VALTIOVARAINMINISTERIÖ

VALTIONHALLINNON

TIETOTURVATASOT

- ESITUTKIMUS –

HANKERYHMÄN LOPPURAPORTTI 25.6.2007

VALTION IT-TOIMINNAN JOHTAMISYKSIKÖN (VALT-IT) KÄRKIHANKE

VALTIOVARAINMINISTERIÖ

PÄÄTULOKSET VALTIONHALLINNON TIETOTURVATASOJEN ESITUTKIMUKSESTA

PÄÄHAVAINNOT VALTIONHALLINNON LÄHTÖTILANTEESTA

Esitutkimushanke osoitti, että hallinnossa jokaisella työntekijällä on yksilöllinen näkemys, siitä mitä tietoturvallisuus omassa työssä tarkoittaa. Myös tietoturvallisuuden hallintaa tukevat toimet ovat eri hallinnonaloilla ja virastoissa osittain erilaiset.

Hankeryhmä selvitti työpajassa 1.3.2007 valtionhallinnon turvallisuuden vähimmäisvaatimukset (perusturvataso). Saman kuukauden 29. päivä pidetyssä työpajassa hankeryhmä selvitti hallinnon turvattavia kohteita. Työpajan yhteydessä kerättiin myös toiveita siitä, millaisia olisivat VM:n hallinnolle tarjoamat tietoturvallisuuteen liittyvät yhteiset rakenteet, palvelut ja välineet.

PERUSTURVATASO VALTIONHALLINTOON

Turvatasot ovat luokiteltuja turvatoimenpide- ja menettelyvaatimuksia, jotka kohdistuvat turvattavan kohteen suojaamiseen. Turvatasot ovat yhteensopivia kansainvälisten standardien, laatumallien ja hyvien käytäntöjen kanssa. Valtionhallinnossa yhteiselle (perus)turvatasolle on mahdollista asettaa yhtenäiset vaatimukset, kun turvattavista kohteista on sovittu ja turvatavoitteet päätetty.

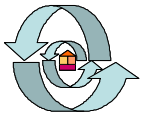
Kyvykäs organisaatio osaa turvata sille tärkeät kohteet tehokkaasti ja sille parhaiten sopivalla tavalla. Tuloksena palveluiden laatu paranee ja ongelmien määrä vähenee. Tuloksena on asiakkaiden sekä oman henkilöstön tyytyväisyys. Koko hallinnon kannalta etuna on säästynyt työaika ja hallinnossa jo tehdyn työn jakaminen muiden käyttöön. Kansallisesti Suomi näkyy asiantuntevana tietoturvaosaajana ja kykenee osoittamaan tasaisen hyvää hallintoa.

ORGANISAATION KYPSYYDEN JA TURVATTAVIEN KOHTEIDEN HALLINTA

Kypsyyskuutio mallintaa kypsyyden eri osa-alueet. Malli auttaa hahmottamaan kokonaisuutta ja antaa välineen, jonka avulla keskustella aiheesta siten, että kukin ymmärtää asian samalla tavoin. Kuutio voidaan jakaa osiin, jolloin alueita on mahdollista tarkastella yksityiskohtaisemmin. Osa-alueet on helppo kohdistaa eri asiantuntijoille. Kuutio on yhteensopiva standardien ja hyvien käytäntöjen kanssa. Organisaatio valitsee tavoiteltavan tason ydintehtäviensä ja tarpeidensa mukaan. Kuutio sopii kaikille organisaatioille.

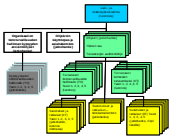
Turvakuution perusrakenne on sama kuin kypsyyskuutiossa. Turvakuutiossa neliportainen jako perustuu turvatasoihin kun kypsyyskuutiossa organisaation kypsyyteen. Kuutio osoittaa valitun turvattavan kohteen (tietoaineisto, palvelu, tietojärjestelmä, yksikkö, henkilöstö, tila, infra, laite, jne.) liittymät turvatasoihin sekä tietoturvallisuuden kokonaishallintaan. Tavoiteltava turvataso valitaan toiminnan ja tehtävien mukaan. Organisaation eri yksiköt tai palvelut voivat suunnitellusti olla eri turvatasoilla.

TUKI HALLINNON TIETOTURVATYÖHÖN



Yhteistoiminnassa valmistellaan ja päätetään turvatasojen skaalaus. Tällä varmistetaan, että tasot vastaavat organisaatioiden tarpeita ja sitouttavat niiden noudattamiseen. Arviointeja tekevät toimijat ja organisaatiot pääsevät vaikuttamaan etukäteen tietoturvatyön kuvaamiseen ja suunnitteluun. Samalla tietoturvatyötä tekevät tietävät etukäteen, millaisiin asioihin auditoinneissa ja niiden kriteereissä tullaan painottamaan.

Turvatasojen vaiheistetussa käyttöönotossa selvitetään tasoajattelun toimivuus hallinnossa ja mahdolliset käynnistysongelmat. Pilottiorganisaatiot saavat ensimmäisinä käyttöönsä uudet välineet. Valtiovarainministeriön jatkohankkeessa pilotteja tuetaan eri tavoin halutulle turvatasolle pääsyyn. Samalla arvioidaan tasomallin kustannukset ja aikataulut.



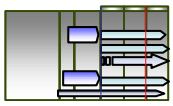
Tietoturvatyön avuksi suunniteltiin käytännönläheinen ja jäsennelty turvallisuuden hallinnan ohjeistorakenne. Hankkeesta hyötyvät valtion organisaatiot, kunnat, niiden asiakkaat ja sidosryhmät.

Välineiksi hankeryhmä suunnitteli ”kättä pidempää” tietoturvavastaaville ja auditoijille. Jatkotyöstettäviä luonnoksia ovat välineet kustannusten laskemiseen, tasojen arviointiin sekä auditointiin. Tietoturvallisuuden tason parantamiseen tähtäävät välineet on tarkoitus tarjota hallinnon käyttöön. Välineiden kehittäminen viimeistellään jatkohankkeessa. Jatkotyöhön ovat sitoutuneet 7 erityyppistä pilottiorganisaatiota julkishallinnosta.

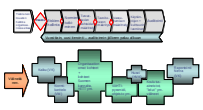
TOTEUTTAMISSUUNNITELMA

Jatkohankkeen tavoitteena on nostaa organisaatioiden kypsyyttä tietoturvallisuuden hallinnassa. Vuonna 2011 kaikki hallinnon organisaatiot ovat ainakin toistettavalla ja palvelut vähintään perustasolla. Turvattavien kohteiden turvatasoa kehitetään yhtenäisillä apuvälineillä ja tuetaan organisaatioiden tietoturvavastaavien työtä käytännössä.

Valtiovarainministeriön toteuttamana jatkohanke keskittää tietoturvallisuuden parhaan osaamisen hallinnon käyttöön. TTT poistaa hallinnosta päällekkäistä työtä sekä välineiden kehittämisessä että tietoturvallisuuden parantamisessa. Eräänä suurena työmäärän vähentäjänä tasoajattelu tuottaa keinot hallita alihankintaa ja toimittajia. Säästettävät työtunnit käytetään virastojen toimintaa tukevaan, ennakoivaan tietoturvatyöhön.



Esitutkimushankkeessa suunniteltiin **jatkohankkeen työn jakamiseen 5 kokonaisuutta:**



I. Turvattavien **kohteiden** kartoitus ja turvatavoitteiden määritys
II. Turvattaviin kohteisiin vaikuttavat **normit**, standardit ja hyvät käytännöt
III. Käytettävien turvatasojen harmonisointi ja **soveltamismahdollisuuksien** tutkiminen
IV. Organisaatioiden kypsyyden ja turvatason **arviointi** ja parantaminen
V. **Tietoturvatasohankkeen** kokonaishallinnan ja ohjauksen toteuttaminen.

Jatkohankkeet toteutetaan yhdessä hallinnonalojen, virastojen ja hallinnon sidosryhmien kanssa. Tietoturvatasot tukevat hallinnon tietoturvavastaavia, meneillään olevia tietoturvahankkeita sekä VAHTIn, YETT:n, VTV:n ja VM/controllerin toimintaa.

Sisällysluettelo

Vene on varmimmassa turvassa

silloin kun se on satamassa,

mutta ei veneitä ole rakennettu sen vuoksi.

- Paolo Coelho –

LUKUOHJE - TIETOTURVATASOJEN ESISELVITYSRAPORTIN SISÄLTÖ

Violetti	Pikavilkaisu päätuloksiin
Sininen	Kypsyys-asiaa organisaation kannalta, kypsyyskuutio
Vihreä	Turvattavan kohteen ja turvatason asiaa, turvakuutio
Keltainen	Tiedot kerätty hallinnolta työpajoissa, yhtymäkohtia VAHTIin
Oranssi	Toteuttamisehdotukset, konkreettiset apuvälineet hallinnolle
Punainen	Kustannusarviot, pilotointi - viranomaisjulkisia
Vaaleanpunainen	Lisätietoja, lähteitä
Valkoinen	Hallinnollista tietoa hankkeesta
Harmaa	Normiohjaus, standardit

1 Tiedolla on tärkeä merkitys toiminnalle

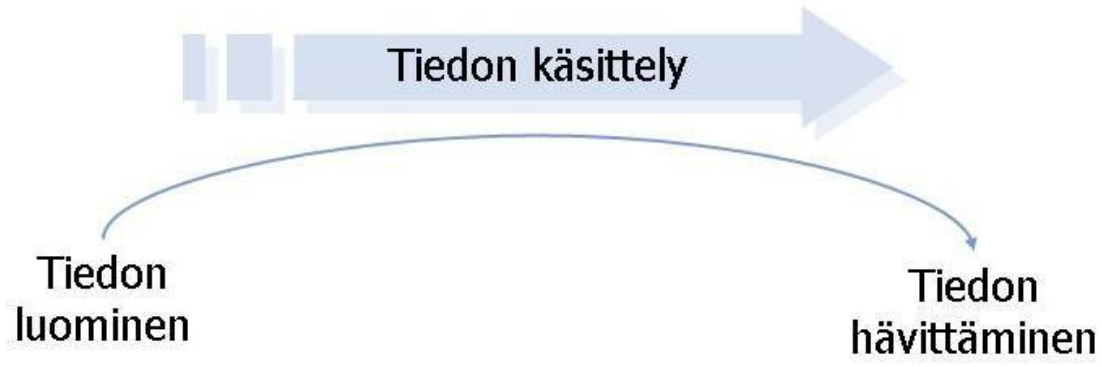
Tieto on toiminnan mahdollistaja ja sen edellytys. Tiedon avulla johdetaan ja tehdään päätöksiä. Sen vuoksi tietoon kohdistuu lukuisia eri vaatimuksia kuten laadukkuus, oikea-aikaisuus, luottamuksellisuus, saatavuus ja todennettavuus.

Tietoa esiintyy lukuisissa eri muodoissa: päässä, paperilla, kuullussa, puhutussa, tallenteella, tietojärjestelmästä ja niin edelleen. Tietoa voidaan myös käsitellä monin eri tavoin, kuten lukea, siirtää, puhua, poistaa, muuttaa, kopioida.

Tietoturvallisuudella tähdätään tiedon käsittelyyn kohdistuvien turvallisuusvaatimusten hallittuun toteuttamiseen kaikissa käsittelyn vaiheissa. Tämä tarkoittaa, että turvatoimenpiteet ja –menettelyt ovat suunniteltuja, laadukkaita sekä perusteltuja.

Tietoturvallisuuden hallinnan tulee ottaa huomioon:

- Tiedon eri muodot ja käsittelytavat;
- Tietoon kohdistuvat riskit ja turvaamisen toteuttamisen keinot;
- Toimintaan ja sitä kautta tietoon kohdistuvat vaatimukset.



Kuva 1. Tietoturvallisuus ja tiedon käsittely liittyy tiedon koko elinkaareen.

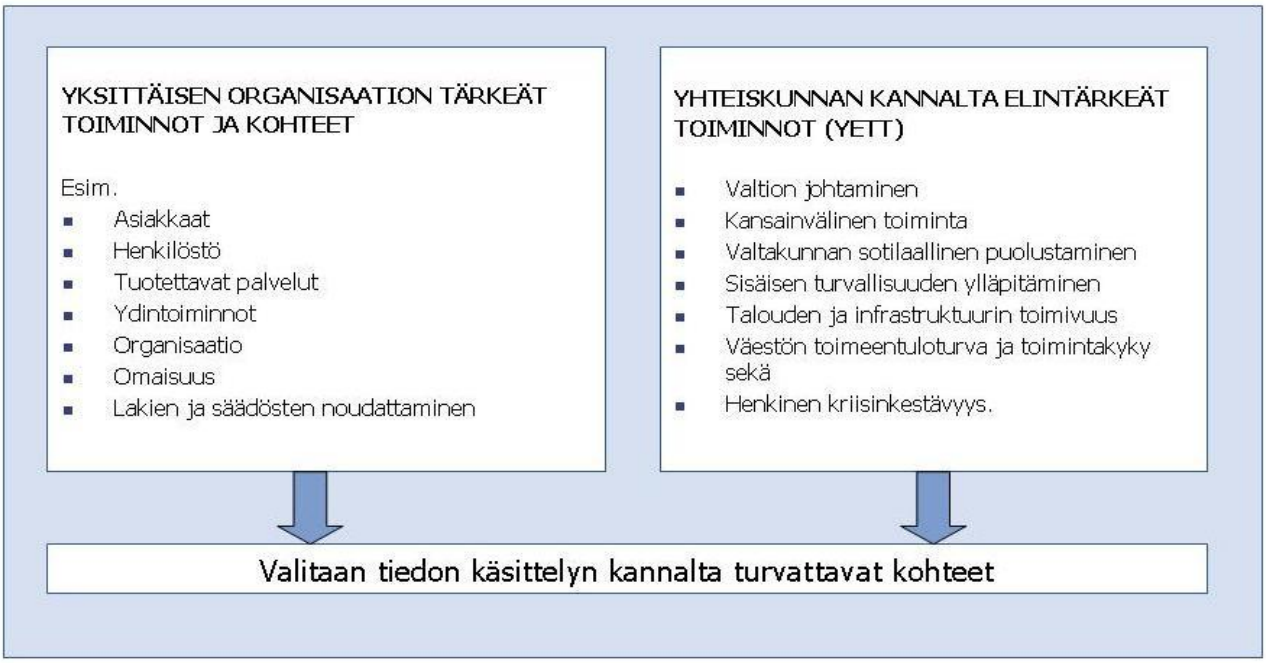
Tietoturvallisuus ja tietoturvatasot käsitteinä

Tietoturvallisuus sanana herättää jokaisessa ihmisessä erilaisia mielikuvia ja ne muokkautuvat tiedon lisääntyessä. Tietoturvatasot käsitteenä on kohtalaisen uusi ja siksi kysyimme mielleyhtymiä hallinnossa keväällä 2007. Mitä erilaisimmat ajatukset ja mielenkiintoiset analogiat löytyvät liitteestä 7.

2 Tärkeät toiminnot, turvattavat kohteet, turvataso ja kypsyys

Organisaation toiminnan luonne, tehtävät ja sen osien keskeisyys yhteiskunnan kannalta vaikuttavat sille asetettaviin turvallisuusvaatimuksiin. Vaatimusten ja turvatoimenpiteiden kohdistaminen vaatii tärkeiden toimintojen ja kohteiden tunnistamista.

Tärkeyttä voidaan arvioida monella eri tavoin, esimerkiksi organisaation oman toiminnan, asiakkaiden, sidosryhmien tai yhteiskunnan kannalta. Tärkeiden toimintojen ja kohteiden määrittäminen on lähtökohta turvallisuuden suunnittelulle ja toteutukselle (kuva 2).



Kuva 2. Organisaation kannalta tärkeät toiminnot ja kohteet tulee tunnistaa. Kohteista valitaan tiedon käsittelyn kannalta turvattavat kohteet. Kuvassa on esimerkkeinä esitetty organisaation ja yhteiskunnan kannalta tärkeitä toimintoja ja kohteita (YETT, yhteiskunnan elintärkeät toiminnot -strategia).

Tietoturvatasot koskettavat kaikkia valtionhallinnon organisaatioita

Vaikka raportissa painotetaankin organisaatioiden merkitystä yhteiskunnan ja kansalaisten kannalta, kannattaa huomioida, että tämä koskettaa kaikkia organisaatioita. Organisaation tehtävä yhteiskunnassa ja sen toiminta vaikuttaa turvatoimenpiteisiin.

Kun tärkeistä toiminnoista tai niiden osista valitaan tietyt kohteet, joihin turvatoimenpiteet ja menettelyt kohdistetaan, voidaan puhua **turvattavista kohteista**. Tiedon käsittelyn osalta turvattavia kohteita voivat olla esimerkiksi

- Tiedot (eri muodoissaan)
- Inhimilliset resurssit
- Tietojärjestelmät
- Käyttöympäristö
- Fyysinen ympäristö
- Ulkoiset palvelut, hankinnat
- Edellä mainittuja palvelevat prosessit

Turvattavia kohteita voidaan tarkastella myös muiden turvallisuuden osa-alueiden näkökulmasta vastaavalla menettelyllä. Kokonais(tieto)turvallisuuden ohjaamisessa tulee olla vahva, kansallinen ja luotettu **turvallisuusviranomainen** (VM), joka kykenee luomaan tarvittavan arviointikapasiteetin.

Eri organisaatioiden välisen luottamussuhteen varmistamiseksi ja yhteistyön helpottamiseksi on tärkeää, että turvattavat kohteet ovat **jäsenneltyjä ja yhteisesti ymmärrettäviä**. Tämä on mahdollista yhteisellä nimeämiskäytännöllä.

2.1 Turvattaviin kohteisiin liittyvistä vaatimuksista saadaan turvatasoja

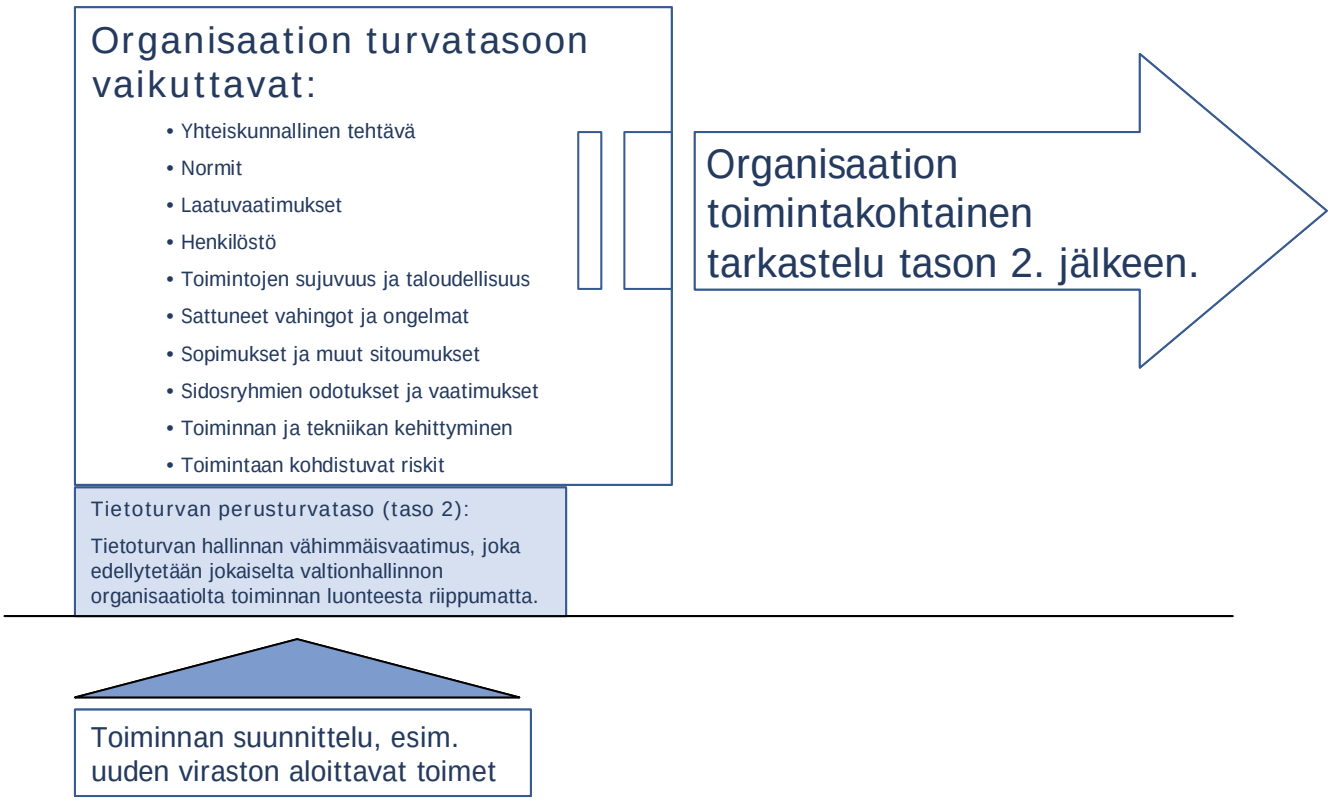
Turvattaviin kohteisiin liittyy erilaisia vaatimuksia (kuva 3). Tässä hankkeessa on tutkittu, millaiset vaatimukset voivat koskea koko valtionhallintoa ja yksittäistä organisaatiota sekä miten ne määritellään, suunnitellaan ja toteutetaan toiminnassa.

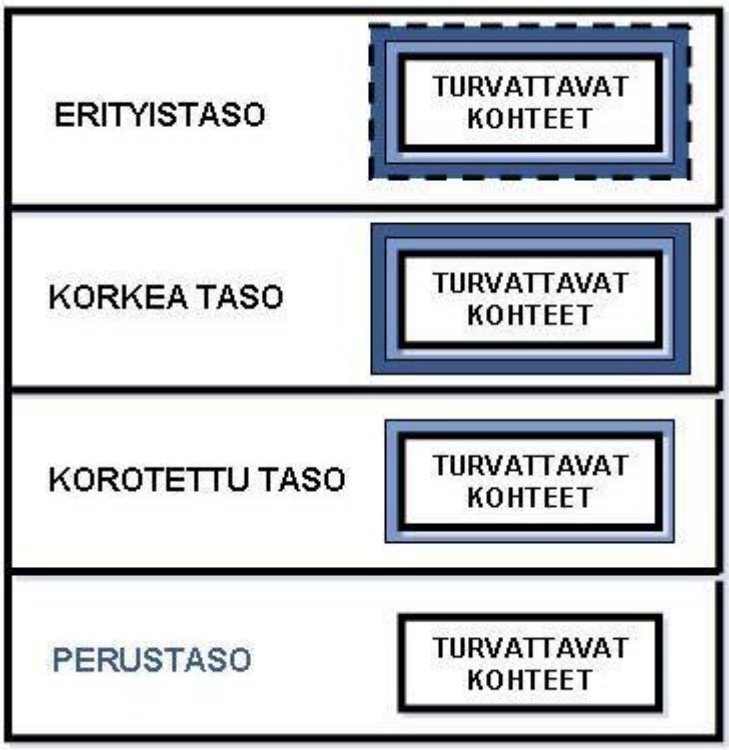
Yksittäisen organisaation tulee erityisesti turvata ne ydintoiminnot, joilla se varmistaa säädösten mukaisen toiminnan. Tiedon käsittelyn turvaaminen on toiminnan jatkuvuuden varmistamisen perusedellytys.

Yksittäiseen, turvattavaan kohteeseen liittyy tietoturvallisuuden osalta tiedon käsittelyn turvaamiseen liittyviä vaatimuksia, kuten:

- Luottamuksellisuus; tiedot ovat vain niiden saatavilla, joilla on siihen oikeus.
- Eheys; tieto on oikeaa, oikea-aikaista ja laadukasta.
- Käytettävyys, saatavuus; tieto on käytettävissä silloin, kun sitä tarvitaan.

Kuva 3. Yllä on kuvattu esimerkki turvattavista kohteista ja niihin liittyvistä tiedon käsittelyn turvallisuusvaatimuksista. Lähtökohtana on turvattavien kohteiden ja niihin liittyvien turvatavoitteiden määrittäminen. Vaatimukset luokitellaan, jolloin syntyy turvatasoja. Alla on kuvattu perustaso organisaation kivijalkana. Toiminnan aloittavan organisaation tulee päästä perustasolle.





Kuva 4. Turvataso liittyy aina turvattavaan kohteeseen.

Kuvassa näkyy neljä turvatason nimeä. Turvattavan kohteen ympärillä oleva kehys kuvaa suojausta.

Valtionhallinnon organisaatioilta edellytetään vähintään perustasoa turvatoimenpiteissä ja –menettelyissä. Erityistason vaatimukset toteutetaan tapauskohtaisesti, sillä erityistason turvallisuutta toteuttavan organisaation tulee olla tarpeeksi kypsä itse vastaamaan tarvittavien toimenpiteiden ja –menettelyjen suunnittelusta sekä toteutuksesta.

Hankkeessa päädyttiin käyttämään neliportaista tasoluokitusta, koska se katsottiin olevan selkeä ja käytetty mm. tilojen sekä turvajärjestelmien turvatasoluokituksessa. On samalla yhteensopiva CMM-mallien kanssa.

Turvatasot ovat luokiteltuja vaatimuksia

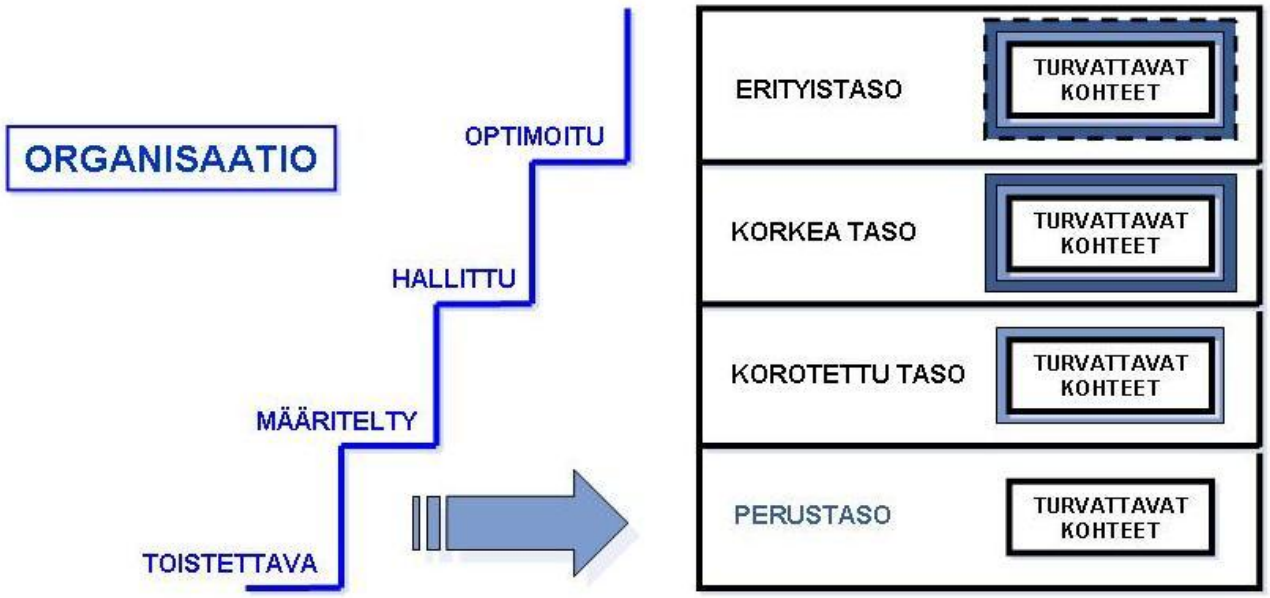
Turvatasot ovat luokiteltuja turvatoimenpide- ja menettelyvaatimuksia, jotka kohdistuvat tietyn turvattavan kohteen tai kohderyhmän suojaamiseen (kuva 4). Sama turvataso ei välttämättä koske koko organisaatiota, vaan sen sisällä voi olla eri tasoja, turvattavasta kohteesta riippuen. .

2.2 Turvataso edellyttää organisaatioilta kypsyyttä

Organisaatio tai sen osa tulee olla tarpeeksi kypsä (kyvykäs) hallitsemaan sen turvattaville kohteille asetettua korkeinta turvatasoa. Mitä keskeisemmin turvattava kohde liittyy organisaation toimintaan, sitä selvemmin kypsyystason tulee näkyä toiminnassa. Kypsä organisaatio osaa hallita, suunnitella ja toteuttaa tarvittavat toimenpiteet ja menettelyt sille parhaiten sopivalla tavalla.

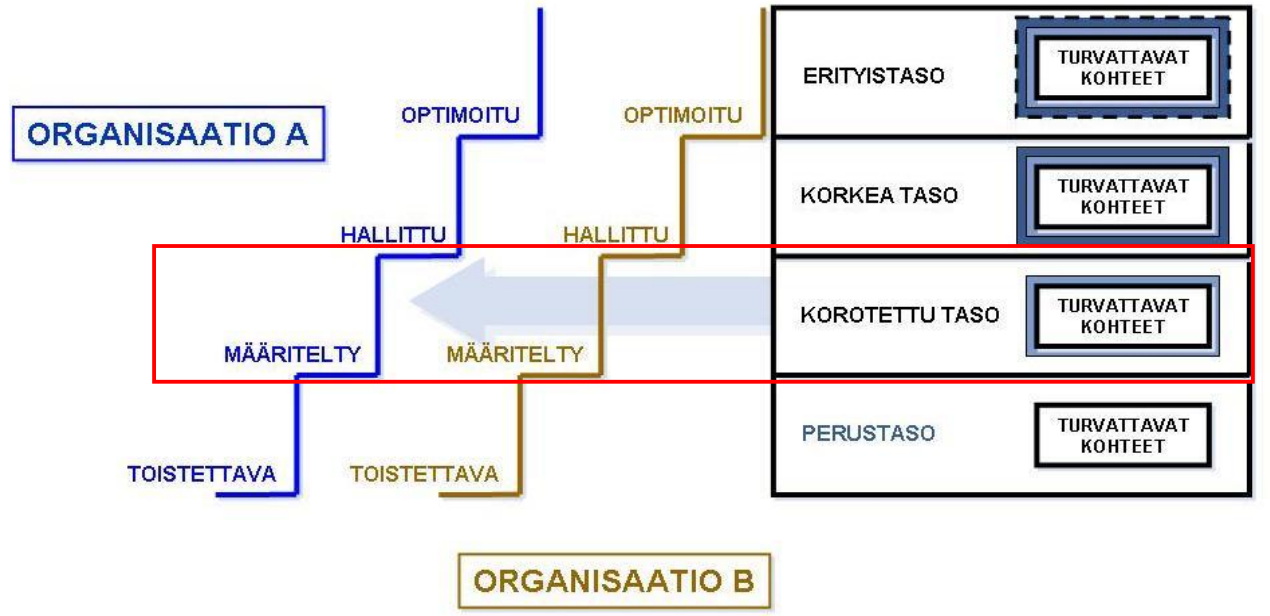
Organisaatiossa voi olla eri turvatason vaativia kohteita. Organisaatiossa voi olla eri kypsyystasolla olevia yksiköitä. Näin voidaan järjestää tiettyjen tärkeiden toimintojen kohdalla. Tällöin organisaation osa voi olla esimerkiksi erityistasolla fyysisesti erotettu, tietyn henkilöryhmän muodostama yksikkö.

Turvataso edellyttää organisaatiolta kypsyyttä vastata sen asettamiin vaatimuksiin. Esimerkiksi toistettavalla tasolla olevalle organisaatiolle erityistason turvatoimenpiteiden ja – menettelyjen toteuttaminen on sattumanvaraista. Hallitulla tasolla oleva organisaatio pystyy vastaamaan kaikkien turvatasojen vaatimuksiin (kuva 5).



Kuva 5. Turvataso edellyttää organisaatiolta kypsyyttä. Kypsyystasot kuvaavat organisaation johtamisen, tietoturvaprosessien ja turvatoimenpiteiden kehittyneisyyttä. Kuva on esimerkki.

Organisaatioilla voi kokonaisuudessaan olla eri kypsyystasot, mutta turvattavien kohteiden kannalta on varmistettava, että turvataso säilyy myös alemman kypsyystason organisaatiossa. Käytännössä tämä voi tapahtua esimerkiksi ohjeistamalla alemman kypsyystason organisaatiota turvatavan kohteen käsittelyssä. Turvattavan kohteen omistajaorganisaatio vastaa turvatason toteutumisen valvonnasta. Yhteistoiminnassa joudutaan joskus välittämään, ylläpitämään tai käsittelemään yhteisesti turvattavia kohteita, kuten tietoja, tietojärjestelmiä, palveluita jne. Tällöin on tärkeää, että kohteen turvallisuus säilyy organisaatiosta riippumatta (kuva 6).



Kuva 6. Turvattavan kohteen vaadittava turvataso tulee toteuttaa myös yhteistyössä, vaikka organisaatioilla olisi eri kypsyystasot. Kuva on esimerkki.

2.3 Palvelun toimittajan kypsyys auttaa tilaajaa hallitsemaan tietoturvallisuutta

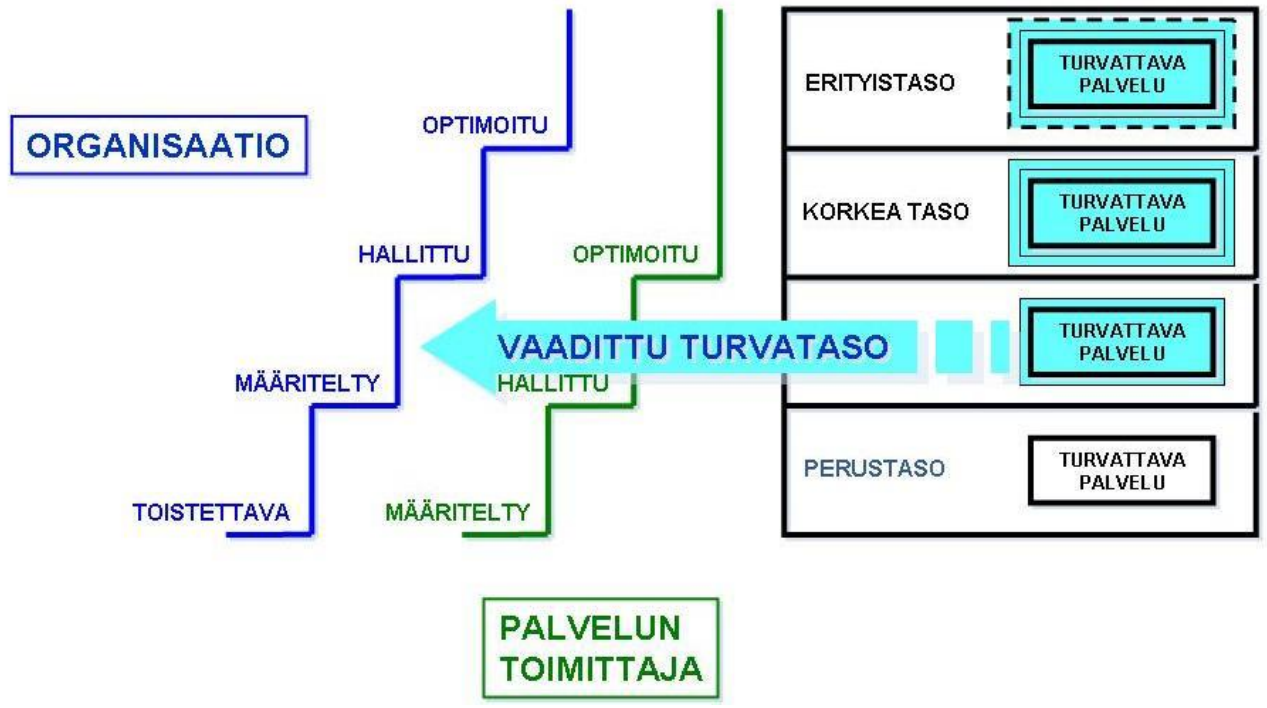
Turvattava kohde voi olla hankittava palvelu. Tällöin palveluntarjoajan tulee kyetä vastaamaan palvelun turvallisuusvaatimuksiin koko elinkaaren ajan.

Koska turvallisuusvaatimukset usein kasvavat, erityisesti pitkäkestoisessa palvelussa (esimerkiksi käyttöpalvelu), palveluntarjoajan tulee kyetä vastaamaan vaativampaan tarpeeseen (kuva 7). Pitkäkestoisessa palvelussa toimittajaorganisaation tulee olla turvattavan palvelun osalta vähintään yhtä kypsä kuin korkeinta turvatasoa vaativa organisaation osa.

Palvelun turvatasovaatimus ja tarjottavan palvelun turvataso tulee alustavasti kuvata jo tarjousvaiheessa. Tason sisältö tulee määritellä ja dokumentoida palvelun sopimusta laadittaessa. Samassa yhteydessä tulee sopia menettelystä turvatason mahdollisessa nostamisessa. Palvelun turvatason toteutumista valvotaan auditoimalla säännöllisesti sovittuun turvatason suhteen.

Palvelun turvatason määrittäminen on yhteinen etu

Palvelun turvatason määrittäminen helpottaa sekä palvelun hankkimista, että sen toimittamista. Kun palvelun hankkija on kuvannut selkeästi halutun turvatason, palveluntarjoaja kykenee määrittämään palvelun turvatason ja palvelun tuottamisen kustannukset sen mukaisesti. Tämä johtaa suunnitelmalliseen hinnoitteluun ja vähentää jälkikäteen käytävää sopimustulkintaa. Oikein sovittu ja hinnoiteltu palvelu varmistaa, että palvelun toimittaja ei tingi laadusta. Vastaavasti hyvin tehdyt sopimukset varmistavat, että palvelun sisältö on helposti tulkittavissa ja auditoitavissa.



Kuva 7. Esimerkki palvelusta, jossa toimittajalla on korkeampi kypsyystaso kuin asiakkaalla.

Tilaavalla organisaatiolla on vastuu palvelustaan ja velvollisuus seurata sovituilla tavoilla palveluntoimittajaa. Toimintaa, taloutta tai palveluita tarkastavilla tahoilla on oltava tarpeeksi pitkälle yltävä auditointioikeus myös palveluntuottamisen aikana. Tilaavan organisaation on huolehdittava sopimuksiin riittävät maininnat auditoinneista ja muista laatua varmistavista käytännöistä.

Tilaavan organisaation haluamiin vaatimuksiin löytyy rakenne ja vaihtoehtoja seuraavassa kappaleessa 3: kypsyyskuution 3.1 ja turvakuution 3.2 mukaiset tietoturvallisuuden hallintakeinot (TH). Valittaviin ratkaisuihin ja palveluntoimittajien tuottamiin kuvauksiin on ehdotus toteuttamiseen liitteessä 1 (keltaiset kortit).

YHTEENVETO TURVATASOISTA

- TURVATASOT OVAT LUOKITELTUJA TURVATOIMENPIDE- JA MENETTELYVAATIMUKSIA.
- TURVATASOVAATIMUS EDELLYTTÄÄ ORGANISAATIOLTA VASTAAVAA KYPSYYTTÄ STRATEGISESSA JOHTAMISESSA, TURVALLISUUDEN HALLINNASSA JA TURVATOIMENPITEISSÄ
- VAATIMUSTEN TULEE PERUSTUA NORMEIHIN, OLEMASSA OLEVIIN STANDARDEIHIN JA HYVIIN KÄYTÄNTÖIHIN.
- TURVATASOJEN JALKAUTTAMINEN EDELLYTTÄÄ OHJAUSTA JA YHTENÄISIÄ NORMEJA.
- VALTIONHALLINNOSSA TULEE TUNNISTAA TOIMINNAN KANNALTA TÄRKEÄT JA TURVATTAVAT KOHTEET. LISÄKSI KOHTEIDEN TURVAAMISEN TAVOITTEISTA TULEE PÄÄTTÄÄ.
- VALTIONHALLINNOSSA YHTEISELLE TURVATASOLLE ON MAHDOLLISTA ASETTAA YHTENÄISET VAATIMUKSET, KUN EM. PÄÄTÖKSET ON TEHTY.
- TURVATASOJEN VAATIMUKSET KOSKEVAT HALLINNON SIDOSRYHMIÄ, KUTEN ALIHANKIIJOITA JA TOIMITTAJIA.
- PERUSTURVATASON VAATIMUSTEN TULEE TÄYTYÄ TAMMIKUUN 2011 ALUSSA.
- RIIPPUMATON AUDITOINTI VARMISTAA YHTEISTEN VAATIMUSTEN NOUDATTAMISEN KAIKILLA TASOILLA JA MUODOSTAA PERUSTAN LUOTTAMUSSUHTEELLE.

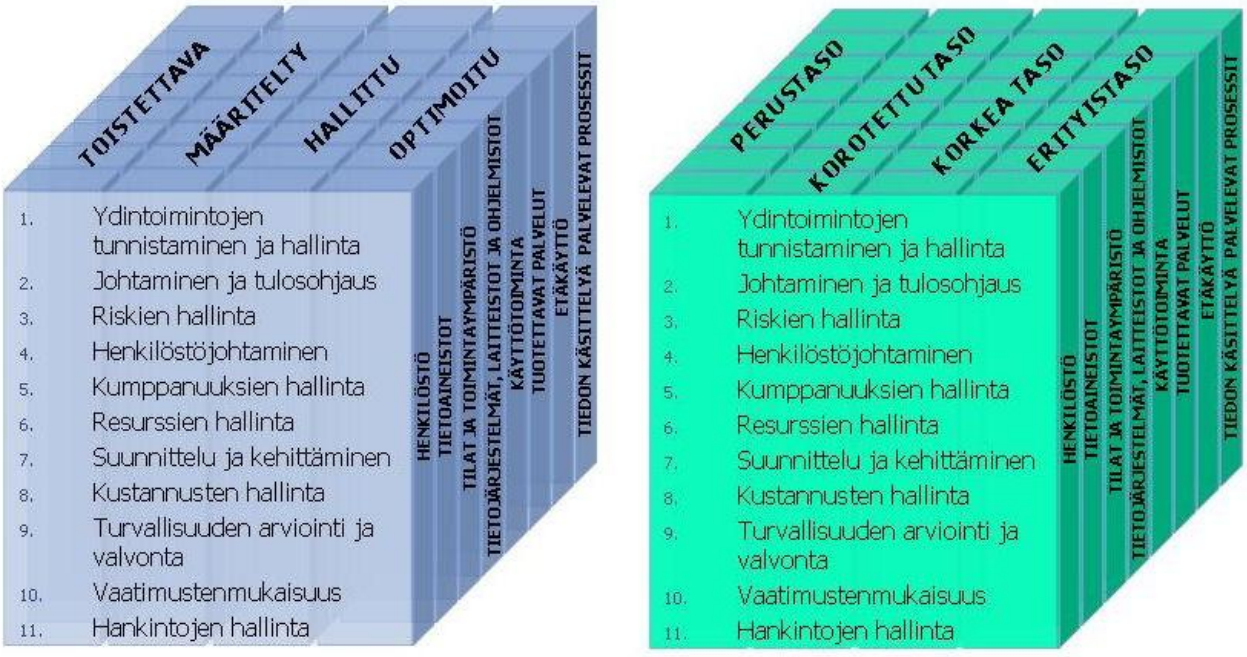
3 Kypsyys- ja turvatasomalli

Hankkeen alussa todettiin, että lähes jokaisella oli eri käsitys organisaation kypsyydestä ja turvatasoista. Kypsyys- ja turvatasokäsitteet koottiin kokonaisuuksiksi, jotka kuvataan kahtena erillisenä kuutiona. Kuutiot auttavat kokonaisuuden hahmottamisessa ja helpottavat yhteisen käsitteistön muodostamista.

Käytännön toteutukseen tarvitaan selkeitä työvälineitä ja palveluita. Välineitä pohdittiin alustavasti hankeryhmän ja seurantaryhmän yhteisessä työpajassa 29.3. Kaikki 29.3. työpajan tulokset löytyvät liitteestä 8. Tärkein tavoite on saada tietoturvallisuuden hallinnan kypsyys ja turvatasot näkymään käytännössä.

Tietoturvallisuuden kehittämiseen tarvitaan yhteistyötä, ohjausta ja palveluita:

- Halutaan normeja, normiluettelo ja normien tulkintoja tietoturvallisuuden kannalta;
- Ohjeistoja, sähköinen portaali VAHTI-ohjeille ja hakutoimintoja;
- Neuvontapalvelua, yhteiskäyttöisiä koulutusmateriaaleja ja koulutusta;
- Tarkistuslistoja ja sopimusmalleja
- Kartoitus- ja auditointipalveluja
- Asiantuntijaverkostoja ja hiljaisen tiedon levittämistä



Kuva 8. Kuutioissa näkyy miten kypsyys ja turvataso on jaettu samantyyppisiin rakenteisiin. Vasen vihreä turvakuutio kuvaa turvattavan kohteen tavoiteltavaa tai sovittua turvatasoa. Oikealla oleva sininen kypsyyskuutio kuvaa organisaation kyvykkyyttä hallita tietoturvallisuutta. Molemmissa tasoja on 4 kappaletta ja etummaisen sivujen turvattavat kohteet ovat samat. Kuutioiden rakenteet

auttavat hahmottamaan kokonaisuutta. Kuutioiden osat avataan ohjeiksi, tarkistuslistoiksi, työvälineiksi, koulutusmateriaaleiksi jne.

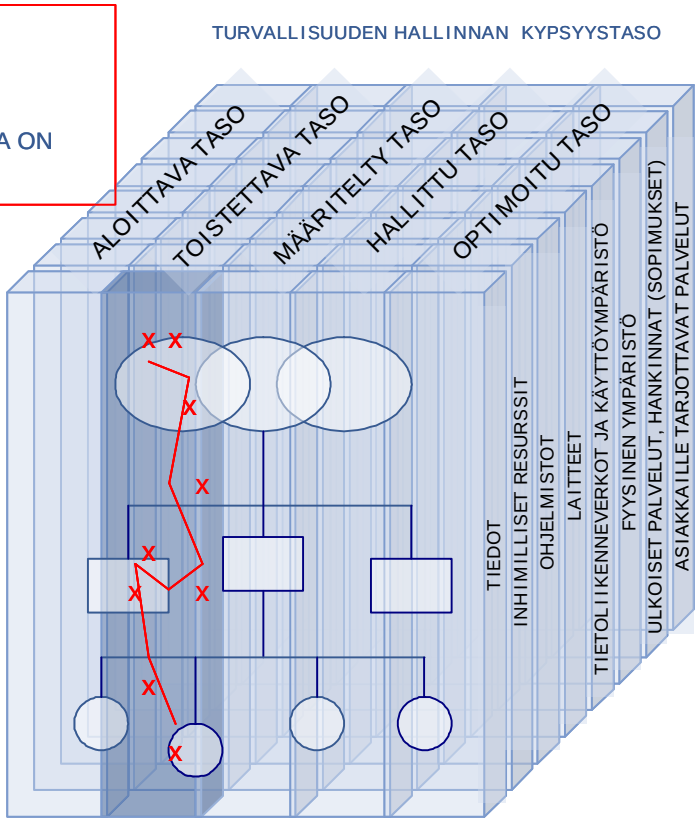
3.1 Kypsyys on organisaation kyvykkyyttä hallita tietoturvallisuutta

Kypsyys muodostuu strategisen johtamisen, tietoturvatoiminnan ja turvatoimenpiteiden kyvykkyydestä. Kypsän organisaation kyvykkyyden eri osa-alueet muodostavat tasapainoisen ketjun johtamisesta käytännön toimenpiteisiin.

KYPSYYS MÄÄRITTÄÄ, MITEN KYVYKÄS ORGANISAATIO ON TIETOTURVALLISUUDEN HALLINNASSA

TURVALLISUUDEN HALLINNAN TAVOITTEENA ON TURVATA VALITUT KOHTEET

1. Johtaminen ja tulosohjaus
2. Henkilöstöjohtaminen
3. Kumppanuuksien hallinta
4. Resurssien hallinta
5. Asiakkaille ja kansalaisille tuotettavien palveluiden hallinta
6. Suunnittelu ja kehittäminen
7. Kustannusten hallinta
8. Toiminnan jatkuvuuden hallinta
9. Riskien hallinta
10. Tietoturvallisuuden arviointi ja valvonta
11. Vaatimustenmukaisuus
12. Hankintojen hallinta



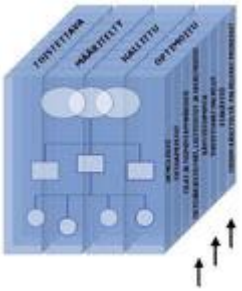
Kypsän ja kyvykkään organisaation tunnuspiirteitä turvallisuuden hallinnassa ovat muun muassa

- ylimmän johdon selvä näkyvyys, esimerkillinen toiminta ja sitoutuminen turvallisuusasioissa
- turvallisuuden vastuuttaminen koko organisaatioon työtehtävien mukaisesti
- turvallisuuden säännöllinen arviointi suhteessa toimintaan ja turvattaviin kohteisiin liittyviin vaatimuksiin

- säännöllinen riskien arviointi, analysointi ja riskienhallinnan suunnittelu
- suunnitellut ja tehokkaasti toteutetut turvamenettelyt ja –toimenpiteet
- turvallisuuden näkyminen käytännön työssä ja toteutuksissa.
- jne..

Kypsyysmallin osa-alueet eli kuution sivut ovat:

1. Turvattavat kohteet



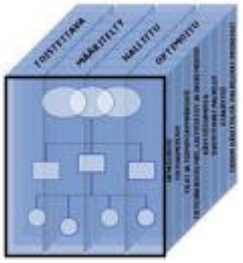
- määräytyvät organisaatiokohtaisesti tai
- asetetaan valtionhallinnon ohjaamana
- lukumäärä riippuu em. tekijöistä
- kohteiden turvaamiseen laaditaan yksityiskohtaiset ohjeet merkinnällä ”**KT**”, kohteiden turvaaminen

2. Skaalattu luokittelu kyvykkyyden perusteella

Neljä (4) kypsyystasoa:

- optimoitu
- määritelty
- hallittu
- toistettava - valtionhallinnon perustaso

3. Tietoturvallisuuden hallintakeinot



- keinot, menetelmät
- niihin liittyvä arviointikriteeristö
- Ohjeistoissa tietoturvallisuuden hallinnan menettelyt merkitään ”**TH**”, tietoturvallisuuden hallinta

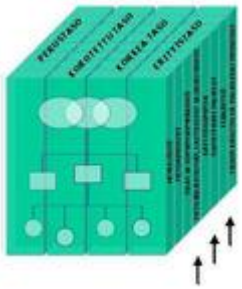
3.2 Turvatasot ovat luokiteltuja turvatoimenpide- ja menettelyvaatimuksia

- Turvatason vaatimukset tähtäävät turvattavan kohteen suojaamiseen. Koska turvatoimenpiteiden ja -menettelyjen vaativuus vaihtelee kohteen tärkeydestä ja kriittisyydestä riippuen, joudutaan vaatimukset luokittelemaan.
- Turvataso muodostuu strategisen johtamisen, tietoturvatoiminnan ja turvatoimenpiteiden vaatimuksista. Turvavaatimusten tehtävänä on muodostaa ehjä ja tasapainoinen ketju.

Turvatasomallin osa-alueet eli kuution sivut ovat:

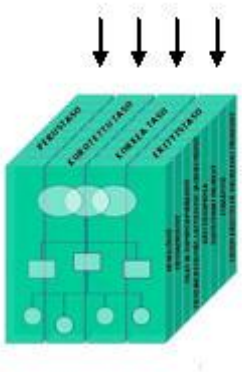
1. Turvattavat kohteet (kuten kypsyysmallissa)

- määräytyvät organisaatiokohtaisesti tai
- asetetaan valtionhallinnon ohjaamana
- lukumäärä riippuu em. tekijöistä



2. Skaalattu luokittelu turvatoimenpiteiden ja –menettelyjen vaatimustason mukaan

- Neljä (4) turvatasoa
- erityistaso
- korkea taso
- korotettu taso
- perustaso valtionhallinnossa



3. Tietoturvallisuuden hallintakeinot

- keinot, menetelmät sekä
- niihin liittyvä vaatimusten kuvaus.

Jos haluat siirtyä raportissa nopeammin eteenpäin ja katsoa, miten konkretisoidaan kuutiot ja saadaan tietoturvallisuutta tukevat välineet käyttöön, siirry suoraan kappaleeseen 7.

4 Koko hallintoa koskevan turvatason toteuttaminen on mahdollista

Kokonaisturvallisuus edellyttää turvallisuuteen liittyvien toimintojen (prosessien) miettimistä ja toteuttamista. Organisaation toiminta on riippuvaista sen turvattavien kohteiden, välineiden ja palveluiden toiminnasta. Liitteessä 4 on kuvattu esimerkki tavoitetilasta, jossa organisaatio tunnistaa turvatasojen perustana olevat tarpeet.

Turvallisuusjohtaminen on organisaation strateginen toiminto. Tulosprisman sitominen turvallisuuteen on toteutettu vasta harvoissa hallinnon organisaatioissa. Jatkohankkeessa tärkeää on lisätä turvallisuus osaksi tulosprismaa. Tulosprisman tulisi tukea kokonaisturvallisuuden hallintaa. Turvallisuus- ja tulosjohtamiselle on ohjeistusta VAHTI-julkaisuissa.

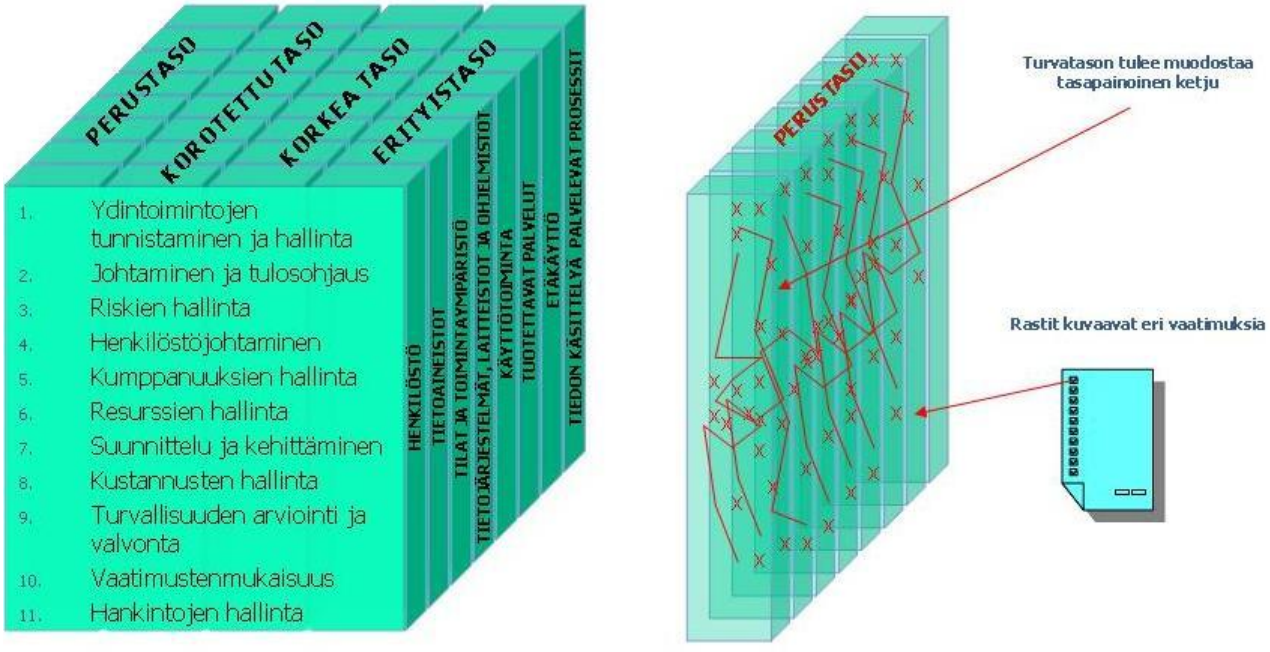
4.1 Koko hallintoa koskeva perusturvataso turvattaville kohteille

Hankeryhmä selvitti, millaista turvatasoa koko valtionhallinnolta voidaan vähimmäisvaatimuksena (perusturvataso) edellyttää. Perusturvataso on mahdollista kuvata karkeasti kolmella eri tavalla:

1. Ottamatta kantaa toiminnan luonteeseen tai turvattaviin kohteisiin. Tällöin tason tulee olla taloudellinen, yleistettävissä ja yleisesti hyväksytty.

2. Se voidaan rajata tiettyihin turvattaviin kohteisiin, jolloin niiden turvatavoitteet ja –taso on määritetään tarkemmin.

3. Se voidaan kohdistaa suurempaan määrään turvattavia kohteita ja määrittää turvatavoitteet sekä –taso on tarkemmin.



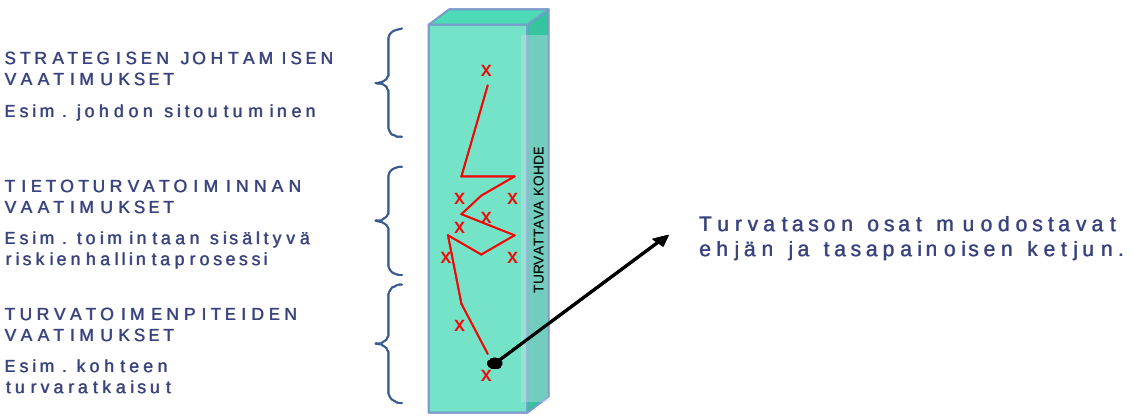
Kuva 9. Turvakuution avaaminen esittää, miten perusturvataso sijoittuu kuutiossa ja miten se muodostaa ketjun .

Toteutusvaihtoehtoa 1. tutkittiin hankeryhmän ja seurantaryhmän yhteisessä työpajassa. Siellä tuotiin esiin mm. seuraavia vähimmäisvaatimuksia:

- Suojattavien kohteiden määrittely ja riskien hallinta sen mukaisesti;
- Tietoturvallisuuden seuranta, valvonta ja raportointi;
- Poikkeamien seuranta käsittely ja seuranta;
- Lokitietojen seuranta ja kriittisissä toiminnoissa jäljitettävyys;
- Säännöllinen, toimintaan ja johtamiseen liittyvä riskianalyysi, jossa tietoturvallisuus on huomioitu;
- Johdon sitoutumisen osoittaminen oman esimerkin kautta;
- Riittävä resursointi tietoturvatyöhön;
- Tietoturvallisuus on vastuutettu työtehtävien ja roolien mukaisesti;
- Tietoturvallisuuden vastuuhenkilö oltava olemassa;
- Tietoturvallisuus tulosohjauksessa pitkän tähtäimen suunnitteluna ja budjetointina;
- Auditointi (mitä, miten, miksi, milloin, kuka, missä);
- Tietojärjestelmien ja Internet –käytön ”pelisäännöt”;
- Tietoturvaohjeiden kattavuus (myös sidosryhmät huomioidaan);
- Jatkuva tietoturvakoulutus vähintään omalle henkilöstölle jo rekrytoinnista lähtien;
- Työsuhteet organisaation ulkopuolella (etätyö, etäkäyttö);
- Tietoaineistojen käsittelyssä tarvittava perustietämys;
- Henkilöstön tietoturvatietoisuus, erityisesti omaa toimintaa koskevat lait ja asetukset.

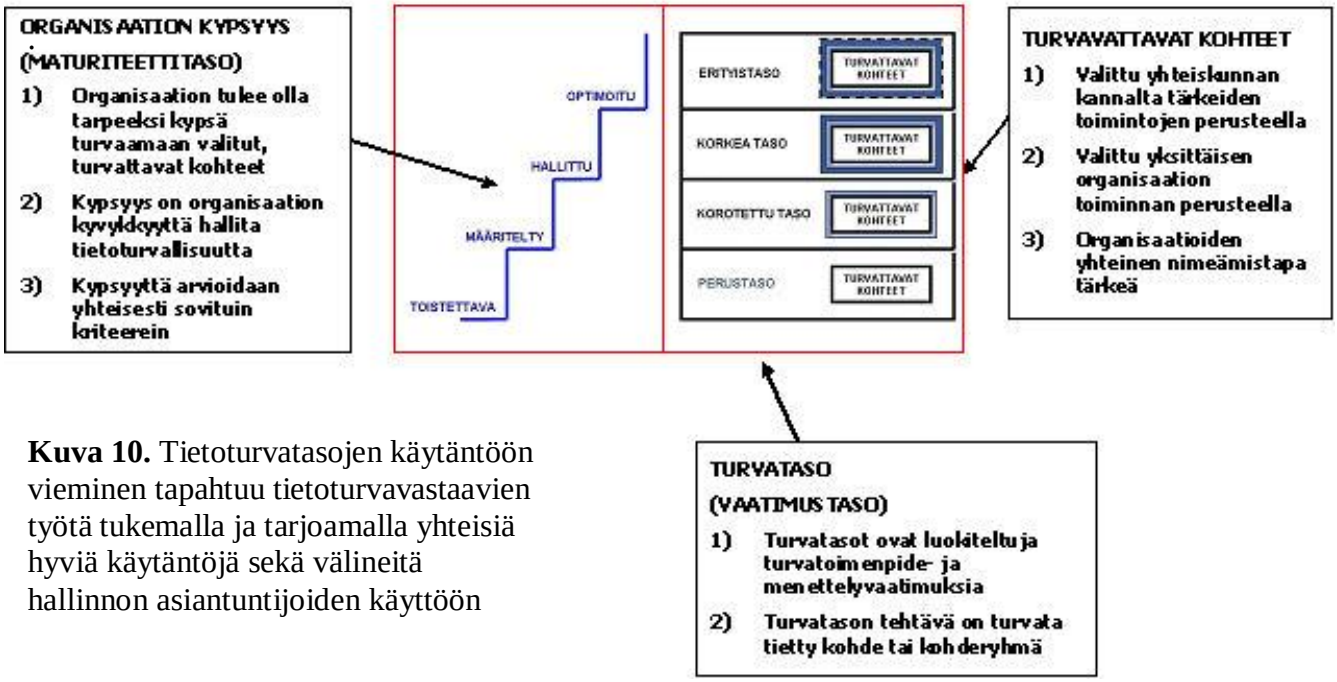
Yllä olevassa listassa ei ole eritelty vaatimuksia turvattaviin kohteisiin ja organisaation kypsyyteen.

Liitteessä 1 on ehdotus turvatasojen rakenteelle ja jatkomäärittelylle. Turvatasojen asettamien vaatimusten toteuttamisen kustannusten laskentaa on tehty luonnos välineessä liitteessä 4.



Koko valtionhallintoa koskevien turvatasojen tarkka määrittäminen edellyttää turvattavista kohteista sopimista ja turvaamistavoitteiden määrittämistä. Alla olevassa kuvassa on esitetty

raportissa kuvattujen osa-alueiden liittyminen toisiinsa.



Kuva 10. Tietoturvatasojen käytäntöön vieminen tapahtuu tietoturvavastaavien työtä tukemalla ja tarjoamalla yhteisiä hyviä käytäntöjä sekä välineitä hallinnon asiantuntijoiden käyttöön

4.2 Kansainvälinen tilanne ja valittu lähestymistapa

Islannissa ja Tanskassa on aloitettu toteuttamaan turvatasoajattelua julkishallinnossa. Molempien turvallisuusvaatimukset perustuvat kansainvälisiin standardeihin ja hyviin käytäntöihin. Islanti on asettanut perustason CMM:n ja COBITin asteikolla kypsyystasolle 3. Tämä taso vastaa lähinnä tämän dokumentin kypsyyskuution määriteltyä tasoa.

Amerikassa National Institute of Standards and Technology, NIST on tuottanut FIPS PUB 200 : minimiturvallisuusvaatimukset hallinnon tiedon ja tietojärjestelmien turvaamiseksi. Ohje on valmisteltu standardiksi FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION - Minimum Security Requirements for Federal Information and Information Systems [lähde 23].

Kypsyyttä ja turvatasoja sovelletaan kansainvälisesti eri keinoin. Yleistyvä käytäntö on eri standardien ja hyvien käytäntöjen yhteensovittaminen (ISO 17799 + CMM; ISO 27001 + ITIL + COBIT jne.).

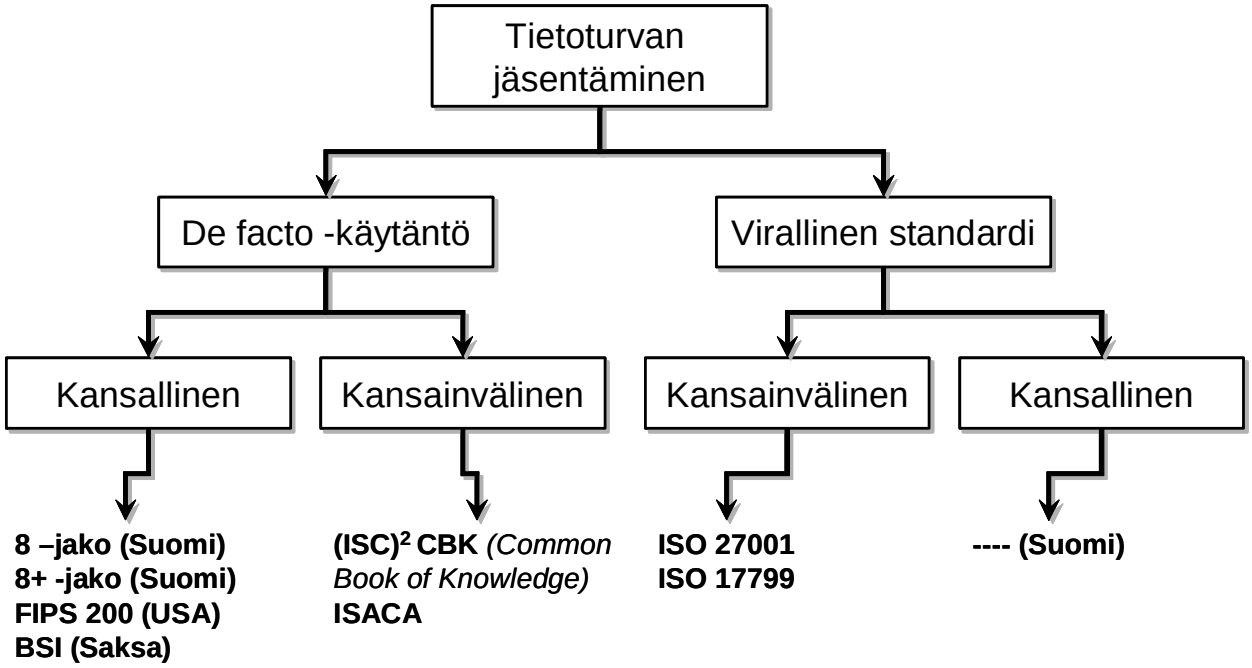
Hankeryhmä päätyi soveltamaan yleisesti käytettyä ISO 27001 –standardin turvakontrollien ja CMM–kypsyysasteikon sekä Cobit–mallin yhdistelmää, jota täydennettiin CAF–laatupalkintokriteeristön elementeillä. Skaalaamisessa käytettiin CMM/Cobitista 4 (ylintä) tasoa.

Hankkeessa poimittiin ISO 27001-standardin turvakontrolleja turvattavien kohteiden suojaamiseen. Standardia sovellettiin tietoturvallisuuden hallinnan kokonaisuuden määrittämisessä. Hanke on yhteensopiva ISO 27001 –standardin kanssa ja antaa pohjan tietoturvallisuuden hallintajärjestelmän rakentamiseen. Alla olevassa kuvassa on kuvattu vaikuttavat asiat ja tavoitetila organisaation tietoturvallisuuden hallinnalle.

5 Standardointi ja hyvät käytännöt apuna kypsyyden ja turvatasojen määrittämisessä

Vaatimusten tulee perustua normeihin, olemassa oleviin standardeihin ja hyviin käytäntöihin. Sillä varmistetaan yhdenmukaisuus eri organisaatioiden kesken. Standardit ja hyvät käytännöt auttavat jäsentämään vaatimuksia sekä niiden todentamista. Kuva 10 alla jäsentää hallinnossa käytettyjä jaotteluita ja standardeja, luettelo ei ole täydellinen.

Suomessa tietoturvallisuuden mallintamiseen on käytetty yli 10 vuoden ajan valtionhallinnon tietoturvallisuuden johtoryhmän, VAHTIn osa-aluejakoa (8). OECD on käyttänyt vastaavaa jaottelua. Jonkin verran uudistustarpeita osa-aluejakoon on esitetty ja uudistettua 8+-jaottelua esitetään VAHTI-8 lisättynä ISO9000-jaottelun mukaiseksi.



Kuva 11. Esimerkki tietoturvallisuuden jäsentämisestä standardien ja hyvien käytäntöjen avulla.

Jatkohankkeessa tulee selvittää, mitä vaikuttavia lähteitä kunkin valitun turvattavan kohteen osalta sovelletaan. Samoin arviointikriteereihin ja eri organisaatioiden väliseen yhteistyöhön kartoitetaan sopivimmat vaikuttavat lähteet.

6 Tietoturvallisuuden ohjaus eri näkökulmista

Valtionhallinnon poliittishallinnollisessa ohjauksessa käytettävät ohjauskeinot ovat:

- lainsäädäntö ja muu normatiivinen ohjaus
  - lait, asetukset ja muut oikeussäännöt sekä
  - organisaatiokohtaiset sitovat normit, kuten työjärjestykset
- taloudellinen ohjaus eli tehtävien hoitoon osoitetut voimavarat ja niiden käyttöä koskeva ohjaus
  - taloudellista ohjausta koskevat normit,
  - voimavarojen allokointikäytännöt/budjettiohjaus,
  - tulosohjaus ja -seuranta,
  - sopimusohjaus sekä
  - uutena keinona yhteishankinnat osana talousohjausta (talousarviolaki 22 a § 447/2006).
- rakenteet:
  - organisaatiot,
  - organisaatiorakenteet,
  - organisaatiomallit,
  - palvelujärjestelmät,
  - henkilöstörakenne,
  - ohjauksen rakenteet
- Kannustejärjestelmät
  - henkilöstön kannustejärjestelmät,
  - organisaatioiden kannustejärjestelmät,
- vastuujärjestelmät,
- johtamisen ohjaus,
- koulutus
- informaatio-ohjauksen eri muodot
  - ml. ohjeet, suositukset, standardit, kehittämislinjaukset ja tavoitteenasettelu
  - ohjelmaperusteiset hankkeet, politiikkaohjelmat, arviointi,
  - tietojen keruu, rekisterit, tilastot, muut tietovarannot ja muu seuranta,
  - tutkimus- ja kehitystyön tuloksena syntyvä tieto sekä koulutus ja professiot

6.1 Normit ja ohjaus organisaatioiden kannalta

Tietoturvatasojen käytäntöön vieminen edellyttää normeja ja ohjausta. Ohjaus ja säädäntö on nähty positiivisena ja jalkautusta helpottavana asiana. Vastaavasti on toivottu tukea käytännön toteutukseen ohjeiden ja palvelujen muodossa. Erityisesti on tuotu esiin tarve puhelinneuvonnalle.

Tietoturvatasojen toteutusta ohjaavana on alustavasti suunniteltu seuraava eteneminen

- 1) Tietoturvatasoja koskeva ohje,
- 2) Tietoturvatasovaatimukset sisällytetään sopivaan periaatepäätökseen ja
- 3) Tietoturvatasovaatimukset sisällytetään sopivaan asetukseen.

Tarkoitus on, että tietoturvatasot sisältyvät mahdollisimman luontevasti valtionhallinnon muuhun ohjaukseen ja toimintaan.

6.2 Valtion yhteisen IT-toiminnan ohjaus

Valtion yhteisen IT-toiminnan ohjauksessa ja koordinoinnissa käytettävät toimenpiteet ovat:

- valtioneuvoston määrittelemät, IT-toiminnan yleiset kehittämis- ja toimintaperiaatteet,
- asianomaisen hallinnonalan IT-toiminnan ohjaus edellä mainittujen linjausten mukaisena tulosohjauksena,
- valtiovarainministeriön informaatio-ohjaus,
  - perustuu valtioneuvoston linjauksiin,
- **yksittäisiä ratkaisuja koskeva velvoittava ohjaus,**
- talouden ohjaus sekä
- yhteishankinnat.

6.3 Ohjaus yhteiskunnan kannalta elintärkeiden toimintojen osalta

Valtioneuvosto hyväksyi 23. marraskuuta 2006 periaatepäätöksen yhteiskunnan elintärkeiden toimintojen turvaamisen strategiaksi. Periaatepäätöksellä ylläpidetään osaltaan valtiollista itsenäisyyttä, yhteiskunnan turvallisuutta sekä väestön elinmahdollisuuksia kaikissa turvallisuustilanteissa.

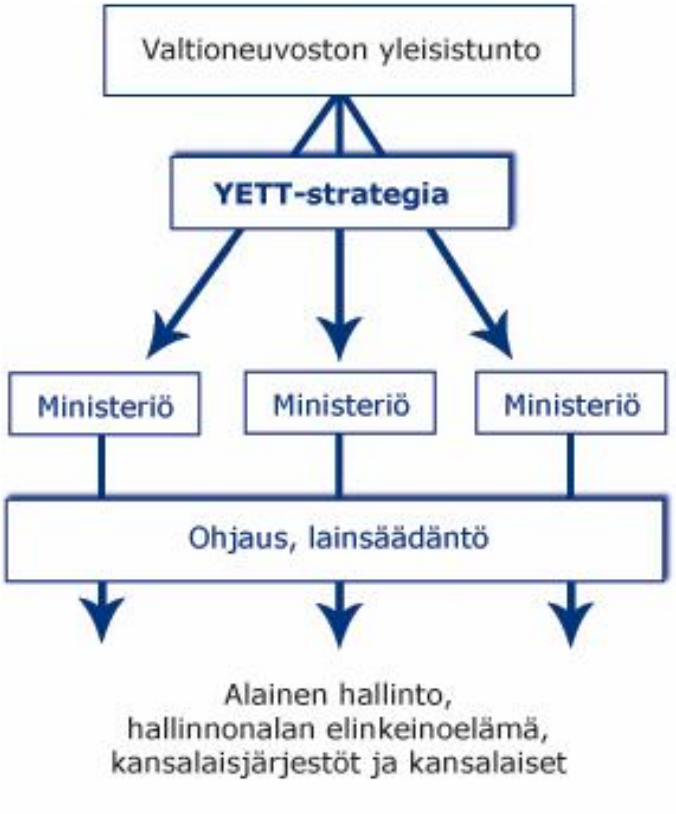
Strategiassa on otettu huomioon kansainvälistymisen sekä turvallisuusympäristön ja yhteiskunnan rakenteiden muutokset. Strategiassa nimetään ja määritellään yhteiskunnan elintärkeät toiminnot, niiden tavoitetilat sekä ministeriöille kuuluvat strategiset tehtävät. Lisäksi strategiassa on esitetty uhkamallit ja niihin sisältyvät erityistilanteet.

Yhteiskunnan elintärkeiden toimintojen turvaamiseksi ministeriöille on osoitettu yhteensä 50 strategista tehtävää. Valtioneuvoston kanslian vastuulla olevat tehtävät liittyvät valtioneuvoston

toiminnan turvaamiseen, EU:ssa päätettävien asioiden valmistelun ja käsittelyn kansalliseen yhteensovittamiseen sekä valtioneuvoston viestinnän toimivuuteen ja tilannekuvan ylläpitämiseen.

Erityistilanteissa valtioneuvoston kanslian vastuulla on tilanne, jossa tarkoituksellisesti haitallisesti vaikutetaan päätöksentekoon, yleiseen mielipiteeseen tai maanpuolustustahtoon.

[Lähde: Valtioneuvoston kanslia http://www.vnk.fi/toiminta/turvallisuus/Yett/fi.jsp]



Kuva 12. Ministeriöt ottavat YETT-strategian linjaukset huomioon hallinnonalansa ohjaamisessa ja lainsäädäntötyössä [Lähde: www.yett.fi]

Hallinnon kokonaisturvallisuuden ja tietoturvllisuuden ohjaamisessa Suomessa on oltava kansallinen ja luotettu turvallisuusviranomainen. Turvatasojen kannalta oleellista on, että viranomainen luo yhtenäiset vaatimukset ja tarjoaa tarvittavan arviointikapasiteetin.

7 Toteuttamissuunnitelma jatkotyölle on jaettu 5 kokonaisuudeksi

Hankeryhmä suunnitteli viisi jatkohanketta. Osiin jakamalla organisaatioiden kypsyyttä ja turvattavien kohteiden turvatasoa kehitetään ja viedään käytäntöön:

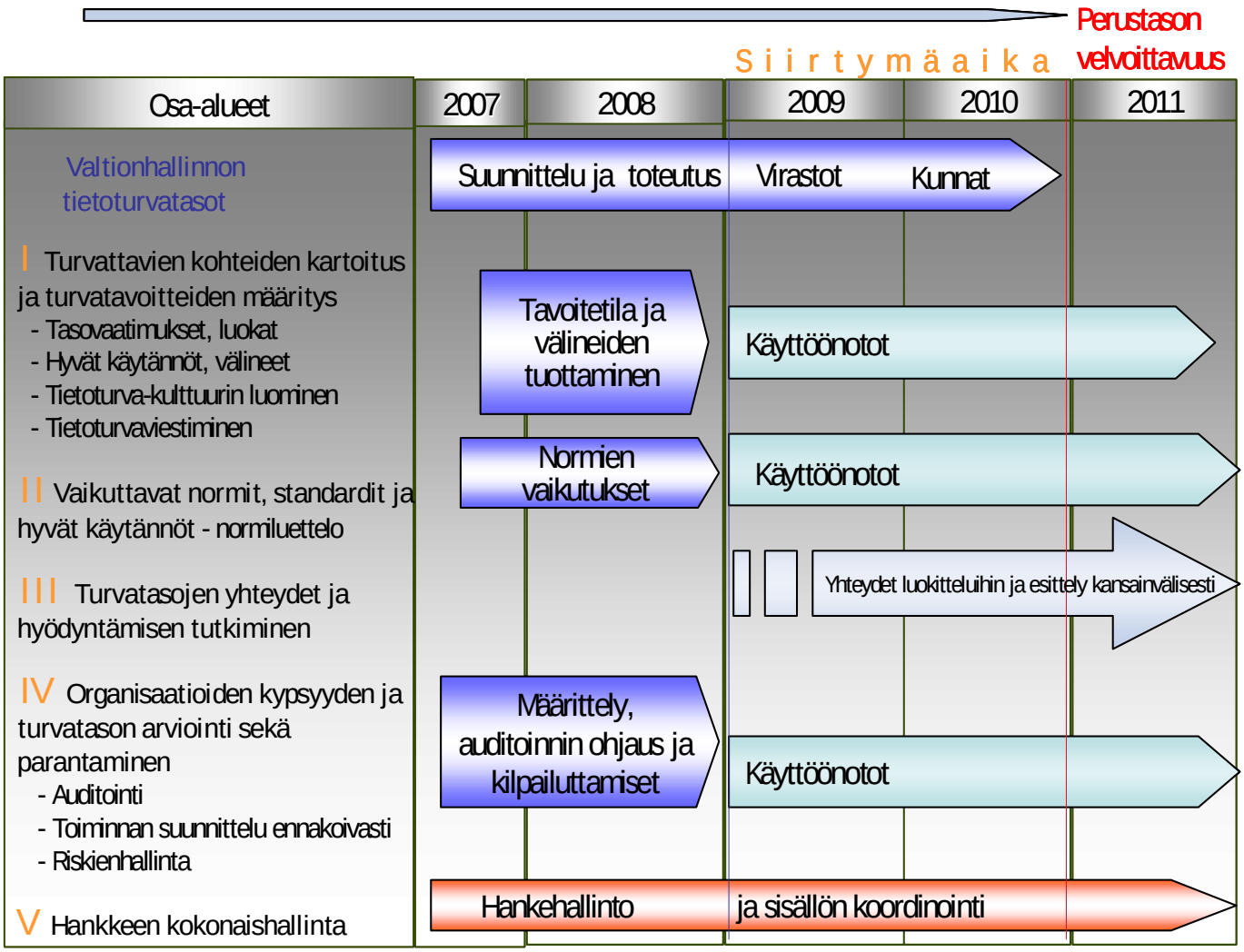
I. Turvattavien **kohteiden** kartoitus ja **turvatavoitteiden** määritys

II. Vaikuttavat **normit**, standardit ja hyvät käytännöt

III. Olemassa olevien tasojen harmonisointi ja **soveltamismahdollisuuksien** tutkiminen

IV. Organisaatioiden kypsyyden ja turvatason **arviointi** ja parantaminen

V. Jatkohankkeen kokonaisuuden **hallinnointi** ja ohjauksen toteuttaminen



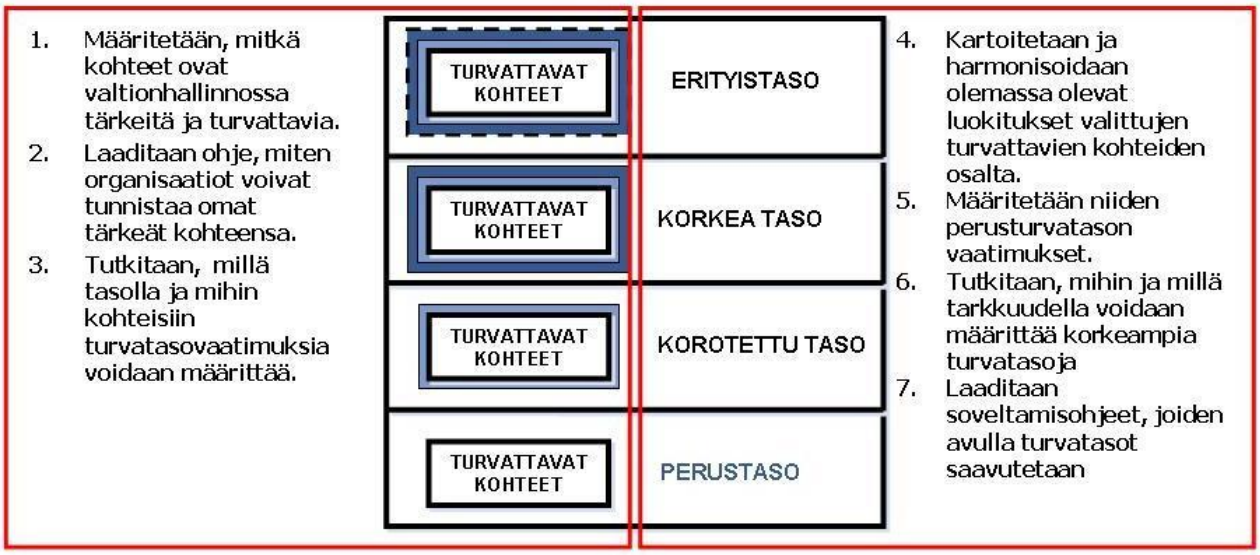
Kuva 13. Jatkohankkeen osien toteuttamisaikataulu.

Seuraavat kappaleet kuvaavat 5 jatkohankkeiden tehtäviä. Haluttuja lopputuloksia on kuvattu mm. toteuttamissuunnitelman keskimmäisessä sarakkeessa (liite 3). Henkilötyöpäivät näkyvät arvioina liitteessä 5. Välineiden toteuttaminen on kuvattu liitteessä 6. Kustannusarvio välineistä ei sisälly julkiseen raporttiin ja lausuntopyyntöön. Hallinnon asiantuntija saa sen halutessaan pyytämällä hankkeen vetäjältä (yhteystiedot liitteessä 9). Liitteessä 12 on arvioitu jatkohankkeiden 5 osa-alueen kustannuksia

Jatkohankkeen toteuttamistapoihin on jätetty liikkumavaraa, jolloin on mahdollista ottaa käyttöön uusia, myöhemminkin esiin tulevia tapoja. Suuri osa jatkohankkeiden työstä toteutetaan asiantuntijatyönä (virkatyötä ja konsultointia). Jokaiselle osa-alueelle on ehdotettu lisäksi toimintaa tehostavia välineitä ja 'kättä pidempää'.

7.1 Turvattavien kohteiden kartoitus ja turvatavoitteiden määritys

Jatkohankkeessa määritetään valtionhallinnon kannalta yhteisesti sovitut turvattavat kohteet, turvatavoitteet ja niiden tavoiteltava turvataso. Toteuttamissuunnitelman kohdassa I on kuvattu tavoitteita ja organisointiehdotuksia (liite 3).



Kuva 14. Vaiheistettuna jatkohankkeen turvattavien kohteiden ja turvatason määrittäminen.

Perustason vaatimuksista on koottu luonnos jatkotyötä varten. Alla on ehdotus sisällysluetteloksi.

Esimerkkejä perustason vaatimuksista ovat:

- Käyttöoikeudet poistettava/passivoitava poislähteneeltä.
- Jokaisella tietojärjestelmällä on oltava roolit: omistaja, pääkäyttäjä ja ylläpitäjä
- Poikkeustilanteisiin on varauduttava etukäteen, niin että riskit on tiedostettu ja organisaation ylin johto on tehnyt päätökset.

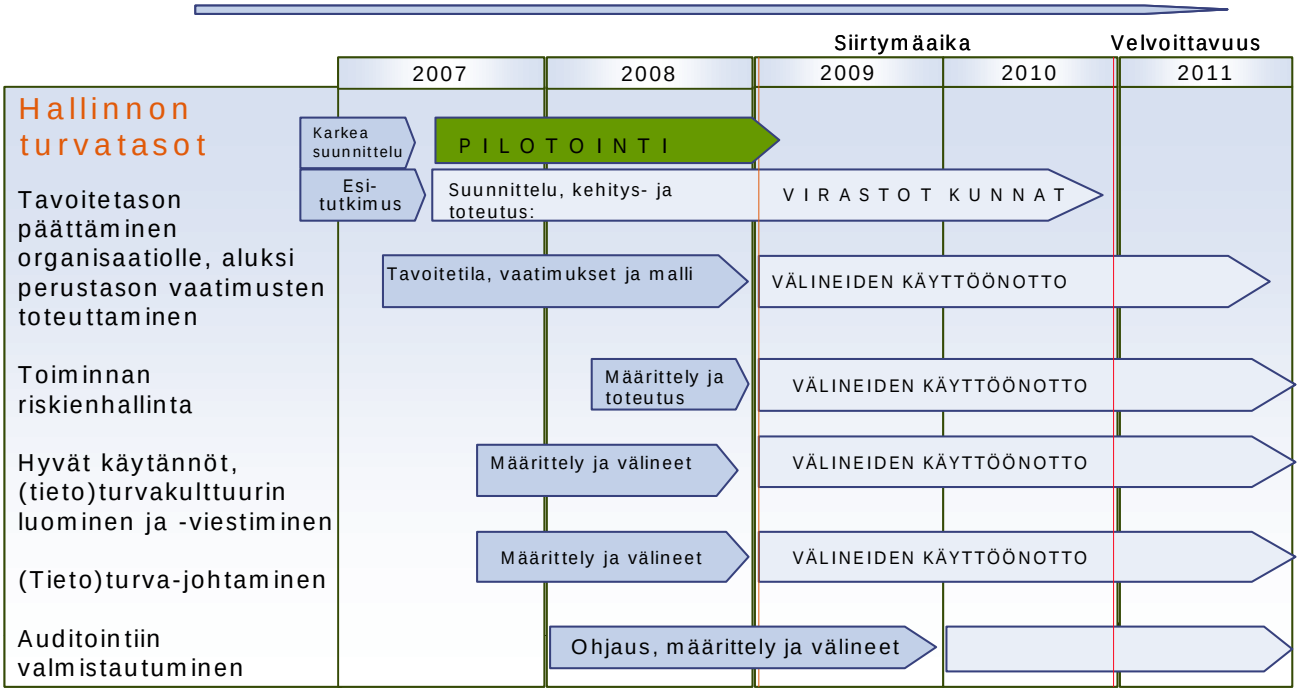
Alla on ehdotus sisällysluettelosta turvattavan kohteen arviointiin.

Kohteiden turvaaminen

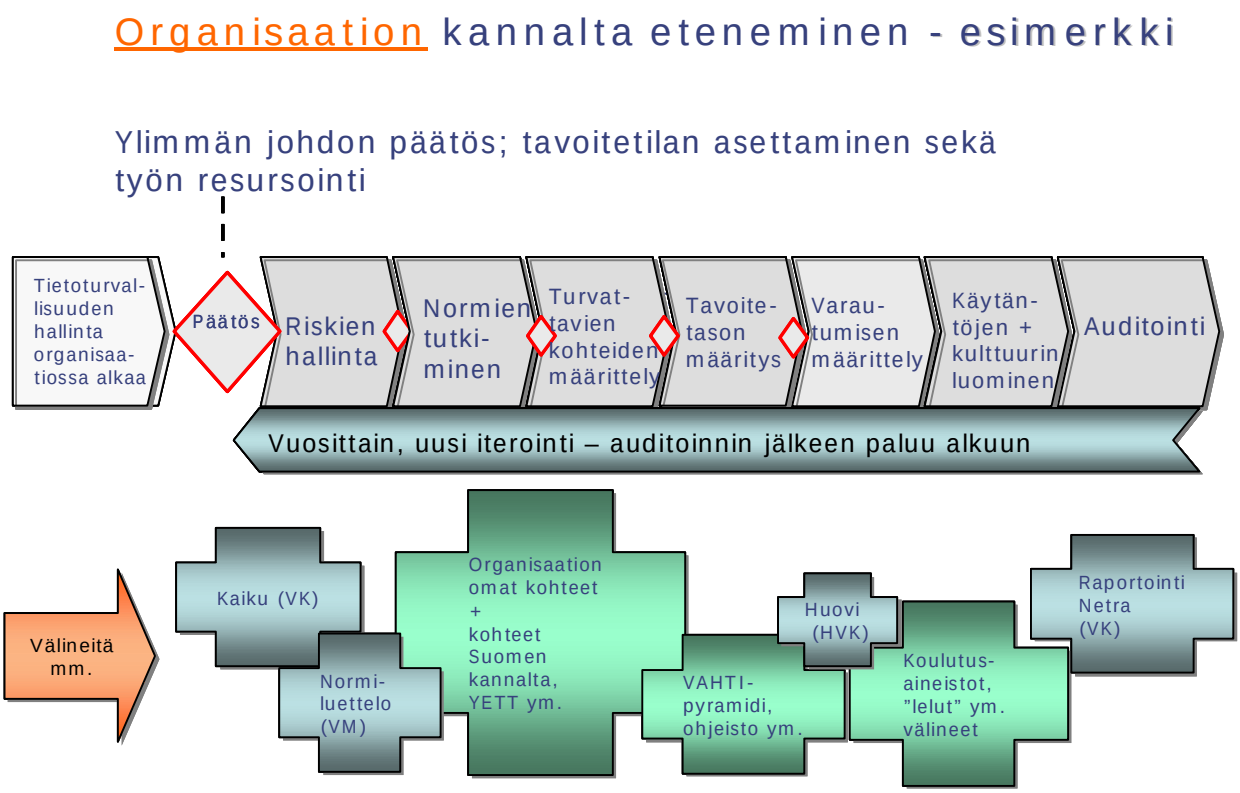
- Henkilöstö
- Tietoaineistot
- Tilat ja toimintaympäristö
- Tietojärjestelmät
- Tietoliikenne
- Laitteistot
- Ohjelmistot
- Käyttötoiminta
- Tuotettavat palvelut
- Etäkäyttö
- Tietojenkäsittelyä palvelevat prosessit:
  - 11.1 Infrastruktuurin hallinta
  - 11.2 Tietojärjestelmäprojektien hallinta
  - 11.3 Hyväksymisvaltuudet
  - 11.4 Käyttövaltuuksien hallinta
  - 11.5 Muutostenhallinta
  - 11.6 Ongelma- ja poikkeamatilanteiden hallinta
  - 11.7 Suorituskyvyn ja kapasiteetin hallinta
  - 11.8 Kohteiden tietoturvatason auditointi

7.1.1 Miten osa-alueen pilotointi toteutetaan?

Pilotointia tekevä organisaatio määrittelee oman turvattavan kohteensa turvatason ja sitoutuu antamaan vastuuhenkilön kohtuullisen määrän työpanosta. Käytännön työ vastuuhenkilöllä on hyvin pitkältä samaa, kuin hän muutenkin tekisi. Tietoturvatasot-jatkohanke antaa etenemispolun ja konkreettisia tavoitteita sekä arviointivälineet tavoi+tteiden saavuttamiseen. Organisaatio sitoutuu antamaan palautetta ja voi testata laajasti tulevia apuvälineitä. Vastineeksi organisaatio saa käyttöönsä vastikkeetta ja etukäteen hallinnolle tarjottavat välineet ja lisäksi kohtuullisesti hallinnon sisäistä konsultointia hankkeelta.



parantamiseksi organisaatiossa, joka toteuttaa tietoturvatasoja.



Kuva 15. Vaiheistettuna organisaation tietoturvallisuuden hallinnan prosessi..

Esimerkki 1. Hallinnonalalla X on useita toimipisteitä, joilla se haluaa olevan eri turvatason. Nämä toimitiloittain luokiteltavat tasot voi toteuttaa turvatasojen avulla. Kohteiden päättämisen jälkeen määritellään tavoiteltava taso ja sen jälkeen tehdään roadmap toteuttamiselle. Lisäksi hallinnonala tarjoaa sähköisiä asiointipalveluita kansalaisille ja sidosryhmille. Jokaiselle 'kruunun jalokivelleen' hallinnonalan edustajat miettivät sisäisen järjestyksen palveluille ja lisäksi tavoiteltavan turvatason. Myös tietojärjestelmät ja perusrekisterit ovat tyypillisiä turvattavia palveluita. Turvattava kohde voi olla myös henkilöstö, kriittinen alihankkija, prosessin, jne. Organisaatio asettaa tavoitetason myös omalle kyvykkyydelleen hallita palveluita ja muita turvattavia kohteita.

Pilotoinnin karkea aikataulu ja vaiheistus sekä jatkohankkeen tulevat pilottiorganisaatiot yhteyshenkilöineen on kuvattu liitteessä 11. Liite on luokiteltu viranomaisjulkiseksi.

7.2 Vaikuttavat normit, standardit ja hyvät käytännöt

Selvitetään olemassa olevat normit, standardit ja hyvät käytännöt valittujen turvattavien kohteiden, turvatasojen ja kypsyyden kannalta. Tavoitteena on koota tietoturvallisuuden ja IT-toimintojen "mitä se on "-normiselitykset käytännön kannalta.

Suunnitellaan, miten niitä voidaan hyödyntää ja yhdenmukaistaa. Lisäksi tutkitaan kuinka eri organisaatioissa voidaan hyödyntää Vahti-ohjeiden, ISO 17799:n ja muiden pohjalta jo tehtyä kehitystyötä. Ensimmäisenä osa-alueen välineenä tuotetaan keskitetysti ajantasainen ja kattava normiluettelo hallinnon käyttöön.

7.3 Olemassa olevien turvatasojen harmonisointi ja soveltamismahdollisuuksien tutkiminen

Tällä hetkellä eri turvattaviin kohteisiin liittyy erilaisia luokitteluja:

I. Tietoaineistot (luottamuksellisuuden mukaan)

II. Henkilöt (avainhenkilöiden osalta)

III. Organisaatiot

IV. Tehtävät (tarkastellaan kriittisen toiminnan kannalta, liittyvät tärkeisiin henkilöihin)

V. Järjestelmät (keskeisyyden ja kriittisyyden mukaan) [lähde: VAHTI 1/2001]

VI. jne...

Tasot eivät ole yhdenmukaisia ja niiden vertailu on vaikeaa. Sen vuoksi hankeryhmä ehdottaa, että olemassa olevat turvatasot harmonisoidaan yhteisesti sovittujen tietoturvatasojen kanssa.

Samassa yhteydessä tutkitaan, miten turvatasoja voidaan soveltaa laajemmin koskemaan muita turvallisuuden osa-alueita ja yhteiskunnan elintärkeiden toimintojen turvaamisen (YETT) strategiaa.

7.4 Organisaatioiden kypsyyden ja turvatason arviointi ja parantaminen

Jatkohankkeessa suunnitellaan

1. miten strateginen, toiminnallinen ja turvatoimenpiteiden kypsyys määritetään sekä todennetaan.
2. menettelyt, joilla parannetaan organisaatioiden kypsyyttä.
3. miten kypsyys ja turvataso toteutuvat yhteistyössä ja palveluissa

Esimerkkejä perustason vaatimuksista ovat:

- Riskien arviointi tehdään organisaatiossa vuosittain ja ylin johto on mukana
- Organisaation ’kruunun jalokivet’ on tunnistettu ja turvataan ne tietoisesti
- Organisaatiossa on nimetty (osa/kokopv.) tietoturvallisuudesta vastaava ja hänellä on aikaa sekä osaamista tehtävään.

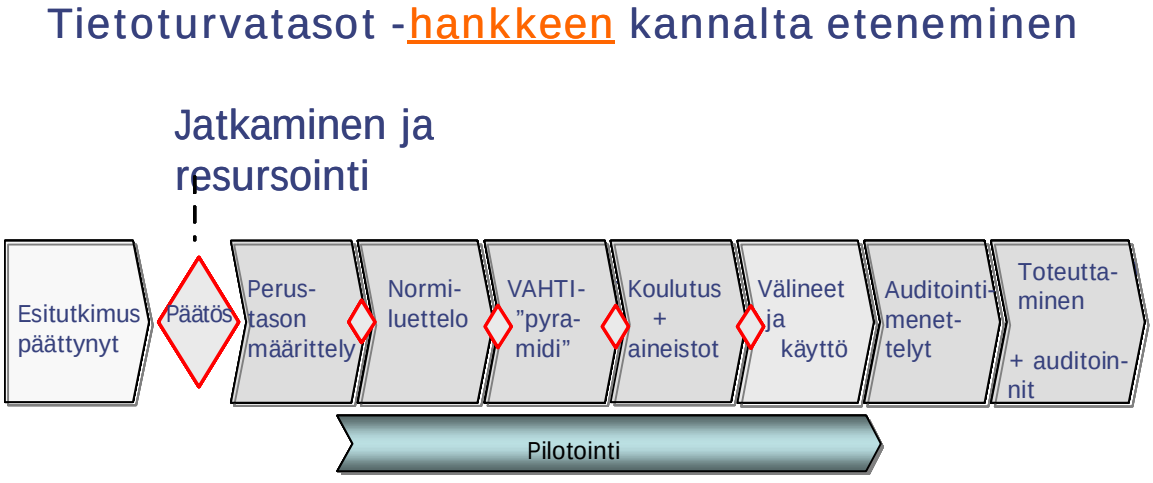
Alla on ehdotus sisällysluettelosta tietoturvallisuuden hallinnan arviointiin.

Vaiheistettua käyttöönottoa (pilotointia) on kuvattu kappaleessa 7.1.1. Karkea aikataulu ja vaiheistus sekä jatkohankkeen tulevat pilottiorganisaatiot yhteyshenkilöineen on kuvattu liitteessä 11. Liite on luokiteltu viranomaisjulkiseksi.

7.5 Tietoturvatasot –hankkeen kokonaisuuden hallinnoinnin ja ohjauksen toteuttaminen

Tietoturvatasot –hankkeen jatkaminen vaatii kokonaisuuden koordinointia ja ohjausta. Sillä varmistetaan, että hankkeen tavoitteet toteutuvat ja eri osa-alueiden tulokset tukevat toisiaan.

Jatkohankkeet toteutetaan yhdessä hallinnonalojen, virastojen ja hallinnon sidosryhmien kanssa. Tietoturvatasot tukevat hallinnon tietoturvavastaavia, meneillään olevia tietoturvahankkeita sekä VAHTIn, YETT:n, VTV:n ja VM/controllerin toimintaa.

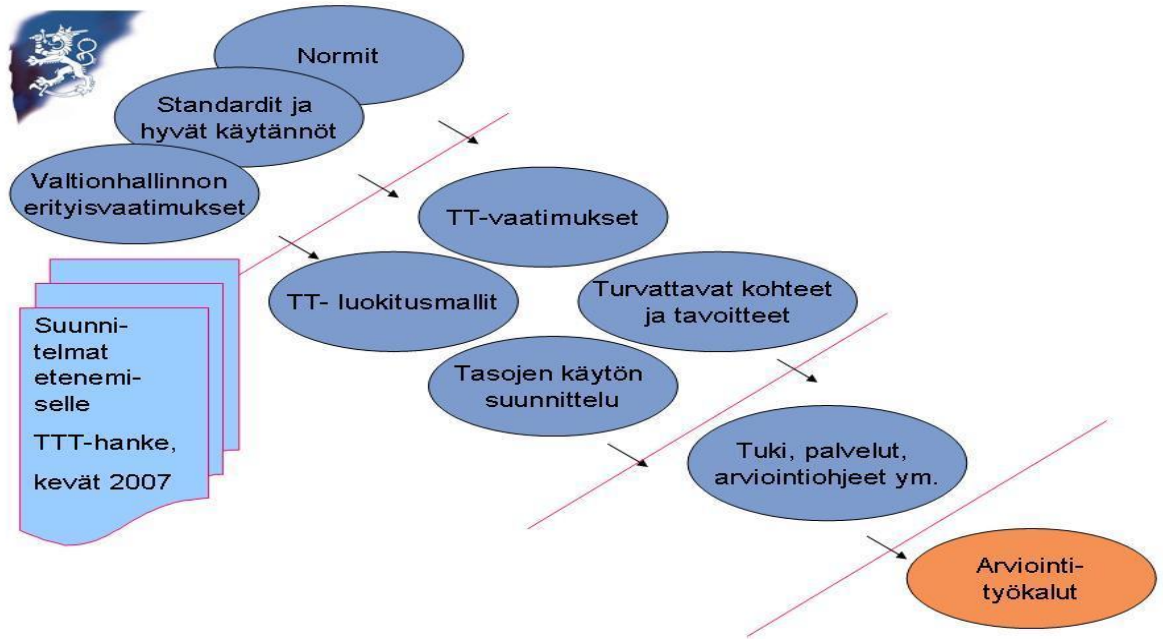


Kuva 16. Jatkohankkeiden keskinäinen prosessi tulosten saavuttamiseksi.

Jatkohankkeiden tavoitteena on nostaa organisaatioiden kypsyyttä tietoturvallisuuden hallinnassa. Vuonna 2011 kaikki hallinnon organisaatiot ovat ainakin toistettavalla ja palvelut vähintään perustasolla.

Turvattavien kohteiden turvatasoa kehitetään yhtenäisillä apuvälineillä ja tuetaan organisaatioiden tietoturvavastaavien työtä käytännössä.

Alla on kuvattu valtiovarainministeriön kannalta vaiheistettu eteneminen.



Kuva 17. Tietoturvatasot –jatkohankkeen prosessikuva ja vaiheistus.

7.6 Toteutuksen osa-alueet, kuvaus ja vastuuorganisaatiot

Tarkka toteuttamissuunnitelma on liitteessä 3. Alla oleva taulukko kuvaa päävastuun ja jatkohankkeen osa-alueiden tärkeimmät sidosryhmät.

Jatkohankkeet	Kuvaus	Vastuuorganisaatio
I Turvattavien kohteiden kartoitus ja turvatavoitteiden määritys	Määritetään valtionhallinnon kannalta yhteisesti sovitut turvattavat kohteet, turvatavoitteet ja niiden turvataso.	VM yhdessä koko hallinnon kanssa.
II Vaikuttavat normit, standardit ja hyvät käytännöt	Selvitetään olemassa olevat normit, standardit ja hyvät käytännöt valittujen turvattavien kohteiden, turvatasojen ja kypsyyden osalta. Suunnitellaan, miten niitä voidaan hyödyntää ja yhdenmukaistaa. Lisäksi tutkitaan kuinka eri organisaatioissa voidaan hyödyntää Vahti-ohjeiden, ISO 17799:n ja muiden pohjalta jo tehtyä kehitystyötä	VM yhdessä hallinnon kanssa, oleellisesti mukana tietosuojavaltuutetun toimisto ja OM.
III Olemassa olevien tasojen harmonisointi ja soveltamismahdollisuuksien tutkiminen	Olemassa olevien turvatasojen harmonisointi yhteisesti sovittujen tietoturvatasojen mukaisesti. Samassa yhteydessä tutkitaan, miten turvatasoja voidaan soveltaa laajemmin koskemaan muita turvallisuuden osa-alueita ja yhteiskunnan elintärkeitä toimintojen turvaamista (YETT).	VM yhdessä hallinnon kanssa, yhteydet Komissioon ja kansainvälisiin tietoturvallisuutta toteuttaviin sidosryhmiin.
IV Organisaatioiden kypsyyden ja turvatason arviointi ja parantaminen	Suunnitellaan miten strateginen, toiminnallinen ja turvatoimenpiteiden kypsyys määritetään sekä todennetaan. Suunnitellaan menettelyt, joilla parannetaan organisaatioiden kypsyyttä. Suunnitellaan, miten kypsyys ja turvataso toteutuvat yhteistyössä ja palveluissa	VM yhdessä hallinnon kanssa, mukana erityisesti Valtion tarkastusvirasto, VM/Controller, Valtiokonttori, auditointipooli sekä hallinnonalojen sisäiset tarkastajat.
V Tietoturvatasohankkeen kokonaishallinnan ja ohjauksen toteuttaminen	Laaditaan hankkeen koordinointisuunnitelma. Varmistetaan hankkeelle tarvittava tuki ja ohjaus. Huolehditaan siitä, että hankekokonaisuus toteuttaa sille asetetut vaatimukset.	VM.

Taulukko 1. Suunnitelma jatkohankkeen osa-alueista, tavoitteista ja vastuutahoista.

8 Usein Kysytyt Kysymykset, UKK (FAQ), mm. vaikutukset VAHTI –ohjeistoon

Tärkein kysymys, miten työtä jatketaan, ratkeaa elokuussa 2007. Silloin saadaan vastaukset lausunnoilta ja valtiovarainministeriö tekee päätökset jatkohankkeesta. Jatkohankkeen osiin on esitutkimuksen hankeryhmä ehdottaa uusien henkilöiden palkkaamista hallinnosta ja osittain konsultointina. Jos lupa jatkaa tulee, organisoinnin valmistelu alkaa syksyllä 2007. Jos kaikki jatkohankkeen osa-alueet toteutetaan, aloitetaan myös välineiden kilpailuttamisen valmistelut sekä sidosryhmien ja hallinnon sisäisen yhteistyön kokoaminen.

Termit on kuvataan jatkohankkeessa. Osittain vakiintumattomat termit saadaan päätetyksi yhdessä hallinnon kanssa. Toistaiseksi tietoturvallisuussanastona käytetään VAHTIn tietoturvasanastoa VAHTI 4/2003.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/name.jsp

Seuraavat alaotsikot kuvaavat, mitä tietoturvatasot tarkoittavat hallinnossa, tärkeiden periaatteiden tai käytäntöjen kannalta. Jos joku oleellinen asia mielestäsi puuttuu, lähettäisitkö sen hankkeen vetäjälle liitteestä 9 löytyviin yhteystietoihin, kiitos!

Usein kysytyt kysymykset (UKK, Frequently Asked Questions FAQ)

8.1 Mitä tietoturvatasot tarkoittavat.. ?

TTT tulosohjauksen kannalta

Tietoturvatasoissa organisaation tulee tunnistaa toimintansa kannalta tärkeimmät ja turvattavat kohteet, se auttaa organisaatiossa keskittämään (tieto)turvallisuuden hallintaan liittyvät toimet ja kustannukset tehokkaasti. Tulosprisman vaikutukset turvatasovaatimuksiin on tarkoitus tehdä jatkohankkeessa.

Tulostavoitteissa on järkevää kuvata organisaation julkiset tavoitteet –myös turvallisuustavoitteet. Turvatasot ovat selkeitä vaatimuksia, jotka liittyvät turvattavien kohteiden turvaamiseen. Selkeille vaatimuksille voidaan helpommin määrittää tulostavoitteet ja arvioida kustannukset sekä lyhyellä että pitkällä tähtäimellä.

TTT välisen organisaatioiden yhteistyön kannalta

Hankkeessa on määritelty tietoturvatasot ja niiden liittyminen organisaation tietoturvallisuuden hallinnan kypsyyteen. Malli auttaa tunnistamaan yhteistyön kannalta tärkeät ja turvattavat kohteet sekä määrittämään niiden turvataso. Organisaatiot saavat lisäksi tavan määrittää sekä oma, että yhteistyökumppanin tietoturvallisuuden hallinnan kypsyys. Tämä korostuu erityisesti tilanteessa, jossa turvattavia kohteita, kuten esimerkiksi tietoa, käsitellään yhteisesti.

TTT hankittavien palveluiden kannalta

Sopimusneuvotteluihin saadaan konkreettinen apuväline mm. alihankkijoilta saatavan laadun hallintaan. Kuten muussa yhteistyössä, organisaatioiden tietoturvallisuuden hallinnan kypsyys korostuu tilanteissa, jossa käsitellään yhteisesti turvattavia kohteita. Palveluiden hankinnassa turvattavia kohteita ovat erityisesti palvelut ja niiden osat. Tietoturvatasot–hankkeessa on määritetty, miten tasot liittyvät organisaatioiden kypsyyteen.

TTT tuottavuusohjelman kannalta

Hallinnon päällekkäinen työ vähenee, kun tietoturvallisuuden hallinnan avulla saavutetaan toiminnan ja tietojärjestelmien tuottavuutta toiminnan keskeytysten ja ongelmatilanteiden vähenemisen kautta. Jatkossa joitakin tietoturvapalveluita voidaan tehdä keskitetysti.

TTT strategisen työn kannalta

Tietoturvallisuuden hallinnan avulla strateginen työ helpottuu, sillä johto saa käytettäväkseen entistä luotettavampaa ja ajantasaisempaa tietoa. Tietojen luottamuksellisuus myös varmistuu entistä paremmin. Samalla henkilöstö osaa käsitellä tietoa sujuvammin.

TTT Suomen julkisuuskuvan kannalta

Hyvä hallinto ja laadukkaat palvelut tuottavat Suomelle mainetta luotettavana kumppanina. Komission tarkastukset vievät vähemmän aikaa. Auditoinnit ja tarkastukset on mahdollista tehdä tasoajattelun käsitemallien avulla, Tietoturvallisuuden hallinta lisää maiden, kansalaisten ja sidosryhmien luottamusta Suomen valtionhallinnon toimintaan.

TTT auditoijien, tarkastajien ja sisäisten tarkastajien kannalta

Auditoijat, tarkastajat ja sisäiset tarkastajat saavat uusia välineitä työhönsä.

TTT ylimmän johdon kannalta

Ylin johto varmistaa toimintansa jatkuvuuden ja hyvän julkisuuskuvan.

TTT teknisten asiantuntijoiden kannalta

Asiantuntijan suunnittelutyö helpottuu. Yhteistyö muiden toimijoiden kanssa on sujuvaa, kun tietoturvatasot määrittävät yhteiset käsitteet ja turvatason. Työn tekemisen avuksi on tarkistuslistoja. Yksittäiset toiminnot muodostavat jatkossa selviä prosesseja tietoturvallisuuden hallintaan.

TTT tietoturvavastaavien työn kannalta

Tietoturvatasot antavat kättä pidempää ja lisäävät organisaation tietoisuutta tietoturva-asioissa. Tietoturvallisuutta suunnitteleva saa avuksi hakupalvelun, joka helpottaa määräysten, ohjeiden ja suositusten löytämistä. Tietoturvatasojen ohjeistojen avulla organisaatioiden on aiempaa helpompaa noudattaa annettuja ohjeita. Tietoturvallisuustietoisuus kasvaa ja siitä tulee luonteva osa organisaatioiden päivittäistä toimintaa.

TTT poliittisen ohjauksen kannalta

Tietoturvatasot tukevat toiminnan ja talouden suunnittelua. Tietoturvallisuutta on mahdollista mitata tietoturvatasoilla ja organisaatioita kypsyystasoilla. Tulosohjauksen avuksi tietoturvallisuuden kustannuksia voi koota eri metodeilla. Tulostietojärjestelmää ja sen tilastointietoja käytetään hallinnon tietoturvallisuuden tason parantamisessa.

TTT Yhteiskunnan elintärkeiden toimintojen ja YETT-strategian kannalta

Tietoturvatasot ovat yhteensopivia kansallisten ja kansainvälisten standardien kanssa. TTT auttaa ehkäisemään tieto- ja viestintäjärjestelmiin kohdistuvia laajoja tuhoja sekä toimintahäiriöitä. Tietoturvatasot auttavat määrittämään ja suunnittelemaan yhteiskunnan kannalta kriittisten toimintojen turvamekanismit.

TTT Valtion IT-toimintojen johtamisyksikön, ValtIT:n kannalta

Tietoturvatasot –hanke käsittelee tietoturvallisuuden hallintaa ja tietoturvavaatimuksia uudella tavalla, käyttäen kuitenkin hyödyksi olemassa olevaa tietoa ja menettelyjä. Se on yhteensopiva olemassa olevien standardien ja normien kanssa. Hankkeen avulla tietoturvavaatimukset voidaan määritellä yksityiskohtaisemmin ja tarkoituksenmukaisemmin.

Tietoturvatasot ja niihin liittyvä ohjeistusten kokoaminen lisäävät valtionhallinnon sisäistä yhteistyötä. Lisääntynyt yhteistyö vähentää päällekkäistä työtä. Organisaatioiden ei tarvitse kehittää samoja menetelmiä hajautetusti, vaan turvallisuudesta vastaavat voivat keskittyä organisaatiokohtaisiin, syvällisempiin ratkaisuihin.

TTT ValtIT-kärkihankkeiden kannalta

Tietoturvallisuuden hallinta lisää asiakkaiden luottamusta palveluihin ja lisää varmistaa palveluiden käytön. Tietoturvatasot –hanke käsittelee asiakaslähtöisyyttä osana tietoturvallisuuden hallintaa. Tietoturvatasojen avulla sähköisten palveluiden turvatason määrittäminen, toteuttaminen ja arviointi helpottuu. Tietoturvatasojen avulla järjestelmäympäristöjen tarkastettavuus helpottuu ja tietoturva osataan ottaa huomioon koko järjestelmän elinkaaren ajan.

Hyvä hallintotapa sisältää myös vaatimukset tietoturvallisuudelle ja tietoturvallisuuden huomioon ottamisen. Yhteiset tietojärjestelmät vaativat yhteisiä ja yhteisesti sopivia käytäntöjä sekä toimenpiteitä. Tietoturvatasojen avulla näiden määrittäminen ja kuvaaminen helpottuu.

TTT Virkamiehen tunnistaminen –hankkeen (ValtIT) kannalta

Tietoturvatasot helpottavat sopivat turvatason määrittämistä sekä itse järjestelmäympäristössä, käyttäjäorganisaatioissa ja ylläpito-organisaatioissa. Hankkeen tulokset auttavat lisäksi varmistamaan, että tietoturvallisuustaso säilyy koko palvelun elinkaaren ajan. VirTu ja sen jatkovaihe tulee tukeutumaan Tietoturvatasojen jatkohankkeessa tehtävään työhön.

TTT pilottiorganisaatioiden kannalta

Pilottiorganisaatiot pystyvät täydentämään nykyistä tietoturvallisuuden hallintaansa. Tietoturvatasoissa mennään syvälle tietoturvallisuuden hallintaan, samalla antaen ”kättä pidempää” tietoturvallisuuden kehittämiseen. Tätä tukee erityisesti tietoturvallisuuteen

liittyvät ohjeistorakenne.

TTT Valtion tietoturvallisuuden johtoryhmän, VAHTIn kannalta

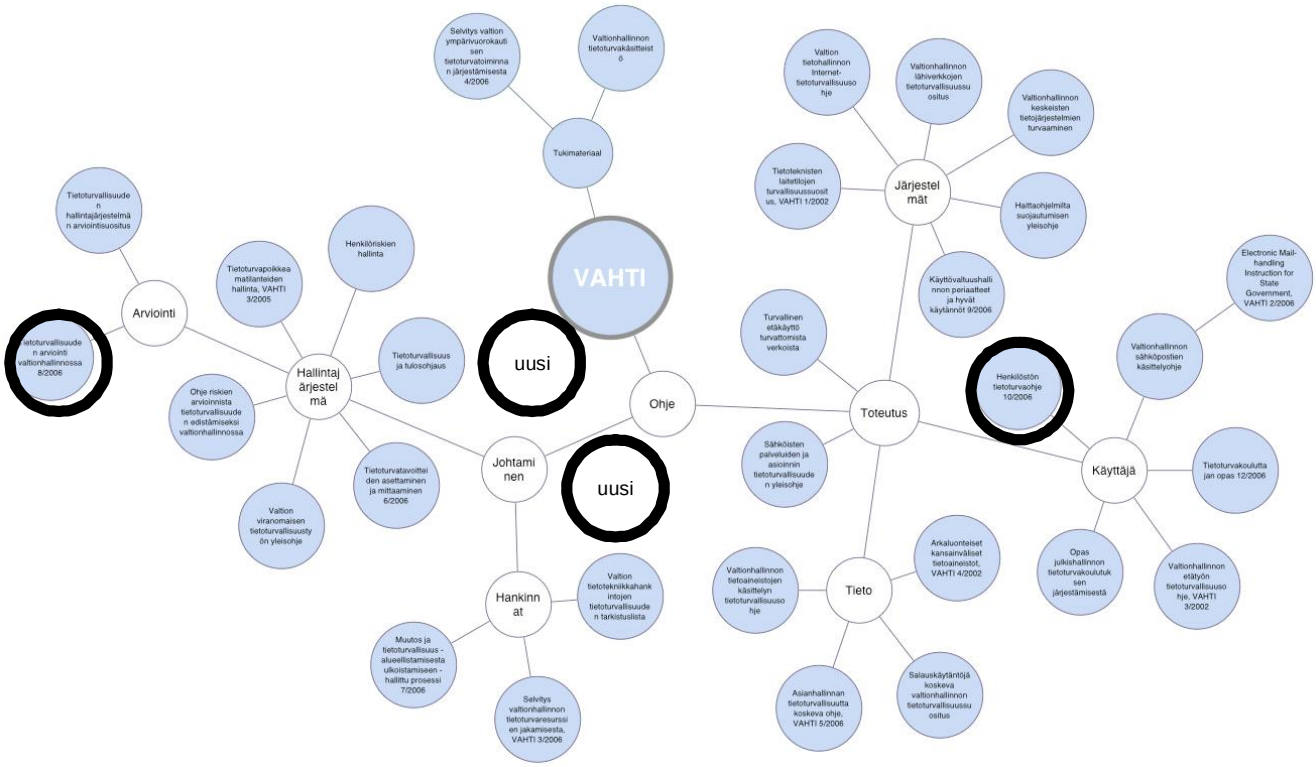
Tietoturvatasot toimii yhdessä VAHTIn kanssa valtionhallinnon tietoturvallisuuden parantamiseksi. Tietoturvatasot toteuttavat VAHTIn linjauksia sekä tuottavat apuvälineitä ja ratkaisuja hallinnon käyttöön.

8.2 Päivitystarpeet nykyiseen VAHTI-ohjeistoon

Hankkeessa sovellettiin VAHTI –ohjeistoa, eivätkä tulokset ole niihin nähden ristiriidassa. Jatkoa silmällä pitäen on kuitenkin tärkeää, että eri olemassa olevat luokat tarkastellaan ja harmonisoidaan.

VAHTI-peruskäyttäjän hallinnolle jaettavaan koulutuspakettiin on mahdollista lisätä kysymyksiä tietoturvatasoista. Tietoturvatasojen jatkohankkeessa voidaan jatkaa peruskäyttäjätyön tukemista (välineet, koulutus ym.).

Uusia VAHTI-julkaisutarpeita on todennäköisesti Tietoturvallisuuden hallintajärjestelmään ja tasojen yhdistämiseen. Lisäksi sopimusten ja alihankkijoiden hallintaan tasot tuovat uusia elementtejä, jolloin tämä voi olla oman julkaisun arvoinen.



Kuva 18. Vaikutukset nykyiseen VAHTI-ohjeistukseen -ehdotus.

VAHTI 8/2006-julkaisu on soveltamiskelpoinen yhdessä tietoturvatasojen kanssa.

Hankeryhmä ehdottaa, että tietoturvatasoista ja VAHTI 8/2006 tulee uusi laajennettu versio jatkotutkimuksen aikana.

8.2.1 Sähköiseen ohjeistuksen rakenteistaminen ja hyperlinkittäminen

VAHTI –ohjeisto sähköisessä muodossa on hankala käsitellä, sillä niiden hakutoiminto puuttuu. Sen vuoksi hankeryhmä ehdottaa, että ohjeistot rakenteistetaan esim. XML –muotoon, jolloin hakutoiminnot ja käsittely mahdollistetaan. Jatkossa laadittavat aineistot tulisi automaattisesti laatia rakenteelliseen muotoon. Tämä helpottaa mm. ohjeiden uusimista esim. lakien muuttuessa.

Ohjeistukseen tulee lisäksi sisällyttää enemmän kaavioita, taulukoita ym. nopeaa hahmotusta parantavia elementtejä. Suuren asiamäärän vuoksi on tärkeää, että ohjeiden viittaukset ovat ajan tasalla olevia verkostoja. Samoin ohjeiden numerointi kannattaa suunnitella uudelleen hankkeen yhteydessä.

8.2.2 Uusi VAHTI-tietoturvaohjeisto

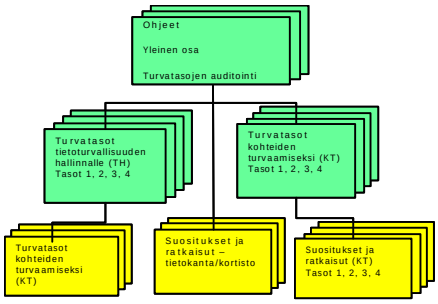
Hankeryhmä ehdottaa, että tietoturvatasoja koskeva ohjeisto jaetaan kuvan 14. mukaisella tavalla. Ohjeistojen rakenteellistamisen yhteydessä myös VAHTI –sivusto selkeytyy. Kävijän on helpompi löytää hakemaansa aineistoa. Lisäksi hankeryhmä suosittelee, että sivuilla ilmoitetaan lausunnoilla tai muussa käsittelyvaiheessa olevien luonnoksien tilanteesta.

Turvatasojen mukaiset suositukset perustuvat pääsääntöisesti olemassa oleviin VAHTI:n suosituksiin ja ohjeisiin. Yleisohjeistuksen alla ohjeet on jaettu tietoturvallisuuden hallintaa ja kohteiden turvaamista koskeviin turvatasoihin. Suositus- ja ratkaisutietokanta sekä kortisto tukevat ohjeistoa. Ratkaisuissa on mahdollista kuvata esimerkiksi tiettyjä tyyppihyväksyttyjä ja sertifioituja (tieto)turvatuotteita. Tuotteet voivat olla mitä tahansa hallinnolle suositeltavia ratkaisuja, kuten esimerkiksi hallinnon oma palvelu VETUMA (http://www.valtit.fi/).

OHJEET

SUOSITUKSET

RATKAISUT



Liitteessä 1 on esitetty luonnos tietoturvaohjeistuksen koko rakenteesta.

1 LIITE 1 Tietoturvaohjeiston rakenne, luonnos jatkotyöskentelyä varten

YLEISTÄ

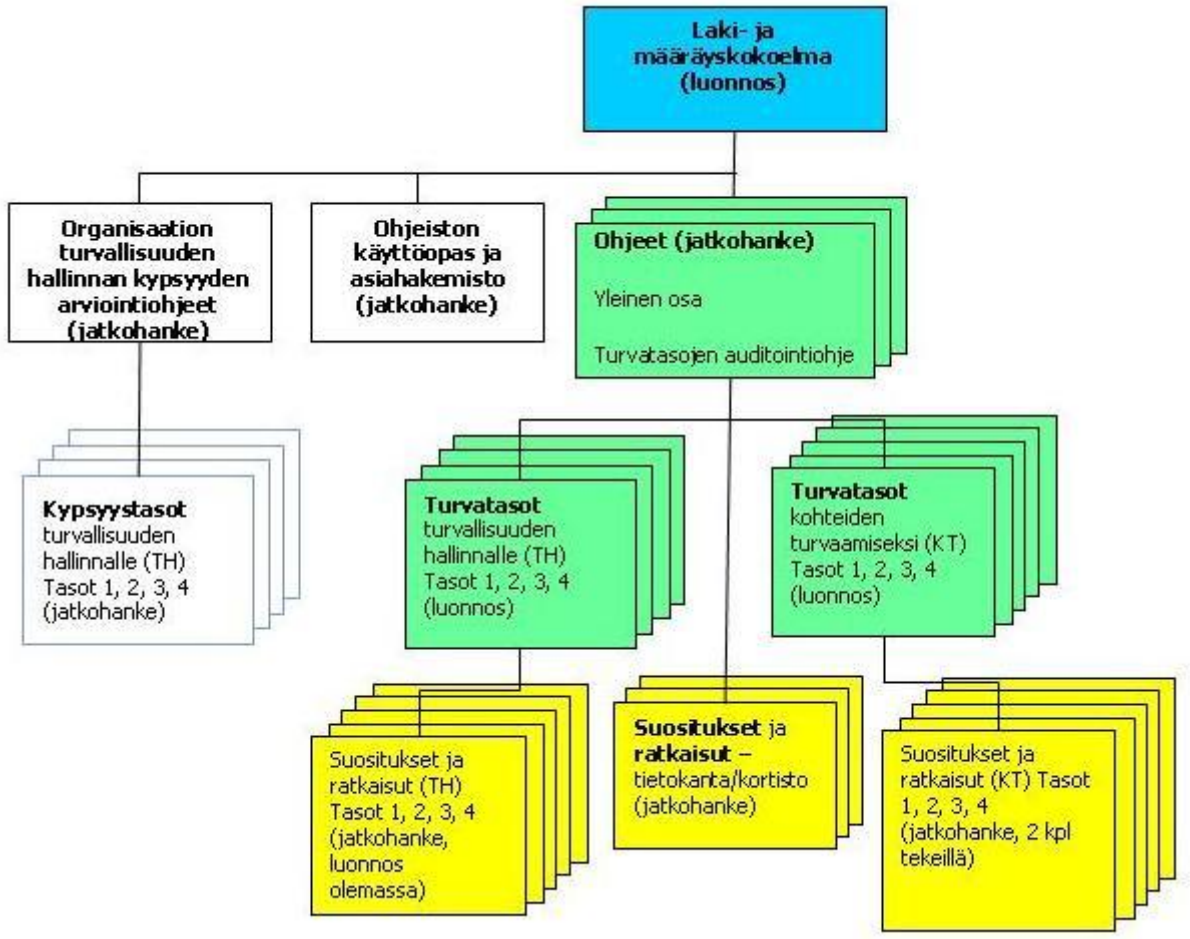
Tietoturvaohjeisto perustuu tietoturvallisuuteen liittyviin säädöksiin, normistoihin, standardeihin ja hyviin käytäntöihin. Ohjeistossa on neljä osaa:

1) **Tietoturvaohjeiston käyttöopas ja asiahakemisto**, jossa on kuvattu ohjeiston rakenne ja käyttötapasuositukset. Ohjeiston liitteenä on koko ohjeiston kattava asiahakemisto.

2) **Laki- ja määräyskokoelma**, jotka on koottu yhteen tärkeimmät, tietoturvallisuuteen liittyvät säädökset ja normit.

3) **Ohjeet**, jotka perustuvat pääsääntöisesti olemassa oleviin VAHTI-ohjeisiin. Yleisohjeistuksen alle ohjeet on jaettu tietoturvallisuuden hallintaa ja kohteiden turvaamista koskeviin turvatasoihin.

4) ”**Suositukset ja ratkaisut**” –kortisto/tietokanta, jotka perustuvat sekä VAHTI-suosituksiin, että hyviin käytäntöihin.



Kuva Liite1.1. Ohjeiston rakenne, luonnos jatkotyön pohjaksi.

TIETOTURVAOHJEISTON KÄYTTÖOPAS JA ASIAHAKEMISTO

Tietoturvaohjeiston käyttöoppaassa on kuvatta ohjeiston rakenne ja käyttötapa. Ohjeiston liitteenä on koko ohjeiston kattava asiahakemisto.

LAKI- JA MÄÄRÄYSKOKOELMA

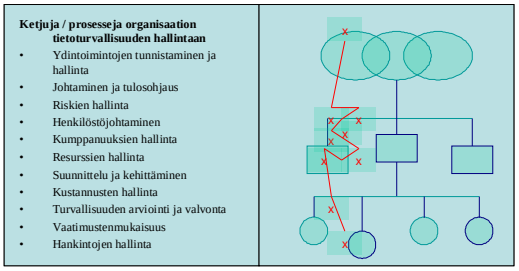
Laki- ja määräyskokoelmassa on koottu tietoturvallisuuteen liittyvät, ajantasaiset säädökset ja normit. Kokoelmaa päivitetään säännöllisesti.

OHJEET

Ohjeet perustuvat pääsääntöisesti olemassa oleviin VAHTI-ohjeisiin. Yleisohjeistuksen alle ohjeet on jaettu tietoturvallisuuden hallintaa ja kohteiden turvaamista koskeviin turvatasoihin.

TIETOTURVALLISUUDEN HALLINNAN TURVATASOVAATIMUSTEN SISÄLTÖ KULLEKIN TURVATASOLLE:

1. Ydintoimintojen tunnistaminen ja hallinta
2. Johtaminen ja tulosohjaus
3. Riskien hallinta
4. Henkilöstöjohtaminen
5. Kumppanuuksien hallinta
6. Resurssien hallinta
7. Suunnittelu ja kehittäminen
8. Kustannusten hallinta
9. Turvallisuuden arviointi ja valvonta
10. Vaatimustenmukaisuus
11. Hankintojen hallinta



ESIMERKKEJÄ VÄHIMMÄISVAATIMUKSISTA OVAT:

- Riskien arviointi tehdään organisaatiossa vuosittain ja ylin johto on mukana
- Organisaation ’kruunun jalokivet’ on tunnistettu ja turvataan ne tietoisesti
- Organisaatiossa on nimetty (osa/kokopv.) tietoturvallisuudesta vastaava ja hänellä on aikaa sekä osaamista tehtävään.
- ...

KOHTEIDEN TURVAAMISEN VAATIMUSTEN SISÄLTÖ KULLEKIN TURVATASOLLE:

1. Henkilöstö
2. Tietoaineistot
3. Tilat ja toimintaympäristö
4. Tietojärjestelmät
5. Tietoliikenne
6. Laitteistot
7. Ohjelmistot
8. Käyttötoiminta
9. Tuotettavat palvelut
10. Etäkäyttö
11. Tietojenkäsittelyä palvelevat prosessit
    - 11.1 Infrastruktuurin hallinta
    - 11.2 Tietojärjestelmäprojektien hallinta
    - 11.3 Hyväksymisvaltuudet
    - 11.4 Käyttövaltuuksien hallinta
    - 11.5 Muutostenhallinta
    - 11.6 Ongelma- ja poikkeamatilanteiden hallinta
    - 11.7 Suorituskyvyn ja kapasiteetin hallinta
    - 11.8 Kohteiden tietoturvatason auditointi

ESIMERKKEJÄ VÄHIMMÄISVAATIMUKSISTA OVAT (ESIMERKIKSI SÄHKÖINEN ASIOINTIPALVELU) :

- Käyttöoikeudet on poistettava/passivoitava poislähteneeltä.
- Jokaisella tietojärjestelmällä on oltava roolit: omistaja, pääkäyttäjä ja ylläpitäjä
- Poikkeustilanteisiin on varauduttava etukäteen, niin että riskit on tiedostettu ja organisaation ylin johto on tehnyt päätökset.
- ...

Ohjeet eivät ole velvoittavia, vaan muitakin kuin niissä esitettyjä ratkaisuja voidaan käyttää, jos ne täyttävät tietoturvallisuudelle asetetut vaatimukset. **Turvatasot ovat valittuihin kohteisiin kohdistuvia luokiteltuja ja skaalattuja vaatimuksia.**

Esimerkki. Turvattavan kohteen, esimerkiksi toimipisteen rakenteet, voi nähdä suojattavina kohteina. Samoin tietojärjestelmän tai palvelun osat on mahdollista määritellä turvaamistarpeen mukaan. Tällöin suojellaan järjestelmän tai palvelujen käyttäjiä, kuten kansalaisia ja sidosryhmiä.

SUOSITUKSET JA RATKAISUT

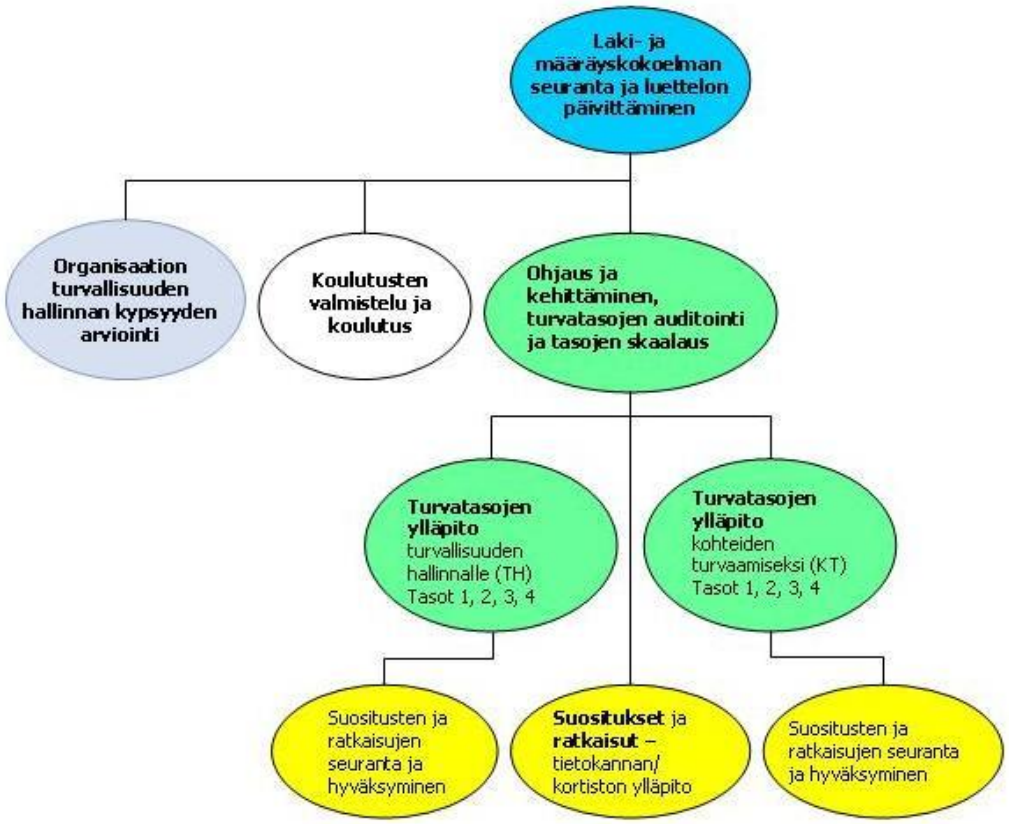
Ohjeita tukemaan muodostetaan suositus- ja ratkaisutietokanta sekä kortisto. Aineisto perustuu VAHTI –suosituksiin sekä hyviin käytäntöihin. Ratkaisuissa on mahdollista kuvata esim. tiettyjä, tyyppihyväksyttyjä ja sertifioituja tietoturvatuotteita. Tuotteet voivat olla palveluita, ratkaisuja, tuotteita tai mitä tahansa hyväksyjätaho ottaa 'keltaisiin kortteihin'.

Tällä hetkellä joitakin ehdotettuja osa-alueita puuttuu VAHTI-ohjeistosta. Näiden pimeiden kulmien (vanhentuneiden, puuttuvien tai keskeneräisten suositusten) huomioonottaminen ja työstäminen helpottuu kuvien Liite 1.1 ja Liite 1.2 pyramidien avulla.

OHJEISTON YLLÄPITO

Tietoturvaohjeistoa tulee ylläpitää säännöllisesti ja systemaattisesti.

Ylläpitäjän on järkevintä olla yleisesti ja yhteisesti hyväksytty, asiantunteva hallinnon organisaatio tai yhteistyöelin. Valtionhallinnon tietoturvallisuuden johtoryhmän, VAHTIn nykyistä hanketyötä on mahdollista muokata tietoturvatasojen työtä tukevaksi tai jopa pysyvän ylläpitäjän rooliin.



Kuva Liite 1.2. Turvaohjeistoa tukeva toiminta, kuvaus ohjeistoa tukevista toiminnoista, prosesseista ja tarvittavista osa-alueista jatkohankkeen toteuttamisessa. Rakenne ja nimitykset ovat ehdotuksia jatkotyölle.

KORTISTOJEN NIMEÄMINEN

Kortistoihin luodaan nimeämiskäytäntö. Lyhenteiden käyttäminen helpottaa nimeämistä, indeksointia, auditointeja sekä hakuja.

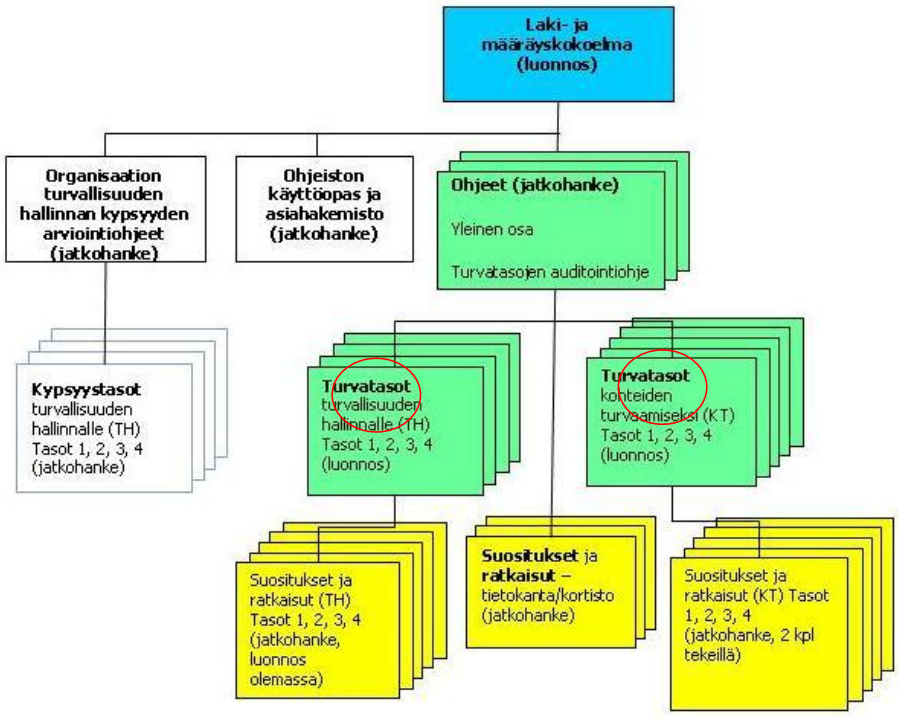
Kansainväliset standardit ja hyvät käytännöt on mahdollista mäpätä soveltuviin osiin. Organisaatiot, joilla on esimerkiksi tietoturvallisuus- tai laatusertifikaatti löytävät kuutioista ja ohjeistuksista standardin sisällysluettelo. Organisaatiot, jotka tähtäävät sertifikaatin mukaiseen toimintaan saavat soveltamis/toteuttamissuunnitelmassaan samalla huomioitua tietoturvatasot ja -vaatimukset.

Esimerkki 2.

Tietoturvatasoja koskevia, tietoturvallisuuden **hallintaa** koskevista ohjeista käytetään lyhennettä **TH**. Kortit olisivat tällöin TH1, TH2, ..

Kohteiden turvaamista koskevia kortteja kutsutaan lyhenteellä **KT.** Kortit olisivat tällöin KT1, KT2, ..

Hallinnon sisällä organisaatiot voivat jopa kuvata toimintaansa tietyn kortin mukaiseksi.



Kuva Liite 1.3 Ehdotus nimeämiskäytännöksi ja lyhenteiksi TH ja KT.

KORTISTON LÄHTEET TIETOTURVALLISUUDEN HALLINTAOSALLE, TH (pohja jatkotyölle)

Kortti/korttisarja TH 1 **Ydintoimintojen tunnistaminen ja hallinta**

* Lähdeaineisto: Alue 6 CAF, DS7 COBIT, ISO 27001 A.10, OECD Awareness, OECD Response, OECD Risk assessment, OECD Security design and implementation, ITIL, ISO 20000, BS 15000, ITSMF, VAHTI 4/2001, VAHTI 5/2004, VAHTI 8/2004

Kortti/korttisarja TH 2 **Johtaminen ja tulosohjaus**

* Lähdeaineisto: Alue 1 CAF, PO6 COBIT, ISO 27001 A.5, OECD Awareness, OECD Responsibility, OECD Security management, VAHTI 5/2004, VAHTI 6/2006, VAHTI 7/2006

Kortti/korttisarja TH 3 **Riskien hallinta**

* Lähdeaineisto: DS8 COBIT, DS4 COBIT, PO9 COBIT, ISO 27001 A.10, ISO 27001 A.13, ISO 27001 A.13, OECD Awareness, OECD Risk assessment, OECD Security design and implementation, NIST SP800-30, FEMA, ISO 13335, OCTAVE, AS/NZ 4360, BS 7799-3, PAS 56, Good Practice Guide for BCP, VAHTI 7/2003, VAHTI 5/2004, VAHTI 3/2005, VAHTI 6/2006

Kortti/korttisarja TH 4 **Henkilöstöjohtaminen**

* Lähdeaineisto: Alue 3 CAF, PO7, DS7 COBIT, ISO 27001 A.8, OECD Awareness, VAHTI 3/2002, VAHTI 5/2004, VAHTI 6/2006, VAHTI 11/2006

Kortti/korttisarja TH 5 **Kumppanuuksien hallinta**

* Lähdeaineisto: Alue 4 CAF, PO4 COBIT, AI5 COBIT, DS 2 COBIT, ISO 27001 A.6, ISO 27001 A.8, OECD Awareness, OECD Response, VAHTI 7/2006

Kortti/korttisarja TH 6 **Resurssien hallinta**

* Lähdeaineisto: Alue 4 CAF, PO1 COBIT, PO2 COBIT, PO3 COBIT, PO4 COBIT, ME 1 COBIT, ME 4 COBIT, PO6 COBIT, AI3 COBIT, AI5 COBIT, DS 2 COBIT, ISO 27001 A.6, ISO 27001 A.8, ISO 27001 A.10, OECD Awareness, OECD Response, OECD Security design and implementation, VAHTI 6/2006, VAHTI 7/2006

Kortti/korttisarja TH 7 **Suunnittelu ja kehittäminen**

* Lähdeaineisto: Alue 5 CAF, PO4 COBIT, AI5 COBIT. ISO 27001 A.6, ISO 27001 A.7, ISO 27001 A.10, OECD Awareness, OECD Response, OECD Security design and implementation, OECD Security management, VAHTI 5/2004, VAHTI 6/2006, VAHTI 7/2006

Kortti/korttisarja TH 9 **Tietoturvallisuuden arviointi ja valvonta**

* Lähdeaineisto: ME2 COBIT, ISO 27001 A.13, ISO 27001 A.14, OECD Awareness, OECD Risk assessment, OECD Reassessment, VAHTI 3/2003, VAHTI 5/2004, VAHTI 8/2004, VAHTI 6/2006, VAHTI 8/2006

Kortti/korttisarja TH 10 **Vaatimustenmukaisuus**

* Lähdeaineisto: ME2 COBIT, ISO 27001 A.15, OECD Awareness, OECD Risk assessment, VAHTI 8/2006

Kortti/korttisarja TH 11 **Hankintojen hallinta**

* Lähdeaineisto: PO5 COBIT, DS1 COBIT, DS2 COBIT, DS 6, PO10 COBIT, DS1 COBIT, ISO 27001 A.9.2, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, OECD Response, OECD Risk assessment, OECD Security design and implementation, VAHTI 2/1999, 2/2001

KORTISTON LÄHTEET KOHTEIDEN TURVAAMINEN –OSALLE, KT (pohja jatkotyölle)

Kortti/korttisarja KT 1 **Henkilöstö**

*Lähdeaineisto: DS7 COBIT, ISO 27001 A.8, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, OECD Response, VAHTI 3/2002, VAHTI 11/2006, VAHTI 5/2004

Kortti/korttisarja KT 2 **Tietoaineistot**

* Lähdeaineisto: DS11 COBIT, ISO 27001 7.2, ISO 27001 A.11, ISO 27001 A.15, VAHTI 4/2001, VAHTI 5/2004

Kortti/korttisarja KT 3 **Tilat ja toimintaympäristö**

* Lähdeaineisto: DS12 COBIT, ISO 27001 A.9, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, BS EN 1047, VAHTI 1/2002

Kortti/korttisarja KT 4 **Tietojärjestelmät**

* Lähdeaineisto: DS5 COBIT, ISO 27001 A.9.2, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.12, ISO 27001 A.15, OECD Awareness, OECD Security design and implementation, VAHTI 4/2001, VAHTI 6/2001, VAHTI 5/2004, VAHTI 5/2006, VAHTI 9/2006, VAHTI 12/2006

Kortti/korttisarja KT 5 **Tietoliikenne**

* Lähdeaineisto: ISO 27001 A.9.2, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, VAHTI 1/2003, VAHTI 5/2004

Kortti/korttisarja KT 6 **Laitteistot**

* Lähdeaineisto: ISO 27001 A.9.2, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, VAHTI 5/2004

Kortti/korttisarja KT 7 **Ohjelmistot**

* Lähdeaineisto: AI2 Acquire and Maintain Application Software, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, SSE CMM, VAHTI 3/2004, VAHTI 5/2004, VAHTI 12/2006,

Kortti/korttisarja KT 8 **Käyttötoiminta**

* Lähdeaineisto: DS13 COBIT, AI4 COBIT, ISO 27001 A.9.2, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, OECD Response, OECD Risk assessment, VAHTI 5/2004, VAHTI 3/2005, VAHTI 12/2006

Kortti/korttisarja KT 9 **Tuotettavat palvelut**

* Lähdeaineisto: DS 1, DS2, DS3, DS4, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS13 COBIT, ME 3 COBIT, ISO 27001 A.9.2. , ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, OECD Response, OECD Risk assessment, OECD Security design and implementation, VAHTI 4/2001, VAHTI 8/2004

Kortti KT 10 **Etäkäyttö**

* Lähdeaineisto: DS13 COBIT, AI4 COBIT, ISO 27001 A.9.2, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, OECD Response, OECD Risk assessment, VAHTI 5/2004, VAHTI 3/2005, VAHTI 9/2006, VAHTI 12/2006

Kortti/korttisarja KT 11 **Tietojenkäsittelyä palvelevat prosessit**

KT 11.1 Infrastruktuurin hallinta

* Lähdeaineisto: AI1 COBIT, AI 13, COBIT, AI7 COBIT, PO4 COBIT, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, OECD Security design and implementation, VAHTI 1/2003, VAHTI 3/2004, VAHTI 5/2004, VAHTI 7/2006

KT 11.2 Tietojärjestelmäprojektien hallinta

* Lähdeaineisto: PO10 COBIT, ISO 27001 A.9.2, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.12, ISO 27001 A.15, OECD Awareness, OECD Response, OECD Risk assessment, OECD Security design and implementation, VAHTI 3/2000

KT 11.3 Hyväksymisvaltuudet

* Lähdeaineisto: PO6 COBIT, ISO 27001 A.10,ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, VAHTI 1/2001, Työjärjestys, ohjesääntö

KT 11.4. Käyttövaltuuksien hallinta

* Lähdeaineisto: PO6 COBIT, ISO 27001 A.10,ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, VAHTI 1/2001, VAHTI 9/2006

KT 11.5 Muutostenhallinta

* Lähdeaineisto: DS9 COBIT, AI6 COBIT, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness, VAHTI 5/2004

KT 11.6 Ongelmien ja poikkeamatilanteiden hallinta

* Lähdeaineisto: DS4 COBIT, DS10 COBIT, DS8 COBIT, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.13, ISO 27001 A.14, ISO 27001 A.15, OECD Awareness, OECD Response, OECD Risk assessment, ISO 18044, VAHTI 7/2003, VAHTI 5/2004, VAHTI 3/2005

KT 11.7 Suorituskyvyn ja kapasiteetin hallinta

* Lähdeaineisto: ME1 COBIT, DS 3, ISO 27001 A.10, ISO 27001 A.11, ISO 27001 A.15, OECD Awareness), VAHTI 5/2004

KT 11.8 Kohteiden tietoturvatason auditointi

* Lähdeaineisto: ME2 COBIT, ISO 27001 A.11, ISO 27001 A.13, ISO 27001 A.14, ISO 27001 A.15, OECD Awareness, OECD Reassessment, VAHTI 3/2003, VAHTI 5/2004, VAHTI 8/2004, VAHTI 8/2006

2 LIITE 2 Esimerkki kypsyyden arviointimallista

Alla oleva taulukko on kartta ja yhteismitallisen arvioinnin apuväline organisaation tai sen yksikön kypsyyden arviointiin. Taulukko on yhteensopiva minkä tahansa standardin kanssa se toimii pohjana jatkohankkeen määrittelyille.

Pystysarakkeet kuvaavat vaatimukset kypsyyden eri tasoille 0, 1, .. , 5. Tasoluokittelut ovat yhteensopivia COBITin ja Capability Maturity Modelin, CMM:n kanssa. Hyväksytty taso Suomessa toimivalle valtionhallinnon organisaatiolle on taso2, perustaso.

Taulukon vasen sarake jakaa tietoturvallisuusvaatimukset *kriteerityyppeihin (6 kpl).*

TASOT ->	0	1 Toimintaa aloittavan yksikön ALOITUSTASO work &work	2 TOISTETTAVA PROSESSI - PERUSTASO plan the work	3 MÄÄRITELTY PROSESSI work the plan	4 HALLITTU, LAADUKAS PROSESSI measure the work	5 OPTIMOIVA, KEHITTYVÄ TASO work the measure
Kriteerityyppi	Ei voida soveltaa osa-aluetta	Epäorganisoitu, ennustamaton, kertaluonteinen ja sattumanvarai-nen.	Suunniteltua, toistettavissa ja seurattavissa, tietyt menettelytavat ovat jo olemassa.	Hyvin määritelty, koordinoitu, tiedotettu ja dokumentoitu.	Laadukas, ennakoitu, mitattu ja valvottu.	Jatkuvasti kehittyvä, virheistä oppiva, tehokas ja optimoitu.
Dokumentti, asiakirja	Ei vaatimuksia	Ennakoimaton taso, laatu riippuu täysin tekijästä.	Dokumentit on kerätty tiettyyn paikkaan ja tiedetään, mihin ne liittyvät ja kuka niiden ylläpidosta vastaa. Lait, sopimukset, määräykset ja systeemityö on huomioitu.	Kaikki työntekijät koulutetaan tietämään dokumentti. Noudattamisohje, standardi tai tehtävänkuvaus on olemassa	Dokumentti laaditaan tiettyjen menettelytapojen tai prosessien avulla ja sitä sovelletaan käytännössä. Dokumentti on testattu ja siitä on tarvittaessa tehty riskianalyysi.	Dokumentti käydään säännöllisin määräajoin esim. vuosittain läpi, etsitään virheitä ja ehkäistään niitä.Uudet tekniikat ym. muutokset otetaan huomioon parantamisvaiheessa.
Toimenpide, menettelytapa	Ei vaatimuksia	Kukin tekee parhaaksi katsomallaan tavalla.	Toimenpiteet suunnitellaan, dokumentoidaan ja aikataulutetaan etukäteen esim. projektien suunnittelu ja hallinta, mutta on hallinnollisia puutteita.	Toimenpiteille on olemassa tietyt vaiheet esim. suunnittelu-määrittely-toteutus-testaus-seuranta. Toimenpiteillä on oma vastuuhenkilönsä.	Käytössä on jokin systemaattinen malli esim. laadunhallinta. Toimenpiteitä ja asiakkaiden tarpeita mitataan ja seurataan. Tuloksia käytetään apuna kehitystyössä.	Prosesseja kehitetään säännöllisesti, tavoitteita asetetaan ja suorituskykyä parannetaan esim. riskien arviointi ja haavoittuvuusanalyy-sit (voi olla jo tasolla 4).

TASOT ->	0	1 Toimintaa aloittavan yksikön ALOITUSTASO work&work	2 TOISTETTAVA PROSESSI - PERUSTASO plan the work	3 MÄÄRITELTY PROSESSI work the plan	4 HALLITTU, LAADUKAS PROSESSI measure the work	5 OPTIMOIVA, KEHITTYVÄ TASO work the measure
Määräys, ohje	Ei vaatimuksia	Jotain määräyksiä saattaa kuulua toimialaan, kukaan ei varmuudella tiedä.	Tunnistetaan lait, määräykset, sopimukset ym. ohjeet, joita on noudatettava. Hallitaan vaatimukset jotenkuten.	Määräysten seuraaminen ja noudattaminen on vastuutettu. Määräyskirjastoa tms. ylläpidetään ja päivitetään.	Määräyksiä käydään läpi projekteissa tai järjestelmän vaiheissa ja vaatimusten soveltuvuutta arvioidaan Virheet dokumentoidaan ja raportoidaan.	Aktiivinen mukanaolo määräysten tai ohjeiden valmistelussa. Olemassa olevia ohjeita parannetaan säännöllisesti.
Koulutus	Ei vaatimuksia	Koulutuksia järjestetään satunnaisesti.	Koulutussuunnitelma on olemassa.	Koulutusmalli on valittu ja koulutusvastuut on jaettu. Koulutuksia seurataan ja kirjataan muistiin.	Tulokset, koulutettavien mielipiteet ja laadunarvioinnit kerätään ja niiden perusteella arvioidaan sekä suunnitellaan uusia koulutuksia.	Suunnitelmat läpikäydään säännöllisesti ja parannetaan. Mukana voi olla erillinen asiantuntija tai organisaatio.
Kokoonpano, työryhmä	Ei vaatimuksia	Ei ole olemassa virallisesti.	Kokoonpanolla on työsuunnitelma ja sitä noudatetaan.	Kokoonpanon vastuut, rajapinnat ja tehtävät on jaettu.	Kokoonpanon suorituksia seurataan, toimenpiteitä kehitetään ja annetaan palautetta.	Kokoonpanon toimia ja ideoita arvioidaan säännöllisesti tai mietitään uusien toimialojen ja/tai jäsenien ottamista.
Tarkastus, arviointi	Ei vaatimuksia	Tarkastajat eivät ole objektiivisia ja tarkastus-menetelmät ovat satunnaisia.	Tarkastuksella on aikataulut sekä työsuunnitelma ja niitä seurataan. Tarkastuksen tavoitteet ovat olemassa.	Tarkastusmenetelmät ovat systemaattisia. Tarkastusvastuut on jaettu, tarkastusta tehdään useassa vaiheessa (esim. projekti).	Tarkastuksen tulokset ovat mitattavia ja tarkastuksella on laatutavoitteet. Tarkastus-/arviointituloksia seurataan säännöllisesti.	Tarkastusmenetelmiä kehitetään ja alan kehitystä seurataan. Tarkastuksen tehokkuutta ja menetelmiä arvioidaan.

3 LIITE 3, Toteuttamissuunnitelma, osat I-V

I Turvattavien kohteiden kartoitus ja turvatavoitteiden määritys	
Kuvaus	Lopputulos
A. Määritetään ja kuvataan, mitkä kohteet ovat valtionhallinnossa tärkeitä ja turvattavia a. Yhteiskunnan kannalta 10 tärkeintä, turvattavaa kohdetta b. Organisaatioiden kannalta 10 kaikille yhteistä tärkeintä ja turvattavaa kohdetta Päätetään valittujen turvattavien kohteiden turvaamistavoitteet. Päätös ohjaa etenemistä.	Suunnitelma, jossa on kuvattu perusteltu ehdotus yhteiskunnan kannalta 10 tärkeimmästä ja organisaatioiden kannalta 10 yhteisestä tärkeimmästä kohteesta. Suunnitelma, jossa on ehdotettu tärkeistä kohteista valittavat turvattavat kohteet ja niiden turvaamistavoitteet. Päätös turvattavista kohteista ja niiden turvatavoitteista. Turvasuositukset ja ratkaisut (”keltaiset kortit”), jotka tehdään yhteistyössä ratkaisuja tuottavien organisaatioiden kanssa. Hallinnon ulkopuolisille toimijoille näiden hyväksyttyihin ratkaisuihin mukaan pääsyyn sisältyy vuosimaksu. Huom. YETT:n liite 3 ministeriöiden strategiset tehtävät (Valtioneuvosto + toimivaltainen ministeriö)
B. Määritetään turvatasovaatimukset, joilla päätetyt turvatavoitteet saavutetaan. Laaditaan soveltamisohjeet, joiden avulla turvatasovaatimukset toteutetaan.	Ohje turvatasovaatimuksista (10 +10 valitun kohteen osalta) Soveltamisohje turvatasojen saavuttamiseksi. Ohje tärkeiden ja turvattavien kohteiden tunnistamisesta sekä määrittämisestä Suunnitelma, jossa on kuvattu ne kohteet, joihin perustason turvatasovaatimukset on perusteltua määrittää. Koulutussuunnitelma hallinnolle. Koulutukset. Konsultointi.
C. Turvatasojen ohjaus ja tasolle pääsy Laaditaan ohje, miten organisaatiot voivat tunnistaa muut omat tärkeät kohteensa kohdassa 1 mainittujen 10 lisäksi. Tutkitaan, millä tasolla ja mihin kohteisiin turvatasovaatimuksia on mahdollista määrittää. Määritetään niiden perusturvatason vaatimukset.Kartoitetaan ja harmonisoidaan olemassa olevat luokitukset yhteisesti sovittujen tietoturvatasojen mukaisesti.	Suunnitelma, jossa on ehdotettu niiden turvaamistavoitteet ja perusturvataso Päätös kohteista, joihin perusturvataso määritetään. Ohje perustason turvatasovaatimuksista Soveltamisohje perusturvatason saavuttamiseksi. Malliesimerkit erityyppisistä pilottiorganisaatioista. VAHTI-ohjeissa olevien luokittelujen läpikäynti ja tarvittaessa päivitys. Lisäksi yhteisten osien tunnistaminen TLL-, tietoaineisto- ja muihin tietoturvallisuuteen liittyviin luokituksiin valtionhallinnossa.

II Vaikuttavat normit, standardit ja hyvät käytännöt

Kuvaus	Lopputulos
A. Selvitetään olemassa olevat normit, standardit ja hyvät käytännöt valittujen turvattavien kohteiden, turvatasojen ja kypsyyden osalta	Valtionhallinnon yhteiset turvatasot-ohjeen liite. Tietoturva-normiluettelon päivitys, ellei sellaista ole tehty jo muuten tai muussa hankkeessa. Normiluettelon laajennus, mahdollisesti normeista myös kuvaus, miten se vaikuttaa, ”mitä se on” organisaation kannalta. Julkiasupaikka joko VAHTIn, ValtIT:n tai suomi.fi-sivustolle. Hallinnonalat toteuttavat omassa toiminnassaan
B. Suunnitellaan, miten hyviä käytäntöjä voidaan hyödyntää ja yhdenmukaistaa.	Suunnitelma normien, standardien ja hyvien käytäntöjen hyödyntämisestä ja yhdenmukaistamisesta turvattavien kohteiden osalta. Lisäksi tutkitaan kuinka eri organisaatioissa voidaan hyödyntää Vahti-ohjeiden, ISO-standardien ja muiden pohjalta jo tehtyä kehitystyötä Peruskäyttäjätuen parantaminen, esim. VAHTI 10/2006 aineistojen lisäksi.

III Turvatasojen hyödyntämisen tutkiminen

Kuvaus	Lopputulos
Tutkitaan, miten turvatasoja voidaan soveltaa laajemmin koskemaan muita turvallisuuden osa-alueita ja yhteiskunnan elintärkeitä toimintojen turvaamista (YETT).	Suunnitelma turvatasojen hyödyntämisestä laajemmin, esim. esittelymateriaalin tekeminen, esitysten valmistelu ja viestintä. Kohderyhmiä voivat olla Komission jäsenmaat tai muut sidosryhmät, kuten OECD, ENISA, jne. Tietoturvakuutio-ajattelu on mahdollista saada keskusteluihin standardointia tekevien tahojen kanssa, koska se on yhteensopiva tietoturva-, laatu- ym. standardien kanssa. Tietoturvakuutio-ajattelu ja tasokuvaukset sopisivat konseptina myös muihin maihin. - esitysmateriaalien kääntäminen ja tekstien oikoluku ammattikääntäjältä.

IV Organisaatioiden kypsyyden ja turvatason arviointi sekä parantaminen	
Kuvaus	Lopputulos
A. Suunnitellaan miten strateginen, toiminnallinen ja turvatoimenpiteiden kypsyys määritetään sekä todennetaan. Kilpailuttaminen tai puitesopimusten valmistelu auditointipalveluja tarjoavien organisaatioiden palveluista ja yhteistyössä menettelyistä sopiminen.	Valtionhallinnon yhteiset turvatasot-ohje Ohje arvioijille Kokoontumiset auditointiasioissa sidosryhmien kanssa: VM/Controller, Valtion tarkastuvirasto, Sisäisten tarkastajien edustus, VM/ValtIT, auditointipooli jne. VAHTIn auditointipoolin roolista sopiminen ja tehtävien määrittely (esim. ohjausryhmätyöskentely toimittajille).
B. Suunnitellaan menettelyt, joilla parannetaan organisaatioiden kypsyyttä.	Valtionhallinnon yhteiset turvatasot-ohje Koulutusmateriaalin valmistelu Koulutussuunnitelma ja koulutukset.
C. Suunnitellaan, miten kypsyys ja turvataso toteutuvat yhteistyössä ja palveluissa	Valtionhallinnon yhteiset turvatasot-ohje Koulutusmateriaali Suunnitelma turvatasoja tukevista palveluista ja välineistä sekä välineiden kilpailuttaminen tai toteuttaminen.
V Tietoturvatasohankkeen kokonaishallinnan ja ohjauksen toteuttaminen	
Kuvaus	Lopputulos
Laaditaan hankkeen koordinointisuunnitelma. A. Varmistetaan hankkeelle tarvittava tuki ja ohjaus. B. Huolehditaan siitä, että hankekokonaisuus toteuttaa sille asetetut vaatimukset.	Hankkeen koordinointisuunnitelma ja muu hallintadokumentaatio. Pilottiorganisaatioiden kanssa pilotoinnin aikataulun tarkka määrittely ja organisaatiokohtaisesti

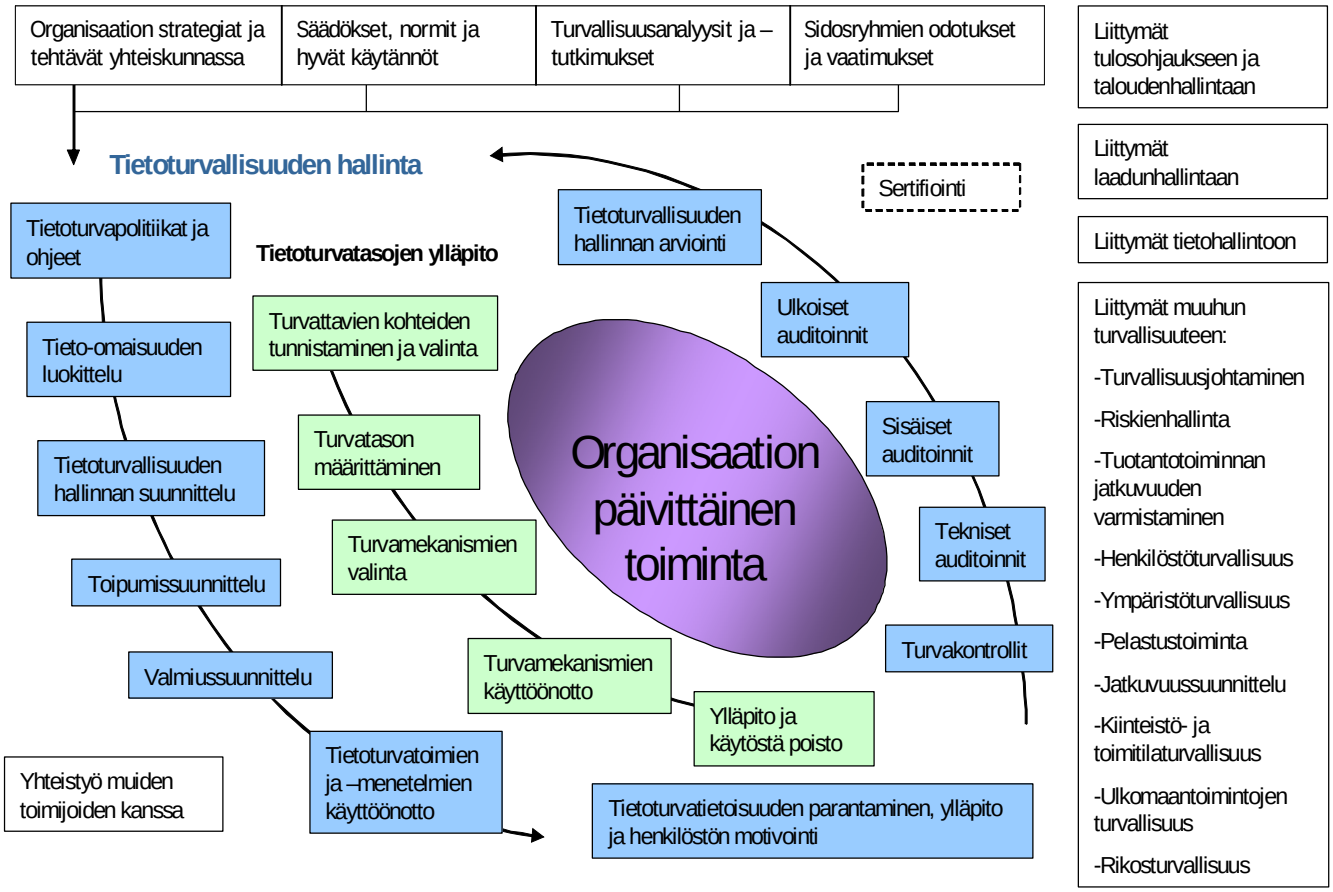
Kuva Liite 2.1. Tietoturvatasot –hankkeen eteneminen ja jatkoaikataulu.

4 LIITE 4 Tietoturvallisuuden tavoite- ja nykytilat

Tietoturvallisuuden hallinta parantaa kokonaisturvallisuutta. Alla olevassa kuvassa on prosessikuvamainen esimerkki organisaation (tieto)turvallisuuden hallinnasta.

Kokonaisturvallisuus edellyttää tietoturvallisuuden hallintaa.

Turvatasot ovat organisaation tietoturvallisuuden kokonaishallintaa



Kuva Liite 4.1 Tietoturvatasojen liittyminen tietoturvallisuuden kokonaishallintaan.

Perustasovaatimukset aiheuttavat tehtäviä organisaatioille. Suurin osa toistettavan perustason kypsyysvaatimuksista liittyy organisointiin ja päätöksiin. Ne eivät pääsääntöisesti aiheuta organisaatiolle ylimääräisiä kustannuksia. Tietoturvallisuusvaatimusten aiheuttamat kustannukset tulisivat olla osa normaalia toimintaa ja johtamista.

Kustannusarvio jokaisen turvatason aiheuttamista kuluista hallinnossa on kuitenkin tehtävä ennen normivaatimusten asettamista. Alla olevassa taulukossa on laskettu esimerkin omaisesti hallinnossa toteutettavan perustason vaatimusten kustannukset. Välinettä on mahdollista muokata sopimaan valtionhallintoon tai kuntasektorille tai vaikkapa yksittäisen organisaation tarpeisiin. Alla olevassa hahmotelmassa numeroarvot ovat esimerkkejä.

Esimerkki perusturvatasosta ja sen kustannusten laskemisesta

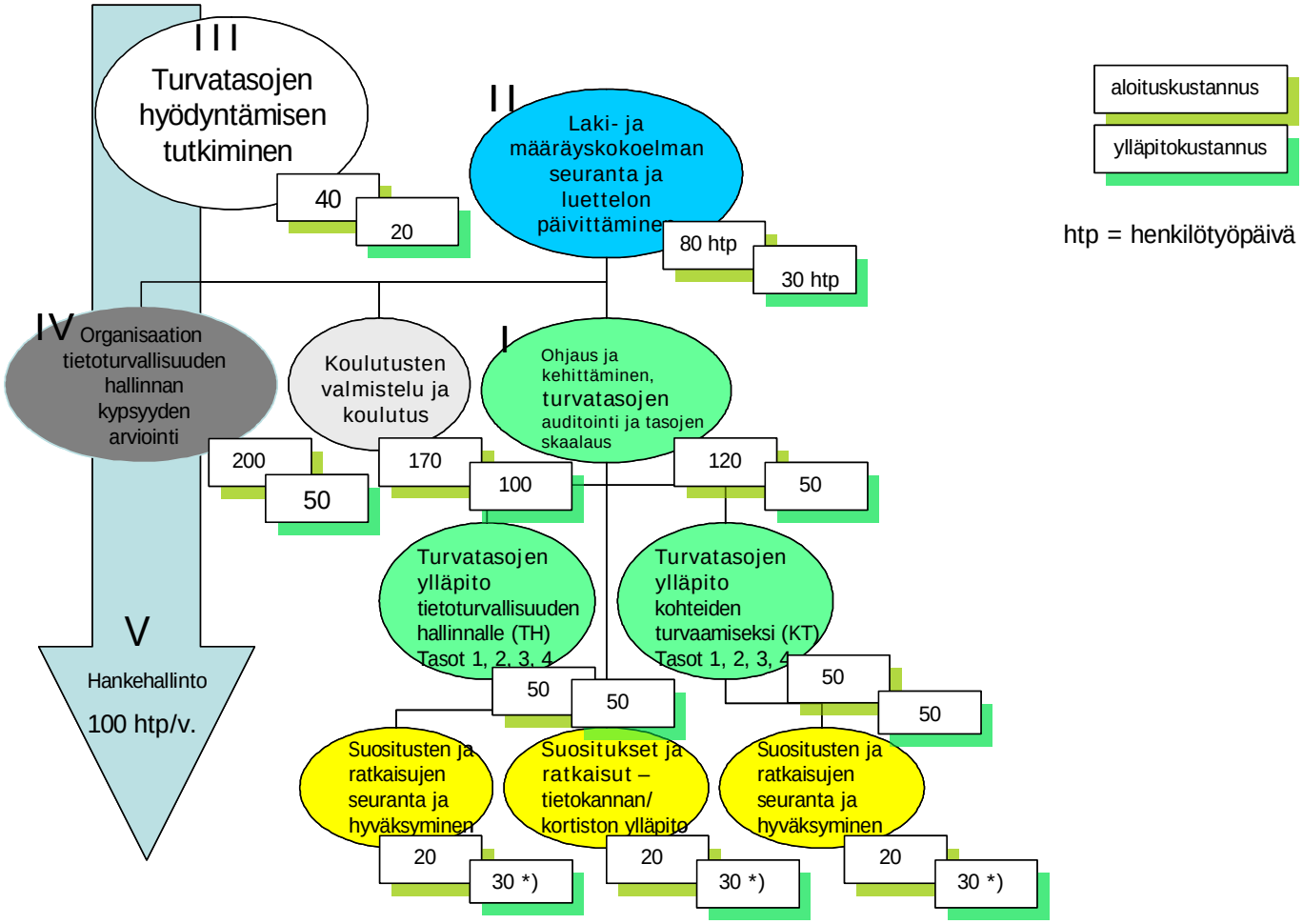
Tietoturvavaatimukset Perustason kustanusten arvio	**LASKELMA JA KUVATUT VAATIMUKSET OVAT ESIMERKKI**				Työpäivän hinta (teur)	*0,34*		
					Organisaatioita	Järjestelmiä	Virkoja	
					183	*5 000*	*123 000*	
		HENKILÖTYÖTÄ (htp)				**KUSTANNUKSET**		**Kust. (yht)**
Vaatimus	**Org.**	**Tietojärj. kohden**	**Henkilöä kohden**	**Asia kunnossa %**	**Org.**	**Tietojärj.**	**Hlö**	**4 178**
Vaatimus 1.1: Tietoturvariskit kartoitetaan säännöllisesti vähintään kahden vuoden välein	5	1	0,01	90 %	34	170	42	**246**
Vaatimus 1.2: Yksikön on luokiteltava toiminnot tai prosessit, jotka ovat sen toiminnalle kaikkein kriittisimmät	5	0,1		80 %	68	34		**102**
Vaatimus 1.3: Yksikön on luokiteltava järjestelmät, jotka ovat sen toiminnalle kaikkein kriittisimmät järjestelmät	5	0,1		80 %	68	34		**102**
Vaatimus1.4. Koko ulkoistamisen elinkaaren ajan organisaatio johto on nimennyt vastuuhenkilön	1	0,1		50 %	34	85		**119**
Vaatimus 2.1: On tietoturvapolitiikka, joka on johdon hyväksymä	2	0,1		95 %	7	9		**15**
Vaatimus 2.2: Organisaatiossa on määritelty Internetin ja sähköpostin käytön säännöt	2		0,01	80 %	27		84	**111**
Vaatimus 2.3: tietoturvasäädösten soveltamis- tai muuta vastaavaa ohjetta	10	1		60 %	272	680		**952**
Vaatimus 3.1: Organisaatiossa on henkilö, joka on tietoturvavastaava	1	0		90 %	7			**7**
Vaatimus 3.2: Organisaation johdon on osallistuttava koko henkilöstön tietoturvakoulutukseen.	2			95 %	7			**7**

Taulukko 1. Luonnos välineestä, jota jatkotyöstämällä on mahdollista arvioida yksittäisten toimien tai vaatimusten kustannuksia hallinnossa.

5 LIITE 5 Jatkohankkeeseen ehdotetut henkilötyöpäivämäärät

Alla olevaan kuvaan on merkitty jatkohankkeiden osakokonaisuudet I-V.

Henkilötyöpäivämäärät (htp) sisältävät yhteensä sekä arvioidun tarpeen virkatyölle valtiovarainministeriössä. Vaaleanvihreä laatikko on investointikustannukset eli työn aloittamiseen tarvittava resursointi (htp). Kirkkaan vihreä laatikko kuvaa ylläpitotyöhön tarvittavia henkilömääriä (htp).



Kuva Liite 5.1 Turvatasojen jatkohankkeen työn osuus valtiovarainministeriössä.

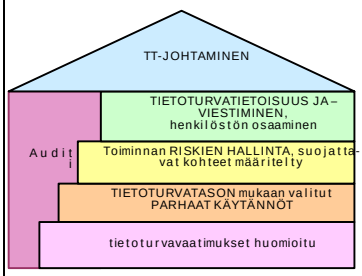
6 LIITE 6 Välineiden toteuttaminen jatkohankkeessa

Turvatasoille pääsemiseen on hallinnolle tarjottava hyödyllisiä apuvälineitä. Jokaisen jatkohankkeen osa-alueen toteuttamisen on tulossa tukea hallinnolle:

- Vaatimukset
- Ohjeet ja soveltamisohjeet
  - Mitä se on ja miksi?
- ”Työkalupakki”
  - välineitä
  - oppimisympäristöjä, muistiapuja ym.
- Koulutussuunnitelma
- Tuki VM:ltä
- Auditointi

Palveluita ja toivottuja välineitä on kuvattu myös liitteessä 8.

Alla olevissa määrittelyissä on kuvattu organisaation kannalta saatavaa tukea turvallisuuden hallintaan.

Kehittämisohjelma:	Tietoturvallisuus ja varautuminen
Kärkihanke:	Valtionhallinnon tietoturvatasot (esitutkimusvaihe 5/2007 asti)
Kärkihankkeen tuottaman palvelun nimi:	**Hallinnon yhtenäiset turvatasot**
Lyhyt kuvaus palvelun sisällöstä: 	**Suomen julkishallinnon organisaatioiden (tieto)turvallisuuden hallinnan yhtenäistäminen turvatasojen avulla** - (tieto)turva-asiantuntijapalvelu, hallinnon sisäinen konsultointi - Yhtenäinen perusturvataso hallintoon * määrittely ja perusteet * tukea toteuttamiselle, todentamiskeinot ja seuranta - (Tieto)turvallisuuden ohjaus organisaatioiden tulosohjauksen osaksi, strategiseksi vahvuudeksi ja TTS:n tasolle - Organisaation (tieto)turvallisuuden hallintaan tukea ja välineitä mm. (tieto)turvallisuuden hallintaan TTT-sivusto/portaali Organisaatiokohtainen (tieto)turvallisuuden hallinta koostuu seuraavista lähtökohdista, katso osat kuvassa vasemmalla: - (Tieto)turvallisuuden normivaatimukset - (Tieto)turvallisuuden hyvät, yhtenäiset käytännöt - **Riskienhallinta yhdessä VM/Controllerin kanssa** - (Tieto)turvatietoisuus, tt-viestiminen ja (tieto)turvakulttuuri - (Tieto)turvajohtaminen - Auditoinnin ohjaus
Palvelun käynnistämisen aikataulu:	Esitutkimus valmis: 2007 / 5 Kehitys- ja toteutusaika: 2007 / 8– 2008 / 12 Ensimmäinen käyttöönotto: 2008 / 1, alkaen pilottiorganisaatioista Käyttöönotto systemaattisesti hallinnossa vaiheittain v. 2009
Palvelun käyttöönoton vaikutukset mm. hallinnonalojen IT-palvelutuotannon nykytilanteeseen :	- (Tieto)turvallisuuden toteuttaminen on uskottavuuden peruselementti organisaatioille ja valtionhallinnolle kokonaisuutena - Edistetään luottamusta hallintoon kansallisesti ja kansainvälisesti - Turvatasot ovat mittaristo, jonka avulla laadunhallinta helpottuu - Tasot auttavat hallintoa hyvien käytäntöjen soveltamisessa. - Etukäteissuunnittelu säästää oikeudellisia ja korjauskustannuksia. - Vähennetään toissijaisiin asioihin käytettyä aikaa ja säästetään aikaa perustoiminnan tekemiseen ja parantamiseen. - (Tieto)turvavaatimusten jalkauttaminen hallintoon osaksi toimintaa - Turvatasot auttavat Controllerin, BO:n, Valtiokonttorin ja VTV:n toimintaa

TURVATASON mukaan valitut

HYVÄT KÄYTÄNNÖT

(tieto)turvavaatimukset

ja NorMIT huomioitu

”Kokonaisturvallisuudesta huolehtiminen ei riitä, jos nitoja on oven välissä kokoukseen tulevia vieraita varten.”

”Miten tämä laki muka vaikuttaa meihin?”

Kehittämisohjelma:	Tietoturvallisuus ja varautuminen
Kärkihanke:	Valtionhallinnon tietoturvatasot
Kärkihankkeen tuottaman palvelun nimi:	**Hallinnon (tieto)turvallisuuden hyvät käytännöt**
Lyhyt kuvaus palvelun sisällöstä:	**Suomen julkishallinnon organisaatioiden (tieto)turvan hallinnan parantuminen, yhtenäistyminen ja hallinnon uskottavuus** Hyvät käytännöt rakentuvat normivaatimusten mukaan - Yhtenäiset (tieto)turvallisuuden minimivaatimukset organisaatioille - Välineitä mm.: * Hyvän hallinnon koulutus työntekijöille * Koulutusmateriaalit, esitykset, videot jne. * (Tieto)turvanormivaatimukset, ohjeet, (tieto)turvakäsitteistö * Turvatasojen kuvaukset * Turvatasojen arviointimalli ja -asteikko * Turvatasojen nostamiseen käytännöt ja seuranta, jotka helpottavat organisaation ylimmän johdon ja (tieto)turvavastaavan työtä. Tavoitteet - Yhtenäinen perusturvataso valtiohallintoon - (Tieto)turvavaatimusten jalkauttaminen hallintoon osaksi toimintaa - (Tieto)turvan kokemusperäistäminen ja ydintoimintaa tukeva rooli - Organisaation (tieto)turvallisuuden hallintaan tukea ja välineitä Kohderyhmä: valtionhallinnon organisaatiot ja kunnat
Palvelun käynnistämisen aikataulu:	Kehitys- ja toteutusaika: 2007 / 8– 2008 / 5 Ensimmäinen käyttöönotto: 2008 / 1, alkaen kehittyneistä organisaatioista ja/tai pilottiorganisaatioista Käyttöönotto systemaattisesti hallinnossa vaiheittain v. 2009
Palvelun käyttöönoton vaikutukset mm. hallinnonalojen IT-palvelutuotannon nykytilanteeseen:	- Julkisuuslainsäädännön jalkauttamisen auttaminen hallinnossa - Tietoaineistojen käsittely ja tulosohjaus helpottuvat - Auttaa hallintoa hyvien käytäntöjen soveltamisessa. - (Tieto)turvaviestiminen organisaatioiden välillä paranee - Etukäteissuunnittelu säästää oikeudellisia ja korjauskustannuksia. - Vähennetään toissijaisiin asioihin käytettyä aikaa ja säästetään aikaa perustoiminnan tekemiseen ja parantamiseen. - Tasot auttavat Controllerin, BO:n, Valtiokonttorin ja VTV:n toimintaa - Edistetään luottamusta hallintoon, toimijoiden maine säilyy

Toiminnan RISKIEN HALLINTA,

TURVAttavat kohteet määritelty

”Riskienhallinta ja turvatasot auttavat priorisoimaan ja johtoa tekemään päätöksiä.”

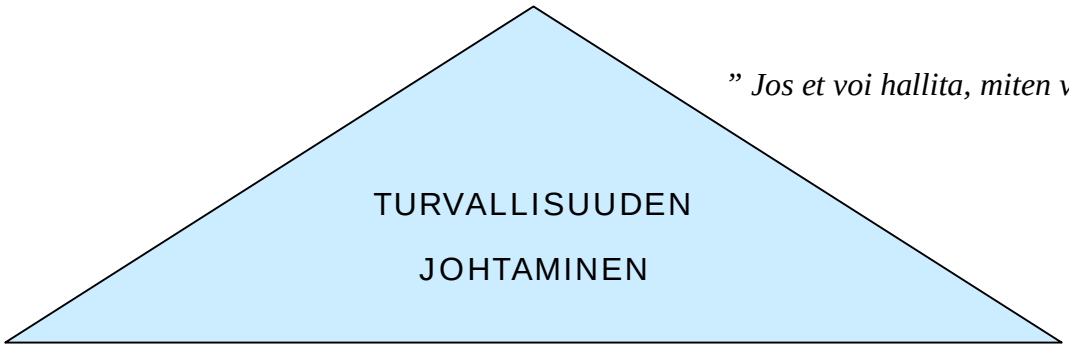
Kehittämisohjelma:	Tietoturvallisuus ja varautuminen
Kärkihanke:	Valtionhallinnon tietoturvatasot
Kärkihankkeen tuottaman palvelun nimi:	**Organisaatioille tukea riskienhallintaan**
Lyhyt kuvaus palvelun sisällöstä:	**Suomen julkishallinnon organisaatioiden toiminnan laadun ja turvallisuuden hallinta riskienhallinnan keinoin** (Tieto)turvallisuutta hallitaan riskinhallinnan välinein; Organisaation on arvioitava toimintaan kohdistuvia riskejä; sellaisia, jotka estävät halutun tavoitteen toteutumisen kokonaan tai osittain. Hallinnon organisaation tavoitteina voidaan pitää organisaatiolle asetetun julkisen tehtävän toteutumista sekä sitä, että tehtävät toteutetaan lainmukaisesti ja kustannustehokkaasti. * Turvatasot ovat myös riskienhallinnan välineitä, ns. työkalupakkeja, joilla suojattavia osa-alueita ja kohteita voidaan ryhmitellä organisaation tarpeita tyydyttäviksi kokonaisuuksiksi. * Riskienarviointivälineet Riskienhallintatoimet ovat toteutettavissa VM/Controllerin COSO-ERM-mallin välineillä. Kohderyhmä: valtionhallinnon organisaatiot ja kunnat
Palvelun käynnistämisen aikataulu:	Kehitys- ja toteutusaika: 2008 / 5– 2008 / 12 Ensimmäinen käyttöönotto: 2008 / 12, alkaen kehittyneistä organisaatioista tai pilottiorganisaatioista Käyttöönotto systemaattisesti hallinnossa vaiheittain v. 2009
Palvelun käyttöönoton vaikutukset mm. hallinnonalojen IT-palvelutuotannon nykytilanteeseen:	- Julkisuuslainsäädännön jalkauttamisen auttaminen hallinnossa - Turvatasojen käyttöönotto tuottaa riskienhallinnan tehostumista - Etukäteissuunnittelu säästää oikeudellisia ja korjauskustannuksia. - Vähennetään toissijaisiin asioihin käytettyä aikaa ja säästetään aikaa perustoiminnan tekemiseen ja parantamiseen. - Tasot auttavat Controllerin, BO:n, Valtiokonttorin ja VTV:n toimintaa - Edistetään luottamusta hallintoon, toimijoiden maine säilyy

(TIETO)TURVATIETOISUUS JA –VIESTIMINEN,

”Yritä muuttaa toimintaympäristöä, älä ihmisiä.”

Kehittämisohjelma:	Tietoturvallisuus ja varautuminen
Kärkihanke:	Valtionhallinnon tietoturvatasot
Kärkihankkeen tuottaman palvelun nimi:	**Valtionhallinnon työntekijöiden (tieto)turvatietoisuus**
Lyhyt kuvaus palvelun sisällöstä :	**Suomen julkishallinnon organisaatioiden (tieto)turvallisuuden hallinta** - (Tieto)turva-asiantuntijapalvelu, hallinnon sisäinen konsultointi - (Tieto)turvavaatimusten jalkauttaminen hallintoon osaksi toimintaa - (Tieto)turvakulttuurin luominen työhön - (Tieto)turvan kokemusperäistäminen ja ydintoimintaa tukeva rooli - (Tieto)turvatietoisuuden lisääminen ja viestiminen - Organisaation käytännön (tieto)turvatyöhön tukea ja välineitä * Hallinnon yhtenäinen koulutusohjelma ja ”(tieto)turva-ajokortti” * Kiinnostava ja moderni verkko-oppimisympäristö * (Tieto)turvallisuuden hallintaan TTT-sivusto/portaali * ”Kättä pidempää” ja tilattavia ”leluja” Kohderyhmä: valtionhallinnon organisaatiot ja kunnat
Palvelun käynnistämisen aikataulu:	Kehitys- ja toteutusaika: 2007 / 8– 2008 / 12 Ensimmäinen käyttöönotto: 2008 / 1 alkaen Käyttöönotto systemaattisesti hallinnossa vaiheittain v. 2009
Palvelun käyttöönoton vaikutukset mm. hallinnonalojen IT-palvelutuotannon nykytilanteeseen:	- Julkisuuslainsäädännön jalkauttamisen auttaminen hallinnossa - Vaatimusten noudattaminen esim. tietoaineistojen käsittelyssä helpottuu - Auttaa hallintoa hyvien käytäntöjen soveltamisessa. - (Tietoturva)viestiminen organisaatioiden välillä paranee - Etukäteissuunnittelu säästää oikeudellisia ja korjauskustannuksia. - Vähennetään toissijaisiin asioihin käytettyä aikaa ja säästetään aikaa perustoiminnan tekemiseen ja parantamiseen. - Edistetään luottamusta hallintoon, toimijoiden maine säilyy

” Jos et voi hallita, miten voit johtaa ?”



Kehittämisohjelma:	Tietoturvallisuus ja varautuminen
Kärkihanke:	Valtionhallinnon tietoturvatasot
Kärkihankkeen tuottaman palvelun nimi:	**Valtionhallinnon (tieto)turvajohtaminen**
Lyhyt kuvaus palvelun sisällöstä :	**Suomen julkishallinnon organisaatioiden (tieto)turvajohtaminen** - Kokonaisturvallisuuden hallinta organisaatiossa - (Tieto)turvatyön johtamiselle tukea - Governance-ajattelu - Tulostavoitteiden määrittelyyn turvallisuusasiat - Apuvälineitä johtamiseen * Tulosprisman hyödyntäminen * Riskienarvioinnin hyödyntäminen * julkaisut * koulutukset * benchmarking * .. - Tärkeä osa (tieto)turvajohtamista on ulkoistamisen johtaminen. - (Tieto)turva-asiantuntijapalvelu, hallinnon sisäinen konsultointi Kohderyhmä: valtionhallinnon organisaatiot ja kunnat
Palvelun käynnistämisen aikataulu:	Kehitys- ja toteutusaika: 2008 / 8– 2008 / 12 Ensimmäinen käyttöönotto: 2009 / 1 Käyttöönotto systemaattisesti hallinnossa vaiheittain v. 2009
Palvelun käyttöönoton vaikutukset mm. hallinnonalojen IT-palvelutuotannon nykytilanteeseen:	- Ylimmän johdon (tieto)turvavastuiden tiedostaminen - Auttaa hallintoa hyvien käytäntöjen soveltamisessa. - Vähennetään toissijaisiin asioihin käytettyä aikaa ja säästetään aikaa perustoiminnan tekemiseen ja parantamiseen. - Edistetään luottamusta hallintoon, toimijoiden maine säilyy

Auditointi

”Jos et voi mitata, miten voit hallita ?”

Kehittämisohjelma:	Tietoturvallisuus ja varautuminen
Kärkihanke:	Valtionhallinnon tietoturvatasot
Kärkihankkeen tuottaman palvelun nimi:	**Organisaatioiden (tieto)turvallisuuden auditointi**
Lyhyt kuvaus palvelun sisällöstä :	**Suomen julkishallinnon organisaatioiden (tieto)turvan hallinnan parantaminen ja seuraaminen auditoinnin avulla** VM toimii yhdessä valtionhallinnon auditointipoolin kanssa - (Tieto)turva-auditointien ohjeistaminen ja järjestäminen - Auditointipoolin organisaatioille tarjoama (tieto)turva-asiantuntijapalvelu, joka on hallinnon sisäistä ennakoivaa konsultointia ja kouutusta - Auditoinnin ohjauksen työvälineet: * julkaisu 8/2006 päivitettynä TTT-hankkeen tuloksilla * auditointi- ja arviointimenetelmät Lisäksi tutkitaan Netran mahdollisuudet auditointien raportointiin; (tieto)turva-auditointi yhdistettynä sähköiseen raportointiin voisi korvata osan VM:n tietohallinto- ym. kyselyitä jatkossa. Kohderyhmä: valtionhallinnon organisaatiot ja kunnat
Palvelun käynnistämisen aikataulu:	Kehitys- ja toteutusaika: 2007 / 8– 2008 / 12 Ensimmäinen käyttöönotto: 2008 / 1, alkaen auditointipoolin ja/tai TTT-hankkeen pilottiorganisaatioista Käyttöönotto systemaattisesti hallinnossa vaiheittain v. 2009
Palvelun käyttöönoton vaikutukset mm. hallinnonalojen IT-palvelutuotannon nykytilanteeseen :	- Turvatasojen käyttöönotto tuottaa riskienhallinnan tehostumista - Tulosohjaus helpottuvat - Auttaa hallintoa hyvien käytäntöjen soveltamisessa. - Etukäteissuunnittelu säästää oikeudellisia ja korjauskustannuksia. - Tasot ja parhaiden käytäntöjen mukainen auditointi auttavat Controllerin, BO:n, Valtiokonttorin ja VTV:n toimintaa - Edistetään luottamusta hallintoon, toimijoiden maine säilyy - Tukee organisaatiojen ylimmän johdon ja (tieto)turvavastaavien työtä

Kustannusarvio välineistä ei sisälly julkiseen raporttiin ja lausuntopyyntöön. Hallinnon asiantuntija saa sen halutessaan pyytämällä hankkeen vetäjältä (yhteystiedot liitteessä 9).

Karkea kustannuslaskelma: investointi ja ylläpito

	Oma virkatyö		Ostettava konsulttityö		Hallinnolta virkatyötä		Välineet
Vaihe	Työ-määrä	Kustan-nukset	Työ-määrä	Kustan-Nukset	Työ-määrä	Kustan-nukset	
Investointi-kustannukset	5 htv	0,3 M €	0 - 3 htv	0 – 0,4 M €	8 htv	0,5 M €	*) 0,9 M €
Ylläpito	2,8 htv	0,2 M €	0 - 1 htv	0 - 0,1 M €	4 htv	0,3 M €	*) 0,3 M €

Investointi-Kustannukset yht.	1,7 -2,1 M €	10/2007 - 12/2008
Ylläpito yht.	0,8 - 0,9 M €	1/2009 -> / v.

*) sisältää VAHTI-ohjeiston rakenteis-tamisen.

7 LIITE 7 Tietoturvataso-sanan mielleyhtymiä TTT-hankkeen aikana

- Pääseekö kaikki tasolle 1-
- 42
- Suhteellinen taso vs absoluuttinen taso
- BS, ISO, CC, CMM
- Liike-energia, jatkuvuus
- Optimitaso
- Myymistä
- Hyväksyvätkö kaikki tasoajattelun?
- Tietoturva-mitä se on?Mitä tasolla tarkoitetaan? Hyvä – huono? Kattava–hatara?
- Voiko sitä määritellä?
- MUURI ja Vahti
- LUOLA
- TIETOJÄRJESTELMÄ
- OHJE – noudattaako joku sitä?
- VAPAAEHTOINEN TAPA TOIMIA
- Turvallisuus
- Taso
- Luokka
- Liokitelu
- Tunne
- Tieto
- Varmuus
- Luottamus
- Vertailu
- Osaaminen
- Kyky
- Halu
- Tahto
- Tietosuoja; eheys, luottamuksellisuus, saatavuus
- Henkilöstön suojaaminen
- Sertifiointi
- Perusturvataso
- Vaativa, ISO, kolmansia maailmassa?
- Finnish (best) practice
- CMM
- Kansainväliset turvavelvoitteet
- Tavoitetason arviointimekanismi
- Luottamus (onko sitä?)
- Asioiden turvaluokittelu
- Tietoturvatasot erisuurikuin tietotekniset turvatasot
- Turvatason saavuttaminen edellyttää resursseja (rahaa, ihmisiä)
- Turvataso = uskottavuuden peruselementti
- F-secure virustorjunta
- Tarvitaanko laki
- Miten koulutus?
- Mistä ymmärrys
- Ohjeet

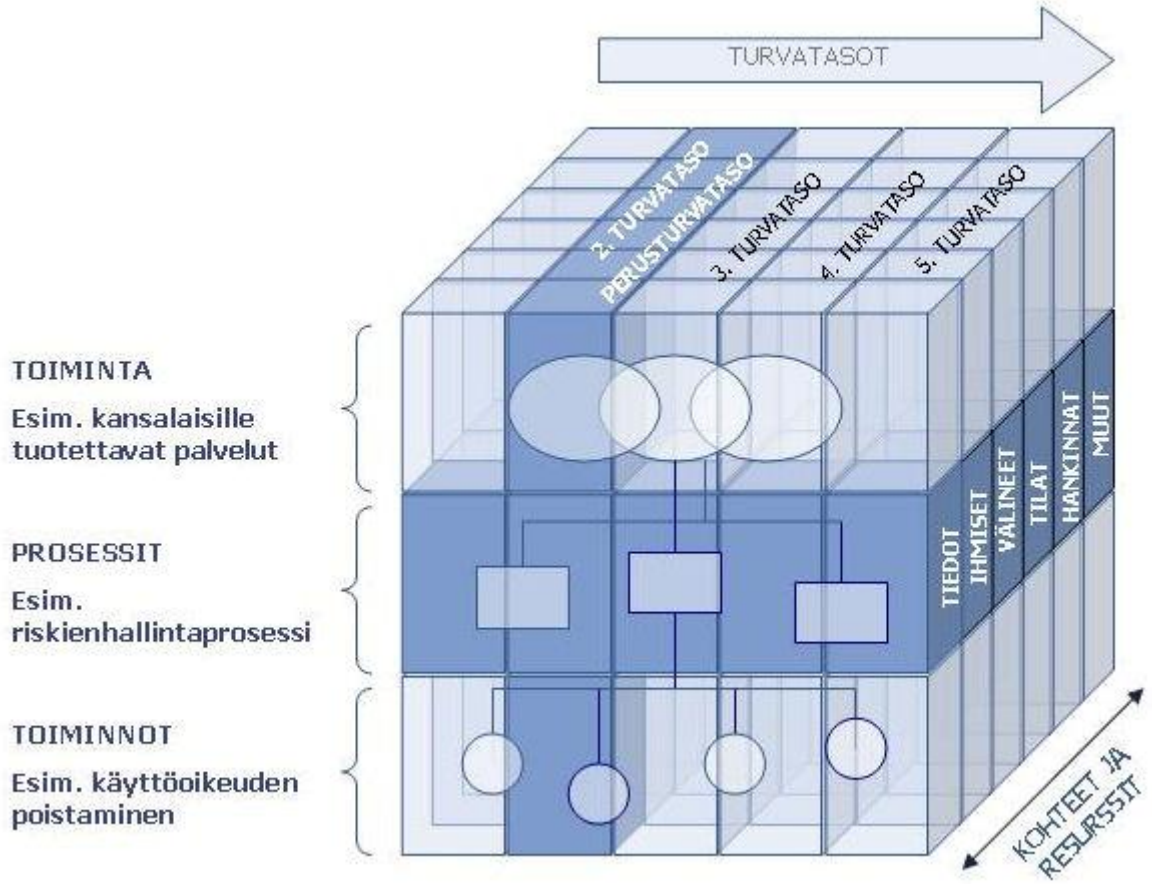
- Johdon sitoutuminen
- Rahat?
- Tietoliikenne-verkko ja pörssiomistus
- Virkakortit
- Kulunvalvonta
- Perusvaatimukset
- Välttämättömyys
- Luottamuksen perusta
- Yhteistoiminnan edellytys
- Oltava auditoitavissa
- Puolueettoman auditoijan todennettava
- Aiheuttaa kustannuksia
- Vaatii hyviä, osaavia resursseja
- Perustaso sisältää normien asettamat vaatimukset
- Standardeihin perustuva kypsyystaso
- Tietoturvatason saavuttaminen vaatii rahaa
- Tietoturvataso vaatii vastaavan ymmärrystason organisaatiolta
- Salaus
- Julkinen asiakirja
- Tenttitulosten julkistus
- Tutkimusprojektin turvavaatimukset
- Vanhojen tietokoneiden hävittäminen
- Henkilöstön suojaaminen
- Kypsyysaste
- Kestävät teknologiavalinnat
- Johtaminen
- Todelliset riskit
- Byrokratia
- Vaatimustenmukaisuus =vaikeaa
- Esimiestyö
- Jalkauttaminen
- Motivaatio
- Varma toiminnan alusta
- Voidaan luottaa ulkomaisten toimittajien järjestelmiin (sertifiointi?)
- Luottamussuhde samantasoisten organisaatioiden välillä => yhteistoiminta
- Mitattua ja eettisen hakkeroinnin avulla koeponnistettua
- Organisaatiot sertifioitu
- On osaamiskeskus, joka opastaa
- Hyvät välit TSV:n kanssa
- JulkNet
- Helppous
- Hyvä hallintotapa
- Hallinnon uskottavuus ja luotettavuus

8 LIITE 8 Tavoitetilan ja nykytilan kuvaus tietoturvallisuuden hallinnasta

Nykytila ja tavoitteet - Työpajan tulokset (tieto)turvallisuusvaatimuksista 29.3.2007

Hankeryhmä selvitti valtionhallinnon tietoturvallisuuden nykytilaa ja tavoitetilaa 29.3.2007 pidetyssä työpajassa. Työpajaan osallistui n. 20 henkeä eri organisaatioista. Tähän liitteeseen on koottu työpajan tulokset. Työpajassa muodostettiin kolme ryhmää. Kukin ryhmä pohti, mitkä voisivat olla valtionhallinnossa kahdeksan tärkeintä suojattavien kohteiden osa-aluetta. Ryhmät suunnittelivat myös, aiemmin määriteltyjen riskien ja ongelmien perusteella, millaisia tietoturvapalveluita valtionhallinnossa tarvitaan ja mitkä ovat niiden nykytilanne. Osallistujat laativat myös ehdotuksen palveluiden organisoinnista. Lopuksi suunniteltiin, millaisia apuvälineitä tarvitaan vaatimusten toteuttamiseksi.

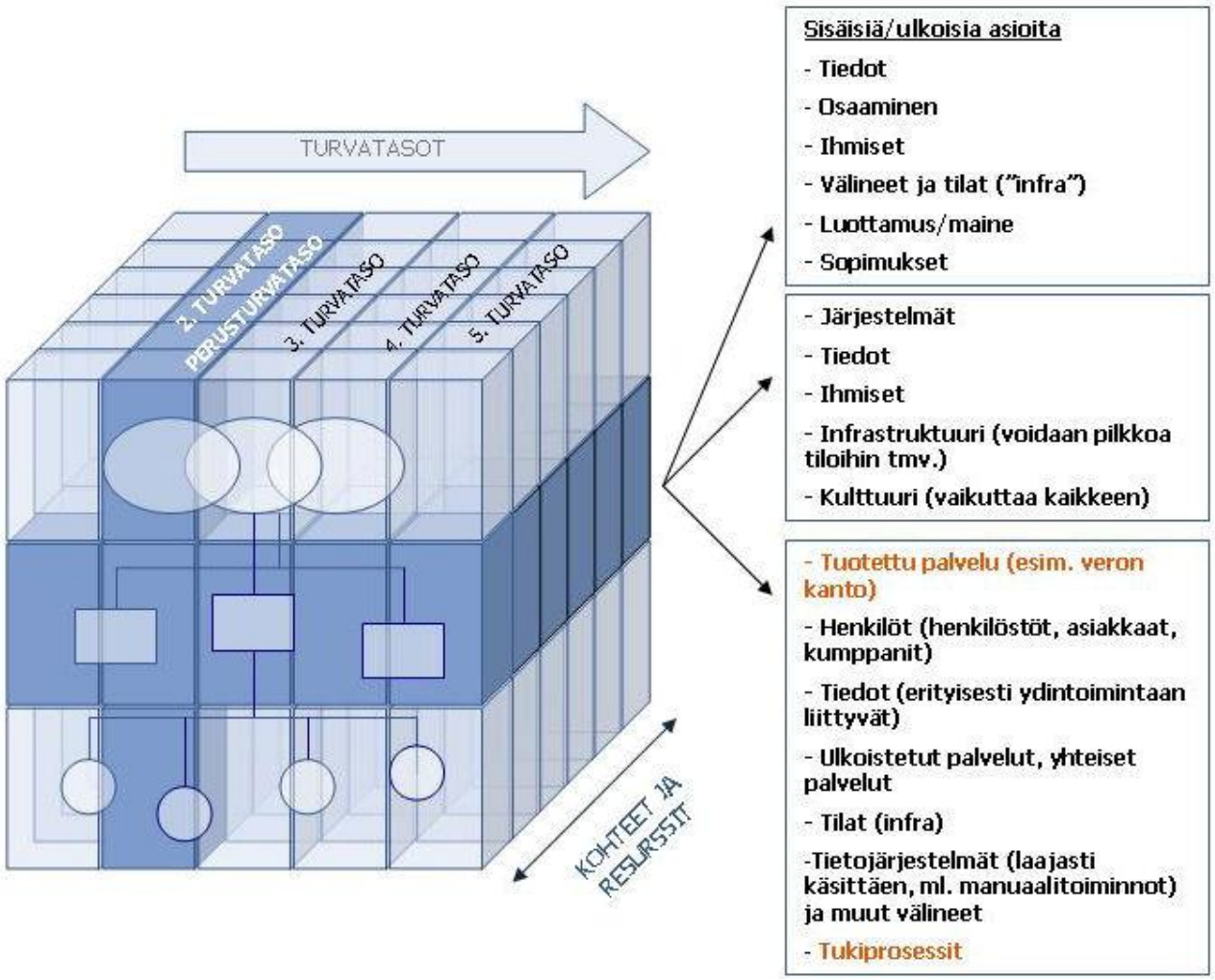
Turvatasojen lukumäärä muuttui kevään aikana. Työpaja pidettiin maaliskuussa ja raportti valmistui kesäkuussa, käytetty käsitemalli muuttui hieman. Alla on esitetty, miten asiaa lähestyttiin keväällä. Tasoja oli tuolloin viisi, mutta perustaso oli jo päätetty tasolle kaksi, jolloin sallittuja tasoja suunniteltiin jo tuolloin olevan neljä.



Kuva Liite 8.1. Turvatasokuutio sellaisena, kuin se esitettiin 2007 maaliskuussa. Tasojen määrää vähennettiin myöhemmin neljään. Kuvassa oikealla näkyvät kohteet olivat esimerkkejä.

Tärkeät ja turvattavat kohteet

Tietoturvavaatimusten kohteet määritettiin ryhmäkohtaisesti. Tulosten perusteella voitiin päätellä, että joitakin yhteisiä kohteita on määritettävissä koko valtionhallintoon. Toisaalta paljon on myös organisaatiokohtaisia kohteita, erityisesti kun ne määritellään yksityiskohtaisesti. Alla olevassa kuvassa on esitetty ryhmien määrittämät turvattavat kohteet.



Kuva Liite 8.1. Kuvassa on esitetty oikealla, millaisia turvattavia kohteita ryhmät määrittivät. Tulosten perusteella voitiin päätellä tietyt kohteet, jotka koskettivat valtaosaa hallinnon organisaatioista.

Tietoturvallisuuden perustasovaatimukset ja nykyiset kehittämiskohteet

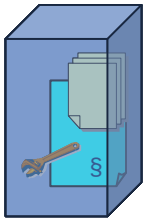
Tietoturvallisuuden perustasomääritykset kartoitettiin 1.3. pidetyssä työpajassa. Samaan aikaan määritettiin toisessa työpajassa valtionhallinnossa havaitut kehittämiskohteet.

- Suojattavien kohteiden määrittely ja riskien hallinta sen mukaisesti
- Tietoturvallisuuden seuranta, valvonta ja raportointi
- Valvonta ja raportointi (sääntörikkomuksiin reagoidaan)
- Poikkeamien seuranta käsittely ja seuranta
- Lokitietojen seuranta ja kriittisissä toiminnoissa jäljitettävyys
- Riskianalyysi, jossa tietoturvallisuus on huomioitu. On osa johtamista ja tehdään säännöllisesti esim. 1 vuodessa
- Johdon sitoutuminen
- Resurssointi
- Tietoturvallisuus mukaan kehittämiskeskusteluihin
- Tietoturvallisuus on vastuutettu työtehtävien mukaisesti
- Tietoturvallisuuden vastuuhenkilö olemassa
- Tulosohjaus
- Auditointi (mitä, miksi, milloin, kuka) Tietoturvavastuut työtehtävien mukaisesti
- Tietojärjestelmien ja Internet –käytön ”pelisäännöt”
- Tietoturvaohjeiden kattavuus (myös sidosryhmät huomioidaan)
- Tietoturvakoulutus
- Työsuhteet organisaation ulkopuolella (etätyö, etäkäyttö)
- Tietoaineistojen käsittelyssä tarvittava perustietämys
- Henkilöstön TT –tietoisuus (omaa toiminaa koskevat lait ja asetukset)
- Kaikkien työntekijöiden (myös johdon motivoituneisuus ja osaaminen) noudattaa normeja ja hyviä käytäntöjä
- Tietoturvallisuus perehdytyksessäPerustietotekniikka kuntoon
- Kulunvalvonta, palvelintilat, lähiverkkolaitteet)
- Kerrospuolustuksen toteutus ja valvonta
- Fyysinen turvallisuus (uusi suositus on tulossa) Tietoturvapäivitysten jatkuva jakelu
- Kerrospuolustuksen toteutus ja valvonta
- Tietoturvallisuuden sisällyttäminen järjestelmiin (turvallinen ja helppokäyttöinen tapa)
- Käyttöoikeuksien hallinta
- Tiedon salaus käyttöön luottamusten tietojen osalta
- Jatkuvuussuunnittelu
- Ydintoimintojen turvaaminen
- Varajärjestelyt (väh. varmuuskopiot kriittisistä tiedoista) Lakeja ym. sitovia normeja noudatetaan
- Ulkopuoliset vaatimukset tiedon käsittelyssä (vaatimusten seuranta ja analysointi)
- Sopimusten tietoturva ym. hallinnolle tärkeät vaatimukset perustuvat vahvasti suojattaviin kohteisiin
- Ulkoistukset ja hankinnat (sopimukset, auditointi)
- Lainsäädännön valmistelusta: tietoturvaa koskeva lainsäädäntö perustuu yleisesti hyväksyttäviin periaatteisiin
- Tietosuojan turvaaminen
- Auditointikäytännöt
- Riskien arviointi ja hallinta
- Tietoturvallisuuden organisointi
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Laitteisto- ja tietoverkkoturvallisuus
- Tietojenkäsittelyn kehittäminen ja ylläpito
- Liiketoiminnan jatkuvuuden suunnittelu
- Vaatimustenmukaisuus
- Tiedon fyysinen säilyvyys on riittävästi varmistettu
- Muutostenhallinta (tulee olla kuvattu)
- Tietojen turvallinen hävittäminen (otetaan myös kovalevyt ym. tietoa sisältävä materiaali huomioon
- Turvallinen viestintä oltava sellainen, ettei sitä kierretä hankaluuden tmv. vuoksi
- Julkinen tieto on järkevästi ulkoisten tahojen käytettävissä
- Viraston toiminnassa tarvittava tieto on sisäisesti riittävän laajasti käytettävissä (saatavuus)
- Tiedon salassapito perustuu hyväksyttyihin salassapitokriteereihin
- Tiedon säilytysaika on määritelty ja tiedotettu
- Viraston toiminnassa ei kerätä eikä säilytetä laitonta tietoa

Taulukko Liite 8.1. Oheisessa taulukossa on esitetty työpajassa määritettyjä perustason vaatimuksia. Punaisella on merkitty ne kohteet, joissa havaittiin kehittämistarpeita.

Tarvittavat palvelut hallinnolle

Vaatimusten noudattamista helpotetaan antamalla tukea ja ohjaamalla. Kuvassa laatikon sisältö:

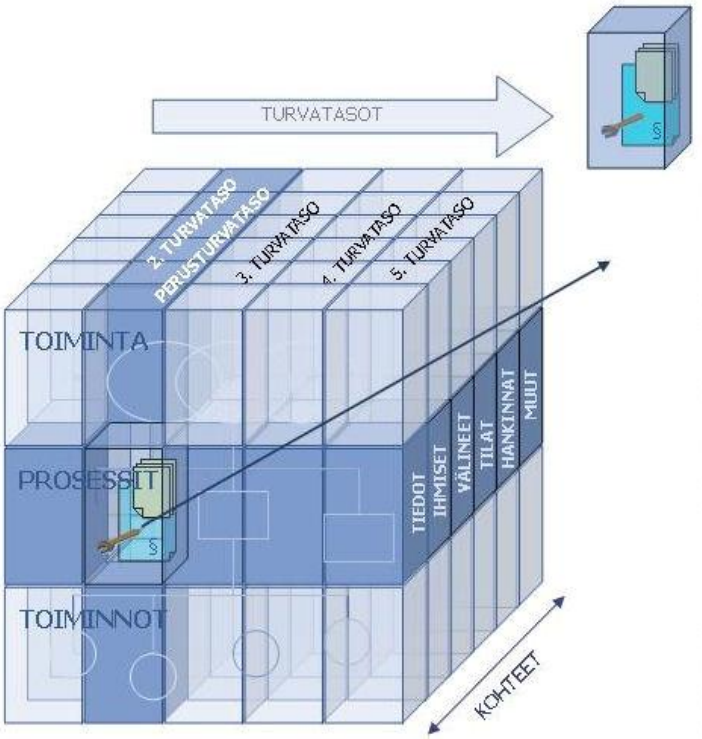


- Normitausta
- Vaatimukset
- Ohjeet
- Mallit
- Apuvälineet

Mitä muuta tarvitaan?

Ryhmät määrittivät, millaisia palveluja tarvitaan tietoturvatyön tueksi. Alla olevissa kolmessa eri kuvassa ovat työryhmien tulokset.

Erityisesti kiinnitettiin huomiota alueisiin, joissa on tähän mennessä puutteita.



Vaatimusten noudattamista helpotetaan antamalla erilaisia välineitä, "kättä pidempää".

-poikkeustilanneohjeet (käytännölliset)

- Verkkotopologia ajan tasalla (tilannekuva, dokumentointi)

-tikettityökalu (seurantaa varten, korvamerkintä)

-Neuvontapiste asiantuntijoille (vertaispiste, jossa voisi luottamuksellisesti)

Jäsennelty ohjeistus (VAHTI –sivusto uudelleen sovellettuna ja TSV -> tietoturvaportaali)

Poikkeamien seurantatyökalu

Riskienhallintatyökalu

Koulutuspalvelu (täsmäkoulutus, käyttäjä, ylläpitäjä, johto/johdon katselmus)

Tietoturvatasojen konkreettiset ja lyhyet tarkistuslistat

Auditointipalvelut

Ylläpitäjien tietoturvatyökalut (esim. TUTKAIN – palvelu ja ETHEREAL, löytyy myös muita sniffereitä)

Laite- ja sovellusrekisteri

Johdon katselmointi ja sen apuvälineet

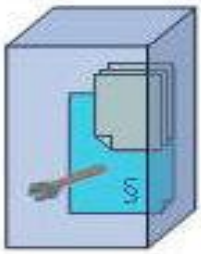
Käytettävyysmetriikka

"Porkkanat"

Mittarit

Suunnittelijoille arkkitehtuurityökalu

Ajantasainen tietoturvanormisto (lait ja oman organisaation ohjeet yhdessä paikassa)



Vaatimusten noudattamista helpotetaan antamalla erilaisia välineitä, "kättä pidempää".

Mitä ne voisivat olla?

- Auditointipooli

- Yhteiset projektityömallit

-Erilaiset sopimukset (mm. vääntövoimaa toimittajiin nähden)

-Koulutuspalvelut ja –aineistot eri kohderyhmille

-Johdolle "tietoturvakummit" (vertaistuki)

-Jatkuvasti ylläpidetyt tarkistuslistat noudatettavista laeista organisaatiokohtaisesti

-Erilaisia yhteisiä tietoturvastandardeja ja rajapintoja (ei liian rajoittavia)

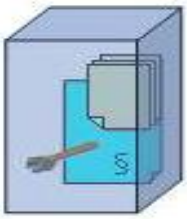
-Riskianalysointivälineet, aukkoanalyysit

-Sisäisiä tietotekniikkapalveluita (esim. erityisasiantuntemusta vaativat pienemmille organisaatioille)

-Yhteisiä asiantuntijapalveluita

-Hallittu hyökkäyspalvelu

-Pelastuspalvelu



Vaatimusten noudattamista helpotetaan antamalla erilaisia välineitä, "kättä pidempää".

Mitä ne voisivat olla?

- Auditointipooli

- Yhteiset projektityömallit

-Erilaiset sopimukset (mm. vääntövoimaa toimittajiin nähden)

-Koulutuspalvelut ja –aineistot eri kohderyhmille

-Johdolle "tietoturvakummit" (vertaistuki)

-Jatkuvasti ylläpidetyt tarkistuslistat noudatettavista laeista organisaatiokohtaisesti

-Erilaisia yhteisiä tietoturvastandardeja ja rajapintoja (ei liian rajoittavia)

-Riskianalysointivälineet, aukkoanalyysit

-Sisäisiä tietotekniikkapalveluita (esim. erityisasiantuntemusta vaativat pienemmille organisaatioille)

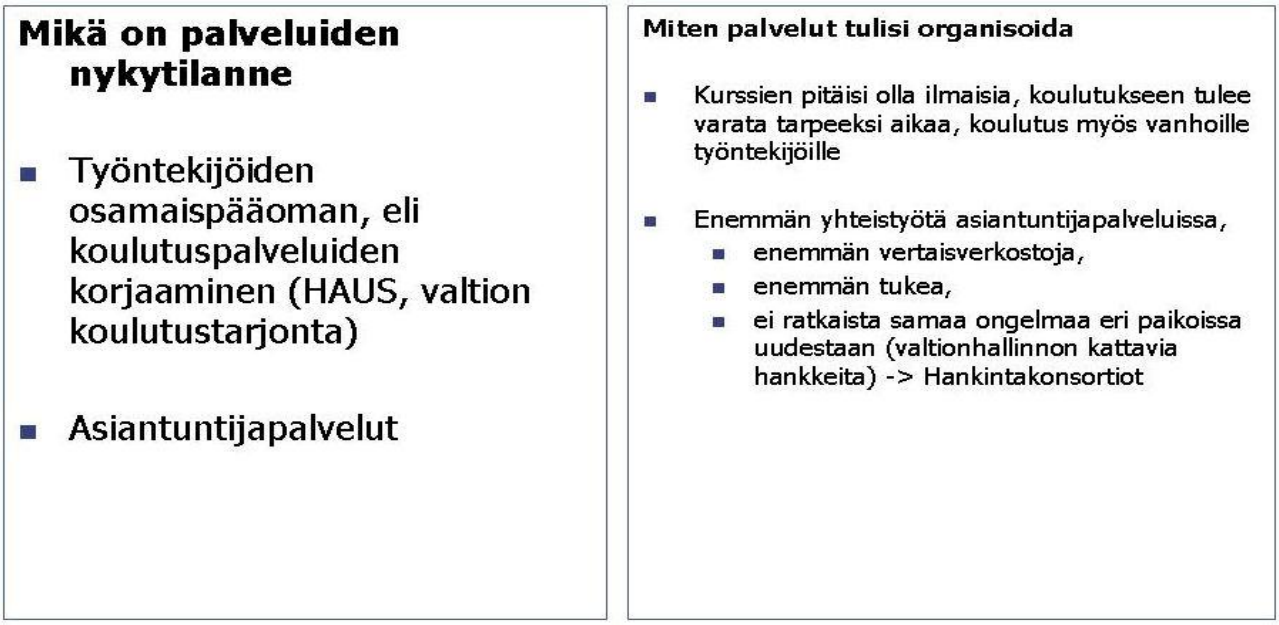
-Yhteisiä asiantuntijapalveluita

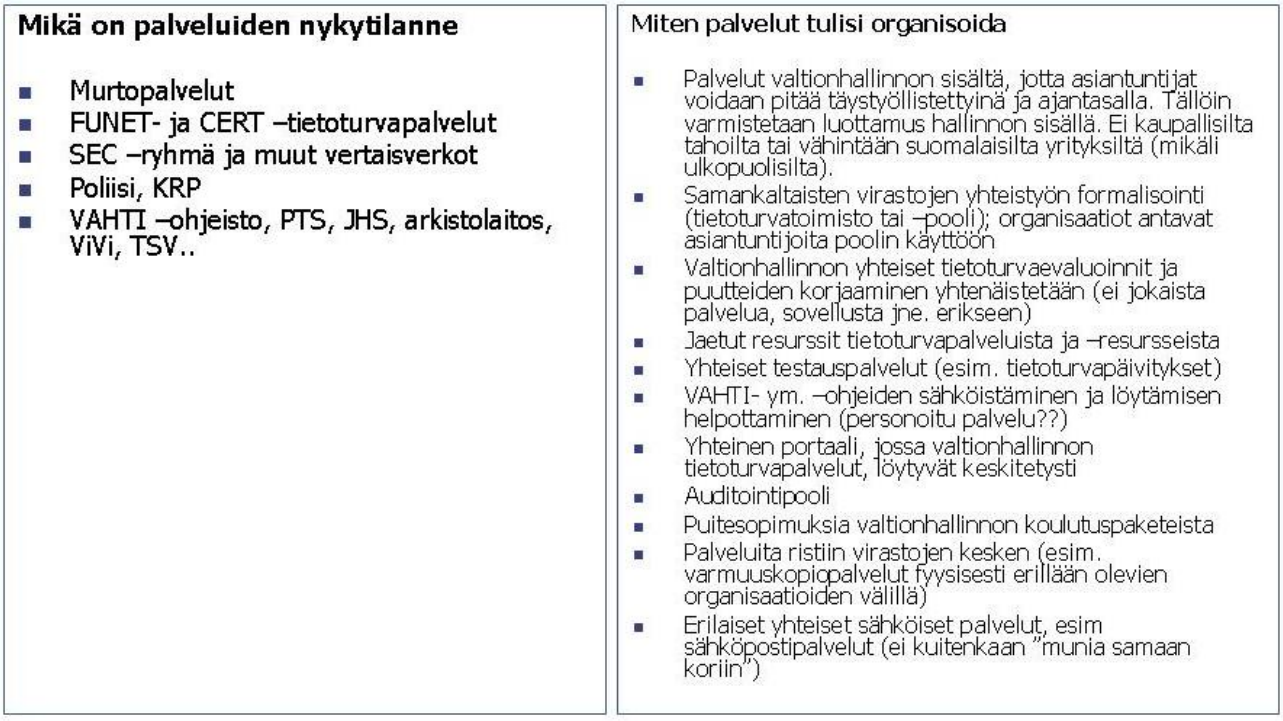
-Hallittu hyökkäyspalvelu

-Pelastuspalvelu

Palveluiden organisointi

Ryhmät määrittävät myös miten tietoturvallisuuden hallintaa tukevat palvelut tulisi organisoida ja mikä on niiden nykytilanne.





Mikä on palveluiden nykytilanne	Miten palvelut tulisi organisoida
▪ VAHTI –ohjeita ei kaikilta osin noudateta	▪ Ei ulkoisteta kaikkea; vastuuta ei voida ulkoistaa ▪ Ohjeiden personointi ja jalkauttaminen ▪ Apua tulosohjauksessa ▪ Hinta-laatusuhteen valvonta ▪ Auditointipalvelut, konsultointipalvelut (tuotteistetut)

Jatkohanke

Tässä liitteessä mainittuja alueita tutkitaan tarkemmin jatkohankkeessa.

Hankkeen toteuttamissuunnitelma on kuvattu raportin liitteessä 3.

9 LIITE 9 Yhteystiedot Tietoturvatasot-hankkeessa: vastuuorganisaatiot ja -henkilöt

Hankkeen hallinto ja yhteyshenkilöt:

Ohjausryhmän puheenjohtaja:	valtion IT-johtaja Leena Honka, VM
Ohjausryhmän vpj, VAHTIn pj	neuvotteleva virkamies, Mikael Kiviniemi, VM
Hankkeen vetäjä	tietoturva-asiantuntija Minna Romppanen, VM
Yhteystiedot	Sähköposti muotoa etunimi.sukunimi@vm.fi
ValtIT:n sivut	http://www.valtit.fi/
VAHTIn sivut	http://www.vm.fi/vahti/

Asettamiskirje VM115:01/2006 löytyy Hankerekisteristä http://www.hare.vn.fi/ tai suoraan http://www.hare.vn.fi/mAsiakirjojenSelailu.asp?h_iId=12314&a_iId=98801

Tiedot meneillään olevista lausunnoista tulevat ValtIT:n nettisivuille [Ajankohtaista]

http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/04_valtion_tietohallinnon_ohjaus/01_ajankohtaista/index.jsp

Valtionhallinnon tietoturvavastaaville tulee syksyllä lisäksi kutsu webikyselyyn.

Avoimet kommentit hankkeesta tai sen sisällöstä, lisätietopyynnöt ja yhteydenotot hankkeen vetäjä Minna Romppaselta sähköpostitse tai p. 09 - 160 33206 / 0400 - 902 968

Ohjausryhmän jäsenet:

Honka, Leena	VM
Kiviniemi, Mikael	VM
Björklund, Eeva	Ilmailulaitos
Santalahti, Kari	SM/PO
Uusikartano, Ari	UM

Hankeryhmän jäsenet:

Huhtamäki, Jari	LVM
Karppinen, Lauri	Tietosuojavaltuutetun toimisto
Koivunen, Erka	Viestintävirasto,
* henk.koht. varajäsen	Kilkkilä, Sami, Viestintävirasto
Kommonen, Mats	Turun yliopisto,
* henk.koht. varajäsen	Peuhkuri, Markus, Teknillinen korkeakoulu

Seurantaryhmän jäsenet:

Holmberg, Jan	VM/Controller
Holmroos, Antti	SM, KuntaIT
Huvila, Matti	Åbo Akademi
Hyytiä, Kalevi	Puolustusvoimat
Kaila, Urpo	CSC
Kilpeläinen, Pirkko	Ilmatieteen laitos
Kuusisto Tuija	PLM
Mård, Pekka	TKK
Markula, Juhani	Teknillinen korkeakoulu
Mannonen, Timo	Tilastokeskus
Mansukoski,Timo	Teatterikorkeakoulu
Perkiö, Seppo	EK
Pirhonen, Jari	Tietoturva ry
Puhakainen, Petri	Verohallitus
Ritola, Jaakko	RVLE
Röning, Juha	Oulun yliopisto
Salminen, Tuomo	Valtiontalouden tarkastusvirasto
Sillanpää, Juhani	VM/HKO
Sinervo, Heikki	EK
Tiihonen, Kalevi	EK
Turunen, Maarit	Valtiokonttori
Voutilainen, Tomi	Valtiontalouden tarkastusvirasto

Kiitokset kaikille;
kollegoille, ystäville, tuttaville
sekä
erityisesti monille teille,
jotka olitte mukana
ilman virallista nimeämistä !

10 LIITE 10 Lähteitä ja lisätietoja

Ohjeet ja määräykset

1 Suomen perustuslaki (731/1999) -10§ ja 12§

2 Laki viranomaisten toiminnan julkisuudesta (621/1999) ja 38§:n muutos (636/2000)

3 Asetus viranomaisten toiminnan julkisuudesta (1030/1999)

4 Asetus valtionhallinnon tietohallinnosta (155/1988) ja muutos (1491/1992)

5 Valtioneuvoston ohjesääntö (202/2003)

6 Arkistolaki (831/1994)

7 Asetus valtion talousarviosta (1243/1992) ja muutokset (600/1997 ja 263/2000)

8 Laki huoltovarmuuden turvaamisesta (1390/1992)

9 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta 11.11.1999

10 VN:n periaatepäätös valtionhallinnon IT-toiminnan kehittämisestä 15.6.2006

11 Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä valtionhallinnossa (VM 0024:00/02/99/1998)

12 Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje (VM 23/01/2000, 18.8.2000, VAHTI 2/2000)

13 Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje (VM 5/01/2000)

14 Suositus toimitilaturvallisuuden huomioonottamisesta valtionhallinnossa,. VM 30.12.1998

15 Julkisuuslain mukaisen tietojärjestelmäselosteen laadintasuositus, VM

16 Tietojenkäsittelyn turvaaminen tietoyhteiskunnassa (PTS, Tietojärjestelmäjaosto 1/1996) korvattu Tietotekniikan turvallisuus ja toiminnan varmistaminen (1/2002) –asiakirjalla

17 Valtion tietotekniikkahankintojen yleiset sopimusehdot, VYSE (VM 1998)

a. Erityisehtoja konsultointipalveluista, VKOE (VM 1998)

b. Erityisehtoja laitehankinnoista, VLAE 1998

c. Erityisehtoja tilaajan sovellushankinnoista, VTSE 1998

d. Erityisehtoja valmisohjelmistohankinnoista, VVOE 1998

e. Erityisehtoja käyttöpalveluista, VKÄE 1998

f. Erityisehtoja laitteiden huolto- ja ohjelmistojen ylläpitopalveluista, VHYE 1998

g. Tarjous- ja soveltamisohje

18 Ohje kansalaisten kuulemisesta

19 OECD:n suositus: Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet

20 Sopimuksiin perustuva varautuminen tietoyhteiskuntasektorilla

21 Yhteiskunnan huoltovarmuuden kannalta keskeisten toimintojen riskiarviointi, HVK Julkaisuja 2/2005

22 Tietotekniikan turvallisuus ja toiminnan varmistaminen, PTS, 1/2002, korvaa Tietojenkäsittelyn turvaaminen tietoyhteiskunnassa (PTS, Tietojärjestelmäjaosto 1/1996)

23 Internet, toiminnan verkottuminen ja sen haavoittuvuus, PTS:n tietojärjestelmäjaoston julkaisu 2/2001

24 Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005

25 Tietojenkäsittelyn turvaaminen tietoyhteiskunnassa, 1996 (VM ja PTS)

26 Suositus toimitilaturvallisuuden huomioonottamisesta valtionhallinnossa, VM 30.12.1998

27 Kansallinen tietoturvastrategia 25.11.2002

28 JHS 129 Julkishallinnon verkkopalvelun suunnittelun ja toteuttamisen periaatteet

Standardit

1 European Foundation for Quality Management

2 Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management, ISO/IEC 13335-1:2004 (PDF)

3 Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security, ISO/IEC TR 13335-3:1998 (PDF)

4 Guidelines for the management of IT Security - Part 4: Selection of safeguards, ISO/IEC TR 13335-4:2000 (PDF)

5 Guidelines for the management of IT Security - Part 5: Management guidance on network security, ISO/IEC TR 13335-5:2001 (PDF)

6 Code of practice for information security management, ISO/IEC 17799:2005 (PDF)

7 Information security management systems – Requirements, ISO/IEC 27001:2005 (PDF)

8 Evaluation criteria for IT security - Part 2: Security functional requirements, ISO/IEC 15408-2:2005 (PDF)

9 Evaluation criteria for IT security -- Part 3: Security assurance requirements, ISO/IEC 15408-3:2005 (PDF)

10 Tietoturvallisuuden hallintaa koskeva menettelyohje, ISO/IEC 17799:fi

11 Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. ISO/IEC 27001:fi

12 ITIL: Security Management Book, Security Management

13 COBIT:

a. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

b. COBIT Security Baseline

c. Aligning COBIT, ITIL and ISO 17799 for Business Benefit: A Management Briefing from the IT Governance Institute and the Office of Government Commerce

14 SSE-CMM:

a. SSE-CMM presentation

b. The Relationship Between The SSE-CMM and IT Security Guidance Documentation, 1999

15 Information security management systems - guidelines for information security risk management, BS 7799-3:2006

16 Information security management measurements, ISO/IEC 27004, joka kattaa sekä turvahallintaprosessit (ISO/IEC 27001:2005 (PDF)) että valvontamekanismit (ISO/IEC 17799:2005 (PDF) josta tulee ISO/IEC 27002 vuoden 2007 aikana.

17 ITIL, BS 15000, ISO 20000 ja ITSMF (tietotekniikkapalveluiden hallinta)

18 Common Criteria, CC

a. Part 1: Introduction and general model

b. Part 2: Security functional requirements

c. Part 3: Security assurance requirements

19 ISO 15408 (tietoturvallisuusprofiili)

20 Secure storage units. Classification and methods of test for resistance to fire. Data rooms and data containers, BS EN 1047-2:2000, laitetilojen fyysinen turvallisuus

21 Statement on Auditing Standard 70, SAS 70

22 ISF Standard of Good Practice

23 NIST Special publications:

a. NIST/FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

b. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems

24 DS 484, Tanskan tietoturvatasot

25 HIPAA Law, HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

26 Sarbanes-Oxley Act of 2002

27 GLBA, Gramm-Leach-Bliley Act, Disclosure of Nonpublic Personal Information

28 BASEL II, International Convergence of Capital Measurement and Capital Standards

29 ISACA Standards for IS Auditing

30 INFOSEC Evaluation Methodology

31 INFOSEC Assessment Methodology

32 INFOSEC Assurance Capability Maturity Model

33 Information Security Management Maturity Model (SOMA)

34 COSO Enterprise Risk Management

Muut asiakirjat

1 Hallituksen tietoyhteiskuntaohjelma

2 The OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (2002)

3 Security Metrics Guide for Information Technology Systems. NIST Special Publication 800-55, July 2003

4 Kansallinen tietoturvakatsaus, Ficora 2002

5 Hyvän tiedonhallintatavan määritys, Valtiovarainministeriö, Työryhmämuistio 11/2001

11 LIITE 11. Pilotoinnin aikataulu, viranomaisjulkinen

Pyydettäessä.

Toimitetaan hallintoon vain työtehtävien mukaan tarvitseville.

[Pilottiorganisaatiot yhteyshenkilöineen.]

[Pilotoinnin tarkka aikataulu.]

12 LIITE 12. Tietoturvatasot-jatkohankkeen kustannusarvio, viranomaisjulkinen

Pyydettäessä.

Toimitetaan hallintoon vain työtehtävien mukaan tarvitseville.

[Jatkohankkeiden tarkka kustannusarvio.]