Standards for Security Categorization of Federal Information and Information Systems*. [Online]

Available at: <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf> [Accessed 28. joulukuuta 2023].

NIST The National Institute of Standards and Technology, 2014. *NIST Special Publication 800-88 Guidelines for Media Sanitization*, Gaithersburg MD: National Institute of Standards and Technology.

NIST The National Institute of Standards and Technology, 2024. *The NIST Cybersecurity Framework (CSF) 2.0*. [Online]

Available at: <https://doi.org/10.6028/NIST.CSWP.29> [Accessed 27. helmikuu 2024].

Official Journal of the European Union , 2013. *Official Journal of the European Union L 274/1*. [Online]

Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488> [Haettu 29. helmikuu 2024].

- Oikeusministeriö Finlex, 2019. *Laki julkisen hallinnon tiedonhallinnasta*. [Online]
Available at: <https://www.finlex.fi/fi/laki/alkup/2019/20190906>
[Haettu 30. toukokuu 2023].
- Oikeusministeriö, 2004. *Finlex*. [Online]
Available at: <https://www.finlex.fi/fi/laki/ajantasa/2004/20040588>
[Haettu 8. tammikuu 2024].
- Oikeusministeriö, 2010. *Finlex*. [Online]
Available at: <https://www.finlex.fi/fi/laki/ajantasa/kumotut/2010/20100681>
[Haettu 28. joulukuu 2023].
- Oikeusministeriö, 2011. *Finlex*. [Online]
Available at: <https://www.finlex.fi/fi/laki/alkup/2011/20111405>
[Haettu 8. tammikuu 2024].
- Oikeusministeriö, 2014. *Finlex*. [Online]
Available at: <https://www.finlex.fi/fi/laki/ajantasa/2014/20140917>
[Haettu 3. tammikuu 2024].
- Oikeusministeriö, 2016. *Finlex*. [Online]
Available at: <https://www.finlex.fi/fi/laki/alkup/2016/20160571>
[Haettu 4. tammikuu 2024].
- Oikeusministeriö, 2016. *Finlex*. [Online]
Available at: <https://www.finlex.fi/fi/laki/alkup/2016/20161397>
[Haettu 4. helmikuu 2024].
- Oikeusministeriö, 2019. *Finlex*. [Online]
Available at: <https://www.finlex.fi/fi/laki/alkup/2019/20191101>
[Haettu 28. joulukuu 2023].
- Oikeusministeriö, 2019. *Finlex*. [Online]
Available at: <https://www.finlex.fi/fi/laki/alkup/2019/20190306>
[Haettu 4. helmikuu 2024].
- Pöyhönen, J., 2018. *Standardit, ohjeet ja suositukset osana teollisuusorganisaatioiden kyberturvallisuuden hallintaa : CIRP-raportti 2017*, Jyväskylä: Jyväskylän yliopisto. Informaatioteknologian tiedekunnan julkaisuja / Jyväskylän yliopisto, 55.
- Pöyhönen, J., 2020. *Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu*, Jyväskylä: Jyväskylän yliopisto.
- Partanen, J., 2009. *Tapaustutkimus: Ohjelmistolisenssien ominaisuuksien vertailu*. [Online]
Available at:
<https://trepo.tuni.fi/bitstream/handle/10024/80931/gradu03805.pdf;jsessionid=AE61000783E65372451046785370D9AF?sequence=1>
[Haettu 28. joulukuu 2023].
- Puhakainen, P., 2021. *Valtiovarainministeriö - Kokemuksia turvallisuusluokittelusta*. [Online]

Available at:

https://vm.fi/documents/10623/0/Luokittelukokemuksia_+Erja+Kinnunen.pdf/c06dcc7a-e510-21c8-24b3-adaaec2e6061/Luokittelukokemuksia_+Erja+Kinnunen.pdf?t=1632224782881

[Haettu 17. helmikuu 2024].

Sanakirja.org Solutions Oy, 2024. *Sanakirja.org*. [Online]

Available at: <https://www.sanakirja.org/search.php?id=187480&l2=17>

[Haettu 7. tammikuu 2024].

Sanastokeskus, 1993. *TEPA - termipankki Erikoisalojen sanastojen ja sanakirjojen kokoelma*. [Online]

Available at:

<https://termipankki.fi/tepa/fi/haku/tietoj%C3%A4rjestelm%C3%A4>

[Haettu 7. tammikuuta 2024].

Sanastokeskus, 2023. *TEPA-termipankki Erikoisalojen sanastojen ja sanakirjojen kokoelma*. [Online]

Available at: <https://termipankki.fi/tepa/fi/haku/vaatimustenmukaisuus>

[Haettu 13. tammikuu 2024].

Sanastokeskus, 2023. *TEPA-termipankki Erikoisalojen sanastojen ja sanakirjojen kokoelma*. [Online]

Available at: <https://termipankki.fi/tepa/fi/haku/conformity%20assessment>

[Accessed 13. tammikuu 2024].

Seppänen, O., 2012. *Tietoturvallisuuden kehittäminen yrityksessä*, Helsinki: Espoo.

Soikkeli, M., 2021. *Lainsäädäntö tieto- ja kyberturvallisuuden perustana - Valtionhallinnon viranomaisen näkökulma*, Jyväskylä: Jyväskylän Yliopisto, Informaatioteknologian tiedekunta.

Suomen Riskienhallintayhdistys, 2012 - 2024. *PK-RH-riskienhallinta*. [Online]

Available at: <https://pk-rh.fi/riskien-luokittelu/operatiiviset-riskit/henkiloriskit.html>

[Haettu 29. helmikuu 2024].

Suomen Standardisoimisliitto SFS ry, 2012. *SFS-EN 45020:en Standardization and related activities. General vocabulary*, Helsinki: Suomen Standardisoimisliitto SFS ry.

Suomen Standardoimisliitto SFS ry, 2022. *ISO/IEC 27001:2022:fi*, Helsinki: Suomen Standardoimisliitto SFS ry.

Tieteen termipankki, 2016. *Tieteen termipankki Filosofia:holistinen*. [Online]

Available at: <https://tieteentermipankki.fi/wiki/Filosofia:holistinen>

[Haettu 30. toukokuu 2023].

Ulkoministeriö, 2023. *Ulkoministeriö*. [Online]

Available at: <https://um.fi/kansallinen-turvallisuusviranomainen>

[Haettu 8. tammikuu 2024].

Valtioneuvosto, 2017. *Yhteiskunnan turvallisuusstrategia*. [Online]
Available at:
https://valtioneuvosto.fi/documents/1410877/2132272/Yhteiskunnan_turvallisuusstrategia.pdf/1f6b0b51-5069-4979-9f3b-579f8c0543d7/Yhteiskunnan_turvallisuusstrategia.pdf.pdf
[Haettu 17. helmikuu 2024].

Valtiovarainministeriö, 2016. *Toiminnan jatkuvuuden hallinta*. [Online]
Available at: <http://urn.fi/URN:ISBN:978-952-251-779-1>
[Haettu 27. Helmikuu 2024].

Valtiovarainministeriö, 2020. *Valtiovarainministeriön julkaisuja 2020:61*.
[Online]
Available at:
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162433/VM_2020_61.pdf?sequence=4&isAllowed=y
[Haettu 27. joulukuu 2023].

15 Kuvaluettelo

Kuva 1 Esimerkki kerroksittaisesta arkkitehtuurista (Onion-architecture) (Lähde: <https://medium.com/expedia-group-tech/onion-architecture-deed8a554423>)

Kuva 2 ICT-palvelujen kehittämisen vaiheet mukailen lähdettä (Julkisen hallinnon tietohallinnon neuvottelukunta, 2010)

Kuva 3 Esimerkki turvallisuuden kontroleista sipulimallina. Kuvan reunalla esitetyt turvallisuuskontrollit sijoittuvat keskellä sijaitsevan ”sipulin” eri kerroksille muodostaen kokonaisturvallisuuteen vaikuttavat kontrollit.

Kuva 4 Standardit tarkastelevat samaa asiaa hieman eri näkökulmista. Näin ne muodostavat osittain toistensa yli käyvän kokonaisuuden.

Kuva 5 Jatkuvuudenhallinnan järjestelmän jatkuva kehittäminen (Valtiovainministeriö, 2016)

Kuva 6 Kuva uuden hakijan akkreditointiprosessista. (Lähde: <https://www.finns.fi/akkreditointi/Akkreditointiprosessi/Sivut/default.aspx>)

Kuva 7 Auditointiprosessi (Lähde: <https://www.kiwa.com/fi/fi/palvelutyypit/sertifiointi-ja-arviointi/johtamisjarjestelmat/auditointiprosessi/>)

Kuva 8 Esimerkki suhteellisuusperiaatteesta. Uhkatason noustessa kasvaa uhan torjuntaan tarvittavien resurssien määrä, jonka suhteen tulisi löytää optimi; kohtuulliset kustannukset – siedettävä riski.

Kuva 9 Tiedon luottamuksellisuus, eheys ja saatavuus muodostavat kokonaisuuden, jossa tulee huolehtia osien tasapainosta.

Kuva 10 Hankintalakien soveltaminen (Lähde: <https://ptcs.fi/lainsaadannon-soveltaminen-turvallisuusorientoituneisiin-hankintoihin/>)

Kuva 11 PDCA-mallin mukainen lähestymistapa vaatimuksenmukaisuuden hallintaan (Lähde: ISO 37301:2021)