VALTIOVARAINMINISTERIÖ

Tieto-turvalli-suuden arviointi-ohje

2/2014 VAHTI

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Tietoturvallisuuden arviointiohje

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä

2/2014 VAHTI

441 729
Painotuote

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Anitta Heiskanen /VM-julkaisutiimi

ISSN 1455-2566 (nid.)
ISBN 978-952-251-622-0 (nid.)
ISSN 1789-0860 (PDF)
ISBN 978-952-251-623-7 (PDF)

Juvenes Print - Suomen Yliopistopaino Oy, 2014

VALTIOVARAINMINISTERIÖ **Ohje** **VM/2423/00.00.00/2014**

27.11.2014

Ministeriöille, virastoille ja laitoksille

Tietoturvallisuuden arviointiohje

Oheisen valtiovarainministeriön antaman Tietoturvallisuuden arviointiohjeen tavoitteena on tukea, kehittää ja lisätä valtionhallinnon tietoturvallisuuden arviointeja. Ohje on valtionhallinnon tietoturvallisuuden arviointien yleisohje ja se korvaa aikaisemmat ohjeet Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006 sekä Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003.

Viranomaisten tulee varmistaa organisaationsa, palveluidensa ja tietoaineistojensa turvallisuus. Tämän toteuttamiseksi tulee säännöllisesti arvioida organisaation tietoturvallisuuden tilaa sekä toteutettujen tietoturvatoimenpiteiden asianmukaisuutta ja riittävyyttä.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) edellyttää tietoturvallisuuden perustason saavuttamista kaikilta valtionhallinnon virastoilta ja laitoksilta. On tärkeää, että viranomaisissa panostetaan riittävästi tietoturvallisuuden hallinnollisiin ja teknisiin arviointeihin asiaa koskevien säädösten ja tämän ohjeen mukaisesti.

Ohje julkaistaan VAHTIn internet-sivuilla. Lisätietoja antaa tietoturvallisuusasiantuntija Aku Hilve (etunimi.sukunimi@vm.fi).

Liikenne- ja kuntaministeri Paula Risikko

Yksikön päällikkö, Tietohallintoneuvos Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite Tietoturvallisuuden arviointiohje (VAHTI 2/2014)

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

Sisältö

Esipuhe

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) edellyttää tietoturvallisuuden perustason saavuttamista kaikilta valtionhallinnon virastoilta ja laitoksilta. Viranomaiset ovat panostaneet merkittävästi tietoturvatyöhön asetuksen voimaan tulon jälkeen. Tietoturvallisuuden arvioinnilla pystytään vaikuttamaan panostusten kohdistamiseen ja niiden vaikuttavuuden arviointiin.

Tietoturvallisuuden arviointi ja mittaaminen on asetuksessa yhtenä vaatimuskokonaisuutena. Sen merkitystä korostaa arviointitoiminnasta erikseen annettu lainsäädäntö. Arviointitoiminnasta on annettu aikaisemmin VAHTI-ohjeita, mutta muuttuneeseen lainsäädäntöön ja siinä annettuihin velvoitteisiin liittyvää kokonaisuutta päätettiin tarkentaa uudella ohjeella.

Ohje on laadittu VAHTIn alaisessa hankeryhmässä, jonka jäseninä ovat toimineet:

- Aku Hilve, valtiovarainministeriö, ryhmän puheenjohtaja
- Erja Kinnunen, Valtori, ryhmän varapuheenjohtaja
- Hellevi Huhanantti, Väestörekisterikeskus
- Juha Tallinen, Pääesikunta
- Laura Kujala, Pääesikunta
- Toni Äikäs, valtiovarainministeriö
- Laura Kiviharju, Viestintävirasto
- Tuomo Salminen, Valtiontalouden tarkastusvirasto
- Timo Larmela, Aalto-yliopisto
- Mika Kuronen, sisäasiainministeriö

Ohje on laadittu virkatyönä ryhmän toimesta. Ohjeen luonnos oli julkisella lausuntokierroksella 13.6.2014 – 8.8.2014. Saadut lausunnot käsiteltiin työryhmän sisällä ja otettiin huomioon ohjeessa. VAHTI-johtoryhmä päätti ohjeen julkaisemisesta marraskuussa 2014 pidetyssä kokouksessaan

1 Johdanto

Tämä ohje on tarkoitettu tietoturvallisuuden arviointien tukemiseksi valtionhallinnon viranomaisille ja niiden sidosryhmille, kuten palvelutoimittajille.

Viranomaisten tulee varmistaa oman organisaationsa, palveluidensa ja tietoaineistojensa turvallisuus. Sen toteuttamiseksi tulee säännöllisesti arvioida organisaationsa tietoturvallisuuden tilaa sekä toteutettujen tietoturvatoimenpiteiden asianmukaisuutta ja riittävyyttä. Lisäksi tietoturvallisuuden arviointia tulee tehdä aina merkittävien muutosten yhteydessä.

Organisaation johto vastaa sen toiminnasta ja lainmukaisuudesta. Johto on vastuussa myös tietoturvatyön organisoinnista ja resursoinnista. Tietoturvatyön ja toteutettavien kehittämistoimenpiteiden tulee perustua organisaation toiminnan asettamiin vaatimuksiin ja niiden mitoitus tulee pohjautua tietoisuuteen organisaation turvallisuuden tasosta. Tietoturvallisuuden arviointi on myös lainsäädännöllinen velvoite. Lainsäädäntöä käsitellään tämän ohjeen kappaleessa 2 ja valtionhallinnossa käytettyjä arviointiperusteita kappaleessa 3. Kappaleessa 4 kuvataan viranomaisten tietoturvallisuuden arviointiin ja kappaleessa 5 sopimuskumppaneiden arviointiin liittyviä seikkoja, kappale 6 kuvaa niihin liittyviä toimijoita. Kappaleessa 7 kuvataan arviointiprosessin kulkua ja siinä huomioitavia seikkoja.

Ohjeen liitteessä 1 on sanasto, joka kuvaa ohjeessa käytettyjä termejä. Liite 2 luettelee muita arviointeja suorittavia viranomaisia ja liitteessä 3 kuvataan tietojärjestelmän elinkaareen liittyviä arviointeja.

1.1 Tausta

Ohje on suositus valtionhallinnon viranomaisille organisaation oman tietoturvallisuuden ja sen palveluiden sekä palveluita tuottavien ulkopuolisten toimittajien ja palveluita hyödyntävien sidosryhmien tietoturvallisuuden arviointiin.

VAHTI-johtoryhmä on antanut ensimmäisen tietoturvallisuuden arviointia koskevan ohjeensa vuonna 2003, jolloin annettiin suositus tietoturvallisuuden hallintajärjestelmän arvioimisesta. Vuonna 2006 sitä täydennettiin toisella ohjeella, jossa oli mukana tarkistuslistoja arvioimisen tueksi. Osa organisaatioista on panostanut tietoturvallisuuden arviointiin, mutta osalla arviointeja ei ole riittävästi toteutettu. Lähinnä sitä ovat tehneet tietoturvatyötä muutenkin järjestelmällisesti kehittäneet viranomaiset.

Valtionhallinnon tietoturvallisuuden kehittämistä koskeva valtioneuvoston periaatepäätös[1] ohjaa valtionhallinnon tietoturvallisuuden kokonaisuutta, ja siinä päätetään tietoturvallisuuden kehittämisen periaatteista ja painopisteistä sekä linjataan keskeiset suuntaviivat viranomaisten tietoturvatyölle. Kehittämisen painopisteisiin kuuluvat esimerkiksi riskienhallinnan, tietoturvallisuuden hallintajärjestelmän, mittareiden ja seurannan sekä palvelu- ja hankintaketjujen tietoturvallisuuden sekä varautumisen kokonaisvaltainen kehittäminen. Viranomaisilla tulee olla valtiovarainministeriön VAHTI-ohjeisiin, tietoturvatasomäärityksiin ja varautumistoiminnan vaatimuksiin perustuvat suunnitelmat, ohjeet ja menettelyt, joita arvioidaan keskitetysti.

Vuonna 2010 tuli voimaan tietoturvallisuusasetus (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, 681/2010) ja sen tueksi annettiin Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010, jossa kuvattiin tietoturvatasojen vaatimukset. Yhtenä vaatimusalueena tietoturvatasoissa on Toiminnan arviointi ja todentaminen, jossa tietoturva-auditointien tekeminen on vaatimuksena jo tietoturvallisuuden perustasolla. Tämä vaatimus sekä tarve tietoturvatason todentamiseen ovat lisänneet arviointeja merkittävästi asetuksen voimaantulon jälkeen. Lisäksi yleinen tietoturvatietoisuuden kasvu ja tietoturvauhkien lisääntyminen ovat kasvattaneet tarvetta arvioinneille.

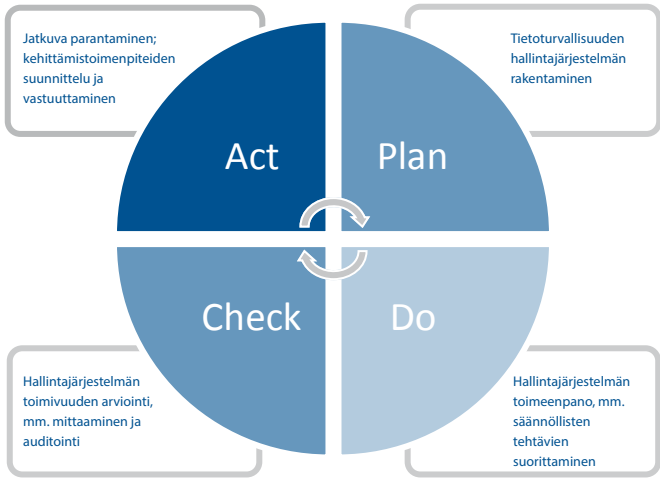
Vaikka arvioinnit ovat lisääntyneet merkittävästi, niin joillakin viranomaisilla on vielä epätietoisuutta siitä, milloin niitä tulisi tehdä, miten, kenen toimesta ja mitä viitekehyksiä arviointiin tulisi käyttää. Tämä ohje pyrkii selventämään näitä kysymyksiä sekä antamaan suosituksia arviointien suorittamiseen.

1.2 Arvioinnin hyödyt organisaatiolle

Tietoturvallisuuden arviointi on väline organisaation tietoturvallisuuden johtamiseen ja kehittämiseen. Se tukee organisaation tavoitteiden toteuttamista kun arvioinnin kohteet valitaan oikein, eli kohdentamalla arvioinnit organisaation toiminnan kannalta tärkeimpiin kohteisiin. Arvioinnin tuloksena johto saa tietoa tietoturvatoiminnan tilasta ja suosituksia tietoturvallisuuden kehittämiseksi. Arvioinnin tuloksena saadaan myös tietoa siitä, mitkä ovat organisaation tietoturvatoiminnan vahvuudet ja hyvin hoidetut alueet. Hyvä tietoturvallisuuden hallinnan kehittäminen noudattaa jatkuvan parantamisen periaatetta: suunnittele – tee – arvioi/mittaa – paranna (PDCA). Sisäisten ja ulkoisten arviointien avulla organisaatio saa tarvittavaa tietoa toiminnan jatkuvan parantamisen toteuttamiseen.

[1] Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä, VAHTI 7/2009, 26.11.2009.

Kuvio 1. Tietoturvallisuuden PDCA-malli



1.3 Edellytykset tietoturvallisuuden arvioinnille

Arviointien avulla organisaatio saa hyvää tietoa tietoturvallisuutensa kehittämiseen, mutta jo ennen arviointitoiminnan aloittamista on suositeltavaa huolehtia tietyistä tietoturvallisuuden perusasioista. Tietoturvallisuuden keskeiset viitekehykset edellyttävät, että tietoturvatyö on hallittua, säännöllistä ja dokumentoitua. Tietoturvallisuusasetuksen tietoturvatasojen tai ISO27001-standardin[2] vaatimukset voidaan toteuttaa hallintamallin/hallintajärjestelmän avulla (ISMS, Information Security Management System). Organisaation tulee laatia oman tietoturvallisuuden hallintajärjestelmänsä kuvaus, jonka keskeiset dokumentit ovat tietoturvapolitiikka ja –strategia, tietoturvakäytännöt, -periaatteet ja ohjeet, kehittämissuunnitelma, tietoturva-arkkitehtuurit, riskienhallinnan kuvaus, jatkuvuus- ja valmiussuunnitelmat, tietoturvaraportointi ja auditointisuunnitelma. sisältöä on kuvattu tarkemmin VAHTI:n yleisohjeessa.[3]

On suositeltavaa, että ennen ulkoisen arvioinnin tilaamista organisaatio suorittaa kohteeseen itsearvioinnin. Sen avulla organisaatio voi huolehtia siitä, että suurimmat puutteet voidaan korjata jo etukäteen ja ulkoinen arviointi on näin ollen järkevää suorittaa.

Kullekin arvioinnin kohteelle tulee löytyä siitä vastuullinen taho, jonka toimintaan ja tietojenkäsittelyyn suojattava kohde liittyy. Vastuullista tahoa voidaan kutsua myös termillä ”omistaja”. Hän vastaa suojattavan kohteen kehittämisestä ja on siten vastuussa myös sen tietoturvallisuudesta ja pääsääntöisesti myös siihen liittyvistä kustannuksista.

ISO/IEC 27001 Tietoturvallisuuden hallintajärjestelmää koskeva kansainvälinen standardi

[3] Tietoturvallisuudella tuloksia, yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007

Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä, palvelu tai toimitila. Vastuullisella taholla on tärkeä rooli tietoturvallisuuden arvioinnissa, koska yleensä hän vastaa arvioinnin tilaamisesta ja sen kustannuksista – silloinkin kun sen tekninen toteutusvastuu mahdollisesti on järjestelmän teknisellä ylläpitäjällä tai palvelutoimittajalla.

1.4 Arviointityypit

Organisaation tietoturvallisuutta voidaan arvioida useilla tavoilla ja eri malleilla. Arvioinnit voidaan jakaa suorittajan mukaan seuraavasti:

Arviointitapa	Kuvaus
Itsearviointi	Arvioinnin kohteen vastuuhenkilön tai työryhmän toteuttama arviointi. Vastuuhenkilö ei välttämättä ole tietoturvahenkilöstöä.
Sisäinen arviointi	Organisaation tietoturvahenkilöstön tai asiantuntijoiden toteuttama arviointi.
Sisäinen tarkastus	Organisaation oma järjestelmällinen ja riippumaton arviointi.
Vertaisarviointi	Arvioijina toimivat henkilöt, jotka työskentelevät samankaltaisen kohteen parissa toisessa organisaatiossa tai yksikössä.
Ulkoinen arviointi	Organisaation ulkopuolisen, riippumattoman toimijan suorittama arviointi.

1.5 Erilaiset arviointikohteet

Kohteesta riippuen arvioinnit voidaan jakaa karkeasti teknisiin ja hallinnollisiin. Teknisissä arvioinneissa tarkastellaan teknisten järjestelyiden riittävyyttä ja vaatimustenmukaisuutta, hallinnolliset arvioinnit kohdistuvat toimintaprosesseihin ja menettelytapoihin. Arvioinnit ovat harvoin luonteeltaan täysin teknisiä, koska myös teknisissä arvioinneissa on aiheellista tarkastella teknisen ympäristön hallinta- tai ylläpitoprosesseja – hyväkään tekninen taso ei säily hyvänä elleivät kyseiset prosessit ole kunnossa. Myös esimerkiksi toimitilojen arviointiin kuuluu sekä teknistä että hallinnollista arviointia.

Arvioinneissa täytyy aina olla joku viitekehys tai vaatimuskokonaisuus, jonka pohjalta arviointi toteutetaan. Hallinnollisissa arvioinneissa viitekehys voi olla esim. sopimus, tietoturvastandardi tai valtionhallinnon viitekehys, kuten tietoturvatasot. Teknisissä arvioinneissa viitekehyksenä voi toimia esim. uuden järjestelmän vaatimusmäärittely, jokin vaatimuskriteeristö tai kansainvälinen suositus. Tietojärjestelmien viranomais- ja arviointilaitosarvioinnissa voidaan käyttää luvussa 3 kuvattuja arviointiperusteita. Arvioinnin tilaaja määrittelee arviointiperusteet, mutta niitä valittaessa on huomioitava arvioinnin kohteeseen liittyvät sopimukset ja mahdolliset lakisääteiset vaatimukset. Tiedon luokitus on tärkeä tekijä silloin kun valitaan esim. sovellettavaa tietoturvatasoa tai KATAKRI:n tasoa.

Viranomaisten oman toiminnan tai omien järjestelmien lisäksi arvioinnin kohteina ovat usein kaupallisilta tahoilta hankitut palvelut. Niiden arviointi perustuu vaatimusmäärittelyihin, sopimuksiin sekä sopimusten liitteinä oleviin palvelukuvauksiin ja palvelutasosopimuksiin. Erityisesti turvallisuussopimuksella liitteineen on tässä keskeinen merkitys.

1.6 Arviointikohteen valinta ja rajaus

Organisaation tulee määrittää toiminnoilleen ja tietojärjestelmilleen tärkeysluokitus[4], jonka perusteella arvioinnit saadaan kohdistettua tärkeimpiin kohteisiin. Tärkeysluokitukseen perustuen määritellään miten usein ja minkä kriteerien mukaan auditointeja suoritetaan. Hyvä lähtökohta kuitenkin on, että kaikki tärkeät järjestelmät auditoidaan ennen tuotantokäytön aloittamista, sekä merkittävien muutosten (mm. teknologia- tai arkkitehtuurimuutokset, uudet toiminnallisuudet, suuremmat versionvaihdot, muutokset vaatimuksissa) yhteydessä. Kriittisiä järjestelmiä on lisäksi syytä auditoida myös säännöllisin väliajoin, vaikka merkittäviä muutoksia ei olisikaan tapahtunut, Säännölliset arvioinnit toteutetaan organisaation auditointisuunnitelman mukaisesti.

Arvioinnin laajuus (scope) kuvaa niitä osia jotka sisältyvät arviointiin, rajaukset poikkeuksia edelliseen. Arvioinnin laajuus määritellään kohteen kriittisyyden, käytössä olevien resurssien ja muiden rajaavien tekijöiden, kuten teknisen valmiuden mukaan.

Teknisissä tarkastuksissa on olennaista tunnistaa

1. palvelun varsinaiseen tuottamiseen vaadittavat komponentit (esim. verkkolaitteet, palvelimet, sovellukset) sekä
2. palvelun tuottamiseen käytettävät muut tukikomponentit (esim. verkkolaitteet, palvelimet/palvelut, työasemat, sovellukset).

Ensimmäiseen kohtaan sisältyy kaikki, mitä palvelun tuottamiseksi vaaditaan, ml. edustapalvelimet, tunnistus- ja yhteyspalvelut, sovelluspalvelimet, tietokannat jne. eli kaikki mitä perinteisesti lasketaan sisältyvän itse palveluun. Toinen kohta taas sisältää kaiken muun tarkastuksen kohteeseen liittyvän, kuten esimerkiksi ylläpitotyöasemat ja hyppypalvelimet, etäyhteyspalvelut, valvonta- ja varmistuspalvelut, mahdolliset NTP-, proxy-, DNS/DHCP- ja levypalvelut sekä virtuaalipalvelinten hallintaympäristöt. Palvelun tuottamiseen käytettävät komponentit tulee mahdollisuuksien mukaan ottaa kokonaisuudessaan mukaan arvioinnin piiriin. Toisesta ryhmästä taas tulee arvioida miltä osin ne on syytä ja mahdollista ottaa mukaan. Arviointiin tulisi sisällyttää sellaiset osuudet, joilla pystytään merkittävästi vaikuttamaan arvioinnin kohteen tietoturvallisuuteen, esimerkkeinä etäylläpitoon käytettävät laitteet, järjestelmiin muutosten tekemisen mahdollistavat valvontajärjestelmät, salassa pidettäviä tietoja sisältävät varmistukset jne. Arvioinnin ulkopuolelle jätettävät osuudet perusteluineen tulee kirjata rajauksiin.

Hallinnollisissa arvioinneissa tulee tunnistaa ne organisaation osat, toimijat ja prosessit, jotka ovat arvioinnin kohteen kannalta merkityksellisiä. Jos esimerkiksi tutkitaan käyttövaltuushallinnan vaatimusten toteutumista palvelussa, kiinnostavia eivät ole organisaation konsernitason ohjeet ja linjaukset, vaan ainoastaan kyseisessä palvelussa noudatettava prosessi.

[4] Apuväline tärkeysluokituksen tekoon löytyy esimerkiksi Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012 liitteestä 4.

Arvioinneista voidaan rajata ulos sinänsä selkeitä osuuksia jos asialle on hyvät perustelut, kuten että kyseinen osuus on jo tarkastettu toisen arvioinnin yhteydessä, se tullaan arvioimaan myöhemmin, tai jos kyseisen osuuden turvallisuus on jo varmistettu muulla keinoin, kuten sertifioinnilla tai itsearvioinnilla. Näissä tilanteissa on kuitenkin olennaista, että asia kuvataan selkeästi arvioinnin rajauksiin.

2 Tietoturvallisuuden arviointiin liittyvä lainsäädäntö

2.1 Tietoturvallisuutta koskeva lainsäädäntö

2.1.1 Laki viranomaisten toiminnan julkisuudesta

Julkisuuslain (621/1999) 18 §:ssä säädetään viranomaisten velvollisuudesta noudattaa hyvää tiedonhallintatapaa, joka tarkoittaa asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä, suojaamisesta ja eheydestä huolehtimista. Viranomaisten asiakirja- ja tietohallintoon kohdistuva hyvän tiedonhallintatavan suunnittelu- ja toteuttamisvelvoite sisältää mm. vaatimuksen asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suojan, eheyden ja laadun turvaamisesta asianmukaisin menettelytavoin ja tietoturvallisuusjärjestelyin.

Hyvän tiedonhallinnan käsitteen avulla on pyritty liittämään yhteen viranomaisten tietoaineistoihin liittyvien erilaisten intressien huomioon ottamista koskevat velvoitteet. Tällaisia ovat asiakirjojen julkisuus ja salassapito, arkistointi, henkilötietojen suoja ja tietojen käyttörajoitukset sekä tietoturvallisuus. Viranomaisen tulee muun muassa laatia kuvaukset tietojärjestelmistään ja selvittää tietojärjestelmien käyttöönoton yhteydessä suunniteltujen toimenpiteiden vaikutukset asiakirjojen julkisuuteen, salassapitoon ja suojaan sekä ryhtyä tarpeellisiin toimenpiteisiin asiakirjojen ja tietojärjestelmien sekä niihin liittyvien tietojen suojan järjestämiseksi. Tietojen suoja, eheys ja laatu tulee turvata asianmukaisin menettelytavoin ja tietoturvajärjestelyin huomioiden tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja toimenpiteistä aiheutuvat kustannukset.

2.1.2 Julkisuuslain perusteella annetut asetukset

Julkisuusasetuksessa (Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta, 1030/1999) täsmennetään julkisuuslaissa säädetyn hyvän tiedonhallintatavan toteuttamista. Asetuksen mukaan viranomaisen on hyvän tiedonhallintatavan toteuttamiseksi selvitettävä ja arvioitava tietojen saatavuuteen, käytettävyyteen, laatuun ja suo-

jaan sekä tietojärjestelmien turvallisuuteen vaikuttavat uhat sekä niiden vähentämiseksi ja poistamiseksi käytettävissä olevat keinot sekä niiden kustannukset ja muut vaikutukset.

Tietoturvallisuusasetuksessa (valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, 681/2010) puolestaan kuvataan asiakirjojen käsittelyä koskevat yleiset tietoturvavaatimukset sekä luokiteltujen asiakirjojen käsittelyvaatimukset, joita valtionhallinnon viranomaisten tulee noudattaa. Yleiset tietoturvavaatimukset velvoittavat viranomaisen muun muassa kartoittamaan toimintaan liittyvät tietoturvallisuusriskit, huolehtimaan riittävästä asiantuntemuksesta tietoturvallisuuden varmistamiseksi sekä estämään tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely käyttöoikeushallinnalla, käytön valvonnalla sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä sekä muilla toimenpiteillä. Turvallisuustoimenpiteiden tulee kattaa kaikki asiakirjan käsittelyvaiheet ja velvoitteita on noudatettava myös silloin, kun tiedonkäsittelytehtävää hoidetaan viranomaisen toimeksiannosta.

2.1.3 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Kansainvälisiä tietoturvallisuusvelvoitteita koskevassa laissa (588/2004) säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Tällaisilla velvoitteilla tarkoitetaan Suomea sitovaan kansainväliseen sopimukseen sisältyvää määräystä sekä muuta Suomea koskevaa velvoitetta liittyen erityissuojattavan aineiston suojaamiseen[5]. Laissa säädetään turvallisuusviranomaisten tehtävistä ja erityissuojattavan aineiston suojaamista koskevista tietoturvallisuustoimenpiteistä.

Erityissuojattavaan aineistoon on merkittävä turvallisuusluokkaa koskeva merkintä ja noudattaa vastaavaa luokkaa koskevia käsittelyvaatimuksia.

2.2 Tietoturvallisuuden arviointia koskeva lainsäädäntö

Tietoturvallisuutta koskevassa lainsäädännössä ei ole asetettu yleistä velvoitetta hakea tietojärjestelmille tai muulle tiedonkäsittelylle viranomaishyväksyntää, vaan tietoturvallisuuden arviointi perustuu edellä kuvatun hyvän tiedonhallintatavan ja tietoturvallisuusasetuksen vaatimuksiin. Tietyissä tilanteissa tiedonkäsittely kuitenkin edellyttää viranomaishyväksyntää. Tällaisia vaatimuksia liittyy erityisesti kansainvälisiin tietoturvallisuusvelvoitteisiin. Esimerkiksi EU:n turvallisuusluokiteltuja tietoja sisältävien tietojärjestelmien on läpikäytävä hyväksymisprosessi, jossa pyritään varmistumaan siitä, että kaikki asiaankuuluvat turvatoimet on pantu täytäntöön ja riittävä turvataso on saavutettu[6]. Lisäksi Suomea sitovat turvallisuusluokitellun tiedon suojaamista koskevat valtiosopimukset edellyttävät pääsääntöisesti henkilöiden ja yritysten turvallisuusselvityksiä

[5] Erityissuojattavalla tietoaineistolla tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, niissä olevia tietoja sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu. Suomea sitovat voimassa olevat valtiosopimukset löytyvät kansallisen turvallisuusviranomaisen (NSA) Internet-sivuilta (http://formin.finland.fi/Public/default.aspx?nodeid=47189&contentlan=1&culture=fi-FI).

[6] Euroopan Unionin neuvoston päätös i (2013/488/EU).

turvallisuusluokasta III (Luottamuksellinen/Confidential) ylöspäin sekä määrättyjen turvallisuusviranomaisten (Designated Security Authority, DSA) välistä sopimusta, jos tietoa siirretään valtioiden välillä sähköisessä muodossa.

Tietoturvallisuuden viranomaisarviointia edellytetään myös hallituksen esityksessä laiksi julkisen hallinnon turvallisuusverkkotoiminnasta (HE 54/2013, 31 §).

2.2.1 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden arvioinnista

Tietojärjestelmien arviointimenettelystä säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa (1406/2011). Laissa on osoitettu viranomaisille menettely, jonka avulla ne voivat saada luotettavan arvioinnin käyttämiensä tietojärjestelmien tietoturvallisuuden tasosta, ja siinä säädetään Viestintäviraston tehtävistä sekä arvioinneissa käytettävistä arviointiperusteista. Lain perusteella Viestintävirasto voi arvioida viranomaisten tietojärjestelmiä ja tietoliikennejärjestelyjä sekä antaa todistuksen vaatimukset täyttävistä järjestelmistä

Viranomainen voi pyytää Viestintävirastolta sen määräämisvallassa olevan tai hankittavan tietojärjestelmän tietoturvallisuuden arviointia ja hyväksymistä osoittavan todistuksen antamista vaatimukset täyttävälle järjestelmälle. Lain tarkoituksena on muun muassa se, että viranomaiset voivat saada Viestintävirastolta ulkopuolisen arvion kriittisistä järjestelmistä. Tällaiset järjestelmät sisältävät korkeimpien turvallisuusvaatimusten piiriin kuuluvia tietoaineistoja, joiden käsittelyyn ja siirtoon liittyvää arviointia on ongelmallista antaa yksityisten arviointilaitosten tehtäväksi[7]. Viranomainen voi siten antaa korkeampien suojaustasojen tietoja sisältävien järjestelmien arvioinnin Viestintävirastolle ja harkintansa mukaan tilata alempien suojaustasojen arvioinnit tietoturvallisuuden arviointilaitokselta.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011) mukaan valtiovarainministeriö voi pyytää Viestintävirastolta selvitystä valtionhallinnon viranomaisten tietojärjestelmien yleisestä tietoturvallisuuden tasosta. Valtiovarainministeriöllä on salassapitosäännösten estämättä oikeus saada tieto arvioinnin lopputuloksista.

2.2.2 Laki tietoturvallisuuden arviointilaitoksista

Tietoturvallisuuden arviointilaitostoiminnasta säädetään laissa tietoturvallisuuden arviointilaitoksista (1405/2011), jossa määritellään arviointilaitosten hyväksymiskriteerit ja tehtävät. Lain tarkoituksena on edistää yritysturvallisuutta luomalla valvontamenettely yritysten tietoturvallisuutta arvioiville laitoksille. Vaikka yrityksiä koskevan turvallisuusselvityksen laatiminen kuuluukin viranomaiselle, yritykset voivat nykyistä paremmin varautua osallistumaan esimerkiksi kansainvälisiin ja kansallisiin hankintakilpailuihin, joissa edellytetään viranomaisen laatimaa turvallisuusselvitystä. Tällöin yritysturvalli-

[7] Viestintävirasto hyväksyy tietoturvallisuuden arviointilaitoksille suojaustasoittain pätevyysalueet, joiden mukaisia arviointeja laitos voi suorittaa. Pätevyys voidaan myöntää suojaustasoille ST IV ja ST III.

suusselvitystä tai tietojärjestelmän hyväksyntää koskeva todistus voidaan antaa arviointilaitoksen tekemän arvioinnin pohjalta. Myös viranomaiset voivat käyttää hyväksytyn arviointilaitoksen suorittamaa arviointia tietoturvallisuuden tason arvioinnissa.

Arviointilaitoksen[8] hyväksyminen edellyttää, että laitos on riippumaton arvioinnin kohteesta, laitoksen henkilökunnalla on hyvä tekninen ja ammatillinen koulutus, riittävän laaja-alainen kokemus arviointitehtävistä sekä toiminnan edellyttämät laitteet ja järjestelmät. Lisäksi laitoksen oman tiedonkäsittelyn tulee täyttää viranomaisvaatimukset ja sillä tulee olla asianmukaiset toimintaa ja sen seurantaa koskevat ohjeet. Vaatimusten täyttyminen todennetaan kansallisen akkreditointiviranomaisen FINAS-akkreditointipalvelun sekä Viestintäviraston toimesta, ja hyväksymismenettelyssä sovelletaan kansainvälisiä pätevyyden todentamista koskevia standardeja[9]. Hyväksyntäprosessia kuvataan tarkemmin Viestintäviraston antamassa ohjeessa[10].

2.2.3 Turvallisuusselvityslaki

Turvallisuusselvityslain (726/2014) tarkoituksena on parantaa mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita, yleistä turvallisuutta tai muuta niihin verrattavaa yleistä etua taikka erittäin merkittävää yksityistä taloudellista etua. Laissa säädetään näiden etujen suojaamiseksi toteutettavista henkilö- ja yritysturvallisuusselvityksistä. Henkilöturvallisuusselvityksellä tarkoitetaan henkilön luotettavuuden varmistamista, yritysturvallisuusselvityksellä yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimista. Laissa luetellaan ne tehtävät, joita hoitavista voidaan pyytää henkilöturvallisuusselvitys sekä säädetään edellytykset yritysturvallisuusselvitysten hakemiselle.

Yritysturvallisuusselvitystä voi hakea se, joka tarvitsee selvitystä laissa säädetyn tai kansainvälisessä tietoturvallisuusvelvoitteesta johtuvan velvoitteen noudattamiseksi sekä viranomainen, valtionhallinnon hankinnoista vastaava yksikkö taikka valtionhallinnolle yhteisiä tai laajaan käyttöön tarkoitettuja tieto- ja viestintekniikkapalveluja tuottava yksikkö, joka luovuttaa selvityksen kohteelle suojaustasoille I-III luokiteltuja asiakirjoja[11]. Yritysturvallisuusselvitys toteutetaan turvallisuusselvityslain 37 §:n mukaisten tietolähteiden sekä yritykseen ja sen toimitiloihin sekä sen tietojärjestelmiin ja tietoliikennejärjestelyihin kohdistuvan tarkastuksen avulla.

---

8 Viestintävirasto ylläpitää listaa hyväksytyistä arviointilaitoksista http://www.viestintavirasto.fi

9 SFS-EN ISO/IEC 17021:2011 Vaatimustenmukaisuuden arviointi. Vaatimukset johtamisjärjestelmiä auditoiville ja sertifioiville elimille. Conformity assessment. Requirements for bodies providing audit and certification of management systems, ISO 27006 standardi ISO/IEC 27006:2011 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems sekä Viestintäviraston ohje tietoturvallisuuden arviointilaitoksille.

10 Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset 1.10.2014

11 Myös tietyillä valvontaviranomaisilla on mahdollisuus hakea yritysturvallisuusselvitystä yrityksestä, joka harjoittaa ydinvoima- tai räjähdysaineisiin liittyvää toimintaa tai on osallistumassa aliurakoitsijana hankkeeseen, jossa sillä tai sen työntekijöillä on pääsy tällaista toimintaa koskeviin tietoihin taikka tiloihin tai alueelle. Lisäksi julkisissa puolustus- ja turvallisuushankinnoissa selvitys voidaan hakea kansainvälisistä tietoturvallisuusvelvoitteista annetun lain perusteella (vrt. 2.1.3).

2.3 Julkisia hankintoja koskeva lainsäädäntö

Julkisista hankinnoista annetussa laissa (348/2007, hankintalaki) ja julkisista puolustus- ja turvallisuushankinnoista annetussa laissa (1531/2011, puolustus- ja turvallisuushankintalaki) säädetään vaatimuksista, joita hankintayksikkö voi asettaa tarjouskilpailuun osallistujalle ja tarjouskilpailun voittaneelle tarjoajalle. Hankintalain mukaisissa kilpailutuksissa tietoturvavaatimusten on liityttävä hankinnan kohteeseen. Toimittajan organisaatiolle ei siis voida hankintalain perusteella asettaa tietoturvavaatimuksia muuten kuin hankinnan kohteen osalta. Puolustus- ja turvallisuushankintalain mukaan tietoturvavaatimusten on perustuttava viranomaiselle asetettujen tietoturvavelvoitteiden toteuttamiseen, mutta laki ei edellytä, että tietoturvavaatimusten olisi suoraan liityttävä hankinnan kohteeseen. Vaatimusten tulee kuitenkin olla syrjimättömiä ja niistä on ilmoitettava tarjouspyynnössä.

Hankintayksikkö voi edellyttää henkilö- ja yritysturvallisuustodistusta tai muita sitoumuksia tai tietoja, jotka liittyvät turvallisuusluokitellun tiedon käsittelyyn, säilyttämiseen, tuhoamiseen sekä luovuttamiseen. Sitoumukseen liittyy usein tilojen, toimintatapojen ja prosessien tarkastus, joita hankintayksikkö voi tehdä itse tai pyytää muilta hankintayksiköiltä tietoja tarjoajan kyvystä suoriutua vaatimuksista.

Kun hankinnan kohteena on tietojärjestelmä tai tietoliikennejärjestely, hankintayksikkö määrittelee tarjouspyyntö- ja sopimusasiakirjoihin liittyvissä teknisissä kuvauksissa hankintaa koskevat tarkoituksenmukaiset tietoturvavaatimukset[12], jotka määräytyvät tietojärjestelmässä käsiteltävien salassa pidettävien tietojen tai jatkuvuudelle asetettujen tarpeiden perusteella. Hankinnan yhteydessä tulee sopia myös niistä menettelyistä, joilla järjestelmälle asetetut vaatimukset todennetaan.

Edellä mainituissa hankintalaeissa on säädetty yleisistä ja erityisistä soveltamisalaa koskevista poikkeuksista (7§), joiden perusteella hankintalakien ulkopuolelle jäävät mm. kynnysarvojen alittavat pienhankinnat, salassa pidettävät, tutkimus- ja kehittämispalveluja koskevat sekä viranomaisten väliset hankinnat. Vaikkei näissä hankinnoissa järjestetä hankintalakien mukaista tarjouskilpailua, on tarjous- ja sopimusasiakirjoissa kuitenkin huomioitava tietoturvavaatimukset sen mukaisesti, mitä salassa pidettävää tietoa palveluntoimittajalle luovutetaan.

Kappaleessa 5 käsitellään vaatimuksenmukaisuuden arviointia toimeksiantosuhteissa.

[12] Myös tietyillä valvontaviranomaisilla on mahdollisuus hakea yritysturvallisuusselvitystä yrityksestä, joka harjoittaa ydinvoima- tai räjähdysaineisiin liittyvää toimintaa tai on osallistumassa aliurakoitsijana hankkeeseen, jossa sillä tai sen työntekijöillä on pääsy tällaista toimintaa koskeviin tietoihin taikka tiloihin tai alueelle. Lisäksi julkisissa puolustus- ja turvallisuushankinnoissa selvitys voidaan hakea kansainvälisistä tietoturvallisuusvelvoitteista annetun lain perusteella (vrt. 2.1.3).

2.4 Tietoturvallisuuden ohjausta koskeva lainsäädäntö

Valtiovarainministeriöstä annetun asetuksen[13] mukaan valtiovarainministeriö vastaa julkisen hallinnon tietoturvallisuuden yleisestä kehittämisestä sekä valtionhallinnon tietoturvallisuuden ohjauksesta. Valtiovarainministeriön tehtävänä on lisäksi julkishallinnon viranomaisten tietohallinnon yleinen ohjaus[14] sekä valtion yhteisten tieto- ja viestintäteknisten palvelujen varautumisen, valmiuden ja turvallisuuden ohjaus[15]. Tällaisia ovat perustietotekniikkapalvelut sisältäen laitteet, ohjelmistot sekä tietoliikenne- ja viestintäpalvelut; tietojärjestelmäpalvelut, jotka tukevat julkisen hallintotehtävän tai organisaatioiden samankaltaisen toiminnan hoitamista sekä sähköisen asioinnin ja hallinnon tukipalvelut.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011) mukaan valtiovarainministeriö voi pyytää valtionhallinnon Viestintävirastolta selvitystä valtionhallinnon viranomaisten tietojärjestelmien yleisestä tietoturvallisuuden tasosta. Valtiovarainministeriöllä on salassapitosäännösten estämättä oikeus saada tieto arvioinnin lopputuloksista.

Valmiuslain (1552/2011) mukaisesti valtiovarainministeriö voi määrätä poikkeusoloissa valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tietoturvallisuuden järjestämisestä.

---

13 Valtioneuvoston asetus valtiovarainministeriöstä (610/2003)

14 Laki julkisen hallinnon tietohallinnosta (634/2011)

15 HE laiksi valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (HE 150/2013)

3 Viranomaisten tietoturvallisuuden arviointi

3.1 Hallinnollisen tietoturvallisuuden arviointi

Hallinnollisissa arvioinneissa tarkastellaan viranomaisten tietoturvallisuuden hallintajärjestelmän kattavuutta ja toimivuutta. Arviointi kohdistuu toimintaprosesseihin ja menettelytapoihin. Hallinnolliset arvioinnit suoritetaan haastatteluiden ja havainnoinnin avulla sekä tarkastamalla dokumentaatiota, kuten ohjeistuksen kattavuutta. Viranomaisten hallinnollisissa arvioinneissa käytetään usein viitekehyksenä VAHTI-ohjeita ja tietoturvatasoja, mutta hallintajärjestelmän arviointia tehdään myös esimerkiksi ISO/IEC 27001 standardin tai muun viitekehyksen mukaisesti.

Hallinnollinen tietoturva-arviointi käynnistyy yleensä viranomaisen omasta aloitteesta, mutta velvoite siihen voi tulla myös toiselta viranomaiselta. Tällainen velvoite on asetettu esimerkiksi valtion tieto- ja viestintätekniikkakeskuksen Valtorin palveluihin liittyville asiakkaille sekä valtiovarainministeriön tietoturvatasojen yhteishankkeiden osallistujille.

Hallinnollisen tietoturvallisuuden itsearviointi säännöllisin väliajoin on tietoturvallisuuden jatkuvan kehittämisen kannalta suositeltavaa. ISO/IEC 27001 -standardin mukaan sertifioitu hallintajärjestelmä edellyttää vuosittaista itsearviointia. Myös viranomaisten väliset vertaisarvioinnit ovat hyödyllisiä ja suositeltavia. Niissä kaksi tai useampi organisaatiota suorittaa toisen viranomaisen tietoturvallisuuden arvioinnin hyödyntäen näin toisen organisaation osaamista ja resursseja.

3.2 Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden arviointi

Viranomaisten käytössä olevien tietojärjestelmien arviointi tehdään ja arvioinnin perusteella annettava todistus annetaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa kuvatun menettelyn mukaan. Viranomaisen on suositeltavaa tärkeysluokituksen ja riskiarvioinnin perusteella valita toimintansa kannalta kriittiset tietojärjestelmät, joihin kohdistuu tietoturva- ja/tai varau-

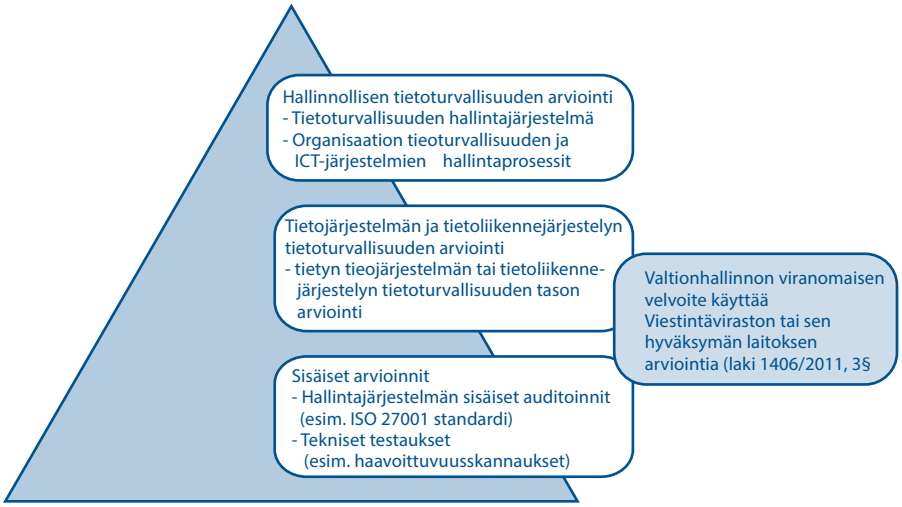
tumisvaatimuksia, sekä teettää näihin järjestelmiin tietoturvallisuuden ulkoinen arviointi. Tarpeen mukaan tulee edellyttää, että järjestelmä täyttää kaikki arviointiperusteen mukaiset vaatimukset, jolloin arvioinnin perusteella voidaan myöntää todistus. Arviointi voidaan toteuttaa hankittavana olevan järjestelmän osalta käyttöönottovaiheessa. Jos kyse on jo käytössä olevasta järjestelmästä, voidaan arvioinnilla selvittää, miltä osin se täyttää vaadittua tietoturvallisuuden tasoa koskevat vaatimukset.

Tietojärjestelmien arviointia koskevan lain mukaisia arviointeja voivat tehdä Viestintävirasto sekä sen hyväksymät tietoturvallisuuden arviointilaitokset. Ainoastaan Viestintävirasto voi antaa viranomaisen tietojärjestelmistä kansainvälisissä tietoturvavelvoitteissa edellytettävän todistuksen. Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä ulkoiseen arviointiin 1.6.2015 lähtien vain tämän lain menettelyä. Velvoitteella varmistetaan se, että valtionhallinnon viranomaiset käyttävät vain luotettavia ulkopuolisia tietoturvallisuuden arviointipalveluja, jotka hoitavat arviointitehtävää julkisena hallintotehtävänä. Tavoitteena on, että valtionhallinnon viranomaisten tietojärjestelmien arvioinnit toteutettaisiin yhtenäisillä menettelytavoilla. Siten toimeksiantaja saisi arvioinnista aiheutuvia kustannuksia vastaavan hyödyn valtionhallinnon tietoturvallisuuden kehittämiseen yhtenäisellä tavalla.

Viranomaiset voivat kuitenkin osana normaalia toiminnan kehittämistä tehdä itse sisäisiä arviointeja, itsearviointeja tai tietojärjestelmien teknistä testausta. Ohjattuja sisäisiä arviointeja ja itsearviointeja voidaan myös hankkia ulkopuolisilta palveluntuottajilta käyttäen esimerkiksi Valtorin kilpailuttamia ja tuottamia asiantuntijapalveluita.

Yhteiskäyttöisten tietojärjestelmien arvioinnissa tulee mahdollisuuksien mukaan tehdä yhteistyötä eri viranomaisten välillä ja välttää päällekkäisiä arviointeja.

Kuvio 2. Viranomaisten tietoturvallisuuden arviointi



4 Tietoturvallisuuden arviointi-perusteet

Tietoturvallisuuden arviointiperusteilla tarkoitetaan niitä tietoturvallisuutta koskevia vaatimuksia, joiden perusteella tietoturvallisuuden arviointi suoritetaan. Ne valitaan arvioinnin kohteesta riippuen tapauskohtaisesti, ja ne perustuvat lainsäädäntöön, sopimuksiin ja niihin kirjattuihin tietoturvavelvoitteisiin tai yleisesti tunnettuihin hyviin käytäntöihin.

4.1 Arviointilakien mukaiset arvioinnit

Arviointiperusteina voidaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annetun lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti käyttää:

1. lailla tai asetuksella säädettyjä viranomaisen toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;
2. kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvavelvoitteiden toteuttamista koskevia ohjeita;
3. Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia ohjeita;
4. julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita; ja
5. vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.

Edellä kohdassa 1 tarkoitetaan pääasiassa tietoturvallisuusasetuksen 5§ tietoturvatasovaatimuksia, joita on täsmennetty valtiovarainministeriön ohjeilla. Asetuksen täytäntöönpanoa koskevia VAHTI-ohjeita sovelletaan tietoturvallisuuden arviointiperusteena silloin, kun arvioinnin kohteessa käsitellään Suomen viranomaisen salassa pidettävää tietoa jonka salassapito perustuu julkisuuslakiin.

Kun määräysvalta salassa pidettävään tietoon on toisen valtion viranomaisella, siellä kotipaikkaansa pitävällä yrityksellä, kansainvälisellä järjestöllä tai toimielimellä, ja Suo-

mella on tietoturvallisuusvaltiosopimus kyseisen valtion tai toimielimen kanssa, sovelletaan tiedon salassapitoon ja tietoturvatoimenpiteisiin lakia kansainvälisistä tietoturvallisuusvelvoitteista. Tiedon käsittelyyn sovelletaan tällöin kansallisten tietoturvavaatimusten lisäksi kansainväliseen tietoturvavelvoitteeseen, eli valtiosopimukseen tai muuhun Suomea koskevaan velvoitteeseen, sisältyviä määräyksiä. Erityissuojattavaa tietoaineistoa eli kansainvälisen velvoitteen mukaisesti turvallisuusluokiteltuja asiakirjoja käsiteltäessä on pidettävä huolta, että tietoaineiston suojaamisesta voidaan huolehtia koko elinkaaren ajan sen turvallisuusluokkaa vastaavalla tavalla. Erityissuojattava tietoaineisto on säilytettävä tiloissa, joissa asiakirjojen ja niihin sisältyvien tietojen suojaamisesta voidaan huolehtia valtiosopimuksessa edellytetyllä tavalla. Erityissuojattavan tietoaineiston käsittely edellyttää viranomaishyväksyntää.

4.2 Kansainväliset turvallisuusvelvoitteet

Kansainvälisen erityissuojattavan tietoaineiston käsittelyssä tulee noudattaa Suomea koskevia kansainvälisiä velvoitteita, joita ovat esimerkiksi:

- EU Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (2013/488/EU)
- NATO:n turvallisuussäännöstö ”Security within the North Atlantic Treaty Organisation, Document C-M(2002)49, 17.6.2002” liitteineen ja direktiiveineen, erityisesti ”NATO Security Committee Directive on the Security of Information AC/35-D/2002-REV3”
- muut EU ja NATO-säädökset
- Suomen kahden- ja monenväliset tietoturvallisuussopimukset (GSA, General Security Agreement)[16]

Edellä mainitut vaatimukset ovat varsin yleisellä tasolla ja ne edellyttävät, että käsittelyssä noudatetaan kansallisia lakeja ja asetuksia, sekä kansallisen viranomaisen antamia ohjeita.

Suomessa toimivaltaisena kansallisena viranomaisena toimii ulkoasiainministeriöön sijoitettu kansallinen turvallisuusviranomainen, NSA-yksikkö (National Security Authority). Se on antanut seikkaperäisen ohjeen kansainvälisen luokitellun aineiston käsittelystä [17].

Kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvien tietoturvavaatimusten todentamisessa käytetään apuna kansallista turvallisuusauditointikriteeristöä (KATAKRI). Kyseistä kriteeristöä käytetään arviointityökaluna silloin kun tarkoituksena on todentaa, täyttävätkö viranomaisten ja yritysten tietojärjestelmät ja toiminta niiltä edellytettävät kansainväliset tietoturvavelvoitteet.

---

[16] Suomen solmimat voimassa olevat tietoturvallisuussopimukset löytyvät kansallisen turvallisuusviranomaisen (NSA) internet-sivuilta http://www.formin.finland.fi.

[17] Kansainvälisen turvallisuusluokitellun tiedon käsittelyohje, päivitetty 10.2.2014.

Jotkut turvallisuusviranomaiset käyttävät KATAKRI:n kriteereitä omalla päätöksellään myös palvelutoimittajiensa tai omien tietojärjestelmiensä auditointiin.

4.3 Tietoturvallisuusasetuksen tasovaatimukset

Aluksi on huomattava, että yleisesti käytettävät kriteeristöt poikkeavat toisistaan tasovaatimuksiltaan ja käyttötarkoitukseltaan. Tietoturvallisuusasetuksen mukaiset käsittelyvaatimukset ovat tarkoituksenmukaisuus- ja kustannussyistä jossain määrin lievemmät kuin esimerkiksi jotkin EU:n neuvoston turvallisuussäännön vaatimukset.

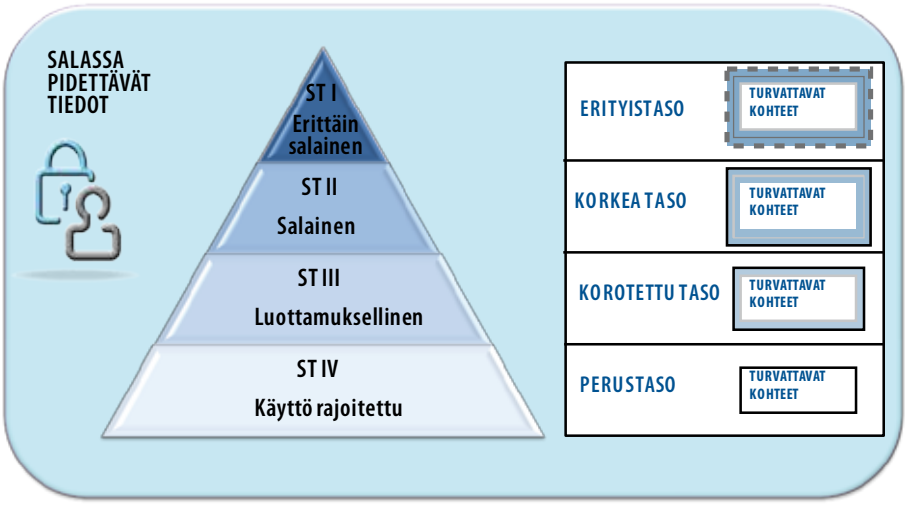
Tietoturvallisuusasetuksen 5 §:ssä on asetettu valtionhallinnon viranomaisille **tietoturvallisuuden perustason** vaatimukset (Liite 4). Niistä konkreettisista toimenpiteistä, joita tietoturvallisuuden perustason toteuttaminen edellyttää, annetaan tarkemmat määrittelyt valtiovarainministeriön VAHTI-ohjeistuksessa. Asetuksen 23 §:n mukaan viranomaisen tietojenkäsittely on saatettava vastaamaan asetuksen 5 §:ssä säädettyjä perustason tietoturvavaatimuksia. Vaatimus koskee kaikkia valtionhallinnon viranomaisia, mutta sen todentamiseen asetus ei ota kantaa.

Tietoturvallisuusasetuksen **korotettua tasoa ja korkeaa tasoa koskevat** vaatimukset ovat yhteydessä asiakirjojen suojaamista koskeviin vaatimuksiin. Kun suojaustasoon ST II – III kuuluvia asiakirjoja tai suojaustasoon ST IV kuuluvia arkaluonteisia henkilötietoja tai biometrisiä tunnistetietoja sisältäviä henkilörekisteriin talletettuja asiakirjoja talletetaan (16 §) tai siirretään (19 §), vaatimukset kohdistuvat valtionhallinnon viranomaisten tietoverkkoon ja tietojenkäsittelyn kokonaisuuteen. Asetuksen mukaan viranomaiset voivat sallia esim. suojaustasoon ST III kuuluvan asiakirjan tallettamisen ja siirtämisen salaamattomana mikäli tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät korotetun tason vaatimukset. ST II edellyttää vastaavasti korkeaa tietoturvatasoa. Salaamis- ja suojaamistarvetta sekä turvatoimenpiteiden laajuutta on kuitenkin arvioitava mm. riskienhallinnan menettelyiden ja toimenpiteistä aiheutuvien kustannusvaikutusten näkökulmasta. Korotetun ja korkean tason arvioinneissa on siten painotettava tietojenkäsittelyn kokonaisuutta, eikä välttämättä kaikkien yksittäisten vaatimusten toteutumista. Arvioinnin kohteen omistaja tekee viime kädessä päätöksen riittävän tason saavuttamisesta ja hyväksyy yksittäisten tietoturvavaatimusten toteuttamatta jättämiseen liittyvät jäännösriskit.

Vaatimus korotetun ja korkean tietoturvallisuustason toteuttamisesta kohdistuu erityisesti yhteiskunnan kannalta elintärkeisiin tietojenkäsittely-ympäristöihin ja niistä vastaaviin valtionhallinnon viranomaisiin.

Riippumatta korotetun ja/tai korkean tason vaatimuksen täyttymisestä, viranomaisten on kuitenkin saatettava asetuksen 23.4 §:n siirtymä-säännöksen mukaisesti luokiteltujen asiakirjojen käsittely vastaamaan asetuksen 4 luvussa säädettyjä vaatimuksia viiden vuoden kuluessa siitä, kun se on päättänyt luokitella tietoaineistonsa.

Kuvio 3. Tiedon luokituksen ja tietoturvatason vastaavuus



4.4 ICT-varautumisen vaatimukset

VAHTI 2/2012 ICT-varautumisen vaatimukset –ohje kuvaa yhden viitekehyksen, jota voidaan käyttää vaatimustenmukaisuuden arvioinnissa.

ICT-varautuminen tarkoittaa riskienhallintaan pohjautuvaa ICT-toiminnan jatkuvuuden hallintaa ja tiedon turvaamista niin normaaliolojen häiriötilanteissa kuin poikkeusoloissa. ICT-varautumisessa näkökulmana on palvelujen ja toimintojen jatkuvuus sekä käytettävyys, kun taas tietoturvatasovaatimusten tavoitteena on tiedon luottamuksellisuuden, eheyden ja osin saatavuuden turvaaminen. Niiden tasot voivat poiketa toisistaan, sillä esimerkiksi joissain toiminnoissa tiedot voivat olla julkisia, mutta palveluilta edellytetään korkeaa käytettävyyttä.

ICT-varautumisen vaatimuksia kannattaa käyttää viitekehyksenä ennen kaikkea silloin kun viranomaiset toteuttavat itse tai kilpailuttavat yhteiskunnan toimivuuden kannalta kriittisiä palveluita.

4.5 Muut valtionvarainministeriön antamat ohjeet

Tietoturvaturvallisuusasetuksen 4 §:ssä säädetään kymmenen vaatimusta tietoturvallisuuden perustasolle. Näitä vaatimuksia täsmentää ja täydentää VAHTI-ohje 2/2010, jossa tietoturvatasojen kaikkien kolmen tason vaatimukset on kuvattu yksityiskohtaisesti. Nämä vaatimukset kohdistuvat menettelytapoihin ja prosesseihin eikä niiden perusteella voida tehdä päätöksiä teknisistä yksityiskohdista ja ratkaisuista, joiden avulla tasovaatimukset voidaan täyttää. Tämän seikan korjaamiseksi tietoturvatasot on huomioitu kai-

kissa asetuksen voimaantulon jälkeen julkaistuissa VAHTI-ohjeissa, joissa annetaan vaatimuksia ja suosituksia eri tietoturvatasoilla sovellettavista ratkaisuista.

Tietoturvatasovaatimuksia toteutettaessa ja arvioitaessa on huomioitava VAHTI 2/2010 -ohjeen lisäksi erityisesti seuraavat ohjeet:

- VAHTI 3/2010 Sisäverkko-ohje
- VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje
- VAHTI 3/2012 Teknisen ympäristön tietoturvataso-ohje
- VAHTI 1/2013 Sovelluskehityksen tietoturvaohje
- VAHTI 2/2013 Toimitilojen tietoturvaohje
- VAHTI 4/2013 Henkilöstön tietoturvaohje
- VAHTI 5/2013 Päätelaitteiden tietoturvaohje

Kappaleessa 7.1 kuvataan tarkemmin ICT-hankintoja ja sovelluskehitystä koskevien ohjeiden käyttöä palveluiden tuottamisessa ja niiden arvioinnissa.

5 Vaatimustenmukaisuuden arviointi toimeksiantosuhteissa

Julkisuuslain mukaisesti viranomainen voi antaa tiedon salassa pidettävästä asiakirjasta toimeksiannon suorittamista tai muuten lukuunsa suoritettavaa tehtävää varten, jos se on välttämätöntä tehtävän suorittamiseksi. Tällöin on kuitenkin ennakolta varmistuttava siitä, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti, mikä voi tapahtua tarjouskilpailuun osallistujalta vaadittavin sitoumuksin tai tietoturvallisuustason todentamisella arvioinnin avulla. Arviointi- tai auditointioikeus on kirjattava sopimuksiin ja arviointi tulee pohjautua sopimuksiin kirjattuihin tietoturvavelvoitteisiin.

Valtionhallinnon viranomaisen on suunniteltava ja toteutettava tietoturvatoimenpiteet siten, että ne kattavat kaikki asiakirjojen käsittelyvaiheet niiden laatimisesta tai vastaanottamisesta arkistointiin tai hävittämiseen, mukaan lukien asiakirjan luovuttaminen ja siirtäminen sekä käsittelyn valvonta. Suunnittelussa on myös huolehdittava siitä, että tietojenkäsittelyä koskevia velvoitteita noudatetaan silloinkin, kun tietojenkäsittelytehtävää hoidetaan viranomaisen toimeksiannosta. Valtionhallinnon viranomaisen on siis varmistuttava siitä, että taho, jolle se toimeksiannon perusteella luovuttaa salassa pidettäviä tietoa, noudattaa tietoturvallisuusasetuksen mukaisia velvoitteita. Toimenpiteet, joilla käsittelysääntöjen noudattaminen varmistetaan, voivat riippua sopijakumppanista sekä siitä, millaisia vaatimuksia sopijakumppanin on lain perusteella noudatettava.

Toimeksiannolla tarkoitetaan erityisesti viranomaisten hankintoja ja muita vastaavia toimeksiantosuhteita viranomaisen ja yksityisen yrityksen, palvelukeskuksen tai toisen viranomaisen välillä. Tietoturvallisuusasetuksen mukaisia velvoitteita on noudatettava riippumatta siitä, onko kyseessä hankintalakien mukaisesti kilpailutettu hankinta vai muu ostopalvelu tai sopimussuhde, jonka toteuttamiseksi luovutetaan tai jota toteutettaessa syntyy salassa pidettävää tietoa.

Viranomainen voi luovuttaa tietoja ulkopuolisille myös ilman sopimussuhdetta. Tällaisia tilanteita ovat esimerkiksi virka-aputehtävään liittyvä ja laissa säädetyn tiedonsaantioikeuden perusteella tapahtuva tietojen luovutus. Viranomaisen on ennen tietojen antamista varmistuttava, että virka-avun antaja huolehtii asianmukaisesti tietojen salassapidosta ja suojaamisesta. Kun viranomainen luovuttaa tietoja taholle, jolla on laissa säädetty tiedonsaantioikeus, on tietoja pyytävän viranomaisen esitettävä selvitys tiedon käyttötarkoituksesta sekä perusteesta, jonka mukaan salassa pidettävä tieto voidaan luovuttaa. Lisäksi pyytäjän on tarvittaessa esitettävä selvitys siitä, että salassa pidettävien tietojen suojaus järjestetään asianmukaisesti. Selvitys voidaan ottaa huomioon tehtäessä tietojen luovutusta

koskeva kirjallinen päätös. Nämä tilanteet poikkeavat kuitenkin toimeksiantoon perustuvasta tietojen luovuttamisesta ja sopimukseen perustuvien tietoturvallisuusmenettelyiden todentamisesta, joita käsitellään seuraavaksi.

5.1 Yksityiset yritykset sopijakumppanina

Yksityiset yritykset ja muut vastaavat toimijat eivät pääsäännön mukaan ole velvoitettuja noudattamaan julkisuuslain hyvää tiedonhallintatapaa tai tietoturvallisuusasetuksen vaatimuksia ilman erillistä sopimusta. Tietoturvavaatimukset on siis huomioitava hankinta- tai muussa sopimuksessa ja tämä voidaan toteuttaa turvallisuussopimusmenettelyllä. Sopimusmenettelyä ja –malleja on kuvattu ohjeissa VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje ja VAHTI 2/2013 Toimitilojen tietoturvaohje. Myös ICT-varautumisen vaatimukset on huomioitava sopimuksessa, jos ne liittyvät sopimuksen kohteeseen. Luonnollisesti tulee huomioida myös organisaation oma hankintoja koskeva ohjeistus.

Tietoturvavelvoitteiden noudattaminen voidaan todentaa viranomaisen harkinnan mukaan ulkoisella arvioinnilla tai sopijakumppanin itsearvioinnilla, ottaen huomioon salassa pidettävien tietojen määrä ja suojaustasoluokka. Jos tietoja käsitellään sähköisesti, voi todennukseen liittyä myös tietojärjestelmän auditointi. Viranomainen voi edellyttää tarjouskilpailuun osallistujalta tai voittajaksi valitulta tarjoajalta yritysturvallisuusselvitystodistusta. Valtioneuvoston asetuksella voidaan säätää, että valtionhallinnon viranomaisen on hankittava yritysturvallisuusselvitys yrityksestä, jolle valtionhallinnon viranomaisen kanssa tehtävän sopimuksen toteuttamiseksi annetaan suojaustasoluokkaan I—III luokiteltuja asiakirjoja.

5.2 Toinen valtionhallinnon viranomainen sopijakumppanina

Valtionhallinnon viranomaisten on noudatettava tietoturvallisuusasetuksen velvoitteita. Tällaisena viranomaisena pidetään valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia. Viranomaisten välinen toimeksianto- tai palvelusopimus on kyseessä esimerkiksi silloin, kun palvelukeskus tai muu vastaava viranomainen tuottaa keskitetysti toisille viranomaisille palveluja taikka kun yksittäinen viranomainen tuottaa toiselle viranomaiselle palvelua[18].

Valtionhallinnon viranomaisten välisissä sopimuksissa sopijapuolet toteavat minkä suojaustason mukaista tietoa sopimuksen perusteella luovutetaan, tai jos kyseessä on tietojärjestelmää taikka tietoliikennejärjestelyä koskeva sopimus, minkä suojaustason mukaisia vaatimuksia järjestelmään sovelletaan. Tietoturvavaatimusten noudattamisen todentamiseksi tietoja luovuttava taho voi pyytää selvityksen siitä, että tietoja vastaanottava taho tuntee käsittelysäännöt ja käsittely-ympäristössä noudatetaan soveltuvaa tietoturvallisuuden tasoa. Tietoturvallisuuden tason noudattaminen voidaan tarpeen mukaan osoittaa

[18] Kansainvälisen turvallisuusluokitellun tiedon käsittelyohje, päivitetty 10.2.2014.

myös tiedon vastaanottavan tahon teettämää tietoturvataso- tai tietojärjestelmäarviointia koskevalla raportilla. Jos esimerkiksi valtionhallinnon palvelukeskus hankkii palvelua kaupalliselta palvelutoimittajalta, se voi suorittaa palvelun tietoturvallisuuden arvioinnin ennen palvelun käyttöönottoa. Muilla palvelua käyttävillä viranomaisilla ei silloin lähtökohtaisesti ole tarvetta suorittaa tietoturvallisuuden arviointia uudelleen.

Koska valtionhallinnon viranomaiset noudattavat suoraan lain perusteella tietoturvavaatimuksia ja ovat siis lain velvoittamina vastuussa tietoturvatoimenpiteiden toteuttamisesta, ei vaatimusten noudattamisesta ole tarpeen sopia yhtä kattavalla turvallisuussopimusjärjestelyillä kuin yksityisten yritysten kanssa. Viranomaisten välisiin sopimusjärjestelyihin tulee siksi soveltaa kevyempiä tietoturvallisuuden todentamismenettelyjä ja päällekkäisiä turvallisuusselvityksiä sekä tietoturvallisuusarviointeja on vältettävä.

5.3 Sopijakumppanina julkisuuslain mukainen viranomainen

Valtionhallintoon kuulumattomat viranomaiset eivät ole velvoitettuja noudattamaan tietoturvallisuusasetusta, mutta niiden on kuitenkin noudatettava julkisuuslakia mukaan lukien sen säännökset ja hyvä tiedonhallintatapa. Julkisuuslain soveltamisalaan kuuluvia ovat muun muassa valtion liikelaitokset, kunnalliset viranomaiset sekä julkisoikeudelliset laitokset. Näiden tahojen ollessa sopimuskumppanina, on valtionhallinnon viranomaisen varmistuttava sopimusteitse, että tietoturvallisuusasetuksen vaatimukset täyttyvät. Sopimuksen sisältö ja laajuus voi kuitenkin riippua sopimusosapuolesta, sillä osa näistä tahoista voi noudattaa tietoturvallisuusasetuksen vaatimuksia vapaaehtoisesti, jolloin turvallisuussopimusta ei välttämättä ole tarpeen tehdä samassa laajuudessa kuin yksityisten yritysten kanssa. Vaatimusten todentamisessa voidaan käyttää apuna ulkoista arviointia tai itsearviointia valtionhallinnon viranomaisen harkinnan mukaan.

5.4 Sopijakumppanina ulkomainen toimija

Viranomaisen tulee varmistua tietoturvavaatimusten noudattamisesta ja asiakirjoja käsittelevien henkilöiden luotettavuudesta myös silloin, kun tietoja luovutetaan ulkomaille. Kun sopijapuolena on ulkomainen taho, riippuu turvallisuussopimukseen liittyvän tarkastusoikeuden toteuttaminen siitä, mitä salassa pidettävää tietoa sopijakumppanille luovutetaan. Turvallisuusluokiteltujen tietojen suojaamista koskevissa valtiosopimuksissa voidaan edellyttää henkilö- ja yritysturvallisuusselvitysten laatimista ennen tiedon luovuttamista.

Jos kyse on asiakirjoista, johon on tehty tietoturvallisuusasetuksen 11 §:n mukainen turvallisuusluokitusta koskeva merkintä, voidaan ulkomaisen tahon arvioinnissa hyödyntää turvallisuusviranomaisorganisaatiota ja pyytää sopijatahon sijaintivaltion kansalliselta turvallisuusviranomaiselta yritys- ja henkilöturvallisuusselvitykset. Jos käsiteltävä tieto on muuta salassa pidettävää tietoa (esimerkiksi liikesalaisuudet tai arkaluontoiset henkilötiedot), on turvallisuusvaatimusten todentaminen ja mahdollisuudet arvioinnin suorittami-

seen ulkomailla arvioitava tapauskohtaisesti viranomaisen harkinnan perusteella. Jos vaatimusten noudattamisesta ei voida riittävällä tavalla varmentua, on harkittava, voidaanko salassa pidettävää tietoa ylipäätään luovuttaa ulkomaille.

6 Ulkoisiin arviointeihin osallistuvat tahot

Tässä luvussa on kuvattu viranomaisarviointeihin osallistuvat tahot ja niiden roolit. Muita tietoturvallisuuteen liittyviä arviointeja ja tarkastuksia suorittavia viranomaisia on kuvattu liitteessä 2.

6.1 Viestintävirasto ja tietoturvallisuuden arviointilaitokset

Viestintävirasto arvioi viranomaisten pyynnöstä niiden määräämisvallassa olevia tai hankittavaksi suunniteltavien tietojärjestelmien vaatimuksenmukaisuutta sekä tekee valtiovarainministeriön pyynnöstä selvityksiä viranomaisten tietojärjestelmien yleisestä tietoturvallisuuden tasosta. Viestintäviraston hyväksyntä tietojärjestelmälle on haettava silloin kun kansainvälinen tietoturvavelvoite edellyttää toimivaltaisen turvallisuusviranomaisen hyväksyntää. Lisäksi arvio ja tarpeen mukaan hyväksyntä voidaan hakea myös muulle tietojärjestelmälle, jos sitä edellytetään esimerkiksi viranomaisen riskienarvioinnin tai hallinnonalakohtaisen ohjeistuksen perusteella. Turvallisuusviranomaisen arviointi on ulkopuolinen arviointi, jonka perusteella annetaan viranomaistodistus, jos tietoturvallisuutta koskevat vaatimukset täyttyvät.

Arviointitoimintaa harjoittava yritys tai palvelutehtäviä julkishallinnolle tarjoava yksikkö voi hakea toiminnalleen Viestintäviraston hyväksynnän. Arviointitoiminta ei ole luvan- tai ilmoituksenvaraista toimintaa, mutta valtionhallinnon viranomaiset voivat käyttää 1.6.2015 lähtien tietojärjestelmiensä ja tietoliikennejärjestelyidensä ulkoisessa arvioinnissa Viestintäviraston lisäksi vain sen hyväksymiä arviointilaitoksia.

Arviointilaitoksen tulee arvioinnissa selvittää, onko arvioinnin kohteen toiminnassa asianmukaisella tavalla toteutettu arviointiperusteina käytetyt tietoturvallisuutta koskevat vaatimukset. Arviointilaitoksen tulee toiminnassaan noudattaa lainsäädännössä, akkreditoinnissa sovellettavissa standardeissa, Viestintäviraston ohjeissa ja arviointilaitoksen hyväksymispäätöksessä asetettuja vaatimuksia. Viestintävirasto valvoo hyväksyttyjen laitosten toimintaa.

Hyväksytty tietoturvallisuuden arviointilaitos hoitaa arviointilaitostehtäviä tehdessään julkista hallintotehtävää ja se toimii riippumattomana arvioijana. Laitoksen suorittama arviointi on ulkoinen arviointi, jonka avulla arvioinnin toimeksiantaja voi osoittaa ulkopuolisille kohteen vaatimuksenmukaisuuden. Tällaista arviointia voidaan hyödyntää

esimerkiksi tietojärjestelmän hyväksyntä- tai vastaanottotarkastuksessa todentamaan, että tietojärjestelmälle asetetut tietoturvavaatimukset on toteutettu sovitulla tavalla. Arviointilaitoksen antaman todistuksen perusteella voidaan hakea myös edellä mainittu viranomaishyväksyntä. Toimivaltainen turvallisuusviranomainen voi hyväksyntää varten tarvittaessa suorittaa tarkentavia arviointeja tai pyytää arvioinnin kohteelta lisäselvitystä sen selvittämiseksi ja varmistamiseksi, että arvioinnin kohde täyttää soveltuvat tietoturvavaatimukset. Tietoturvallisuuden arviointilaitoksen arviointia voidaan käyttää myös sidosryhmien arviointiin, kun viranomainen edellyttää yhteistyökumppanilta ulkoista arviointia.

6.2 Turvallisuusselvityslain mukaan toimivaltaiset viranomaiset

Ulkoasiainministeriön NSA-yksikön lisäksi kansainvälisten tietoturvallisuusvelvoitteiden täytäntöönpanoa tukevat määrätyt turvallisuusviranomaiset (Designated Security Authority, DSA), joita Suomessa ovat puolustusministeriö, pääesikunta ja Suojelupoliisi. Ne huolehtivat muun muassa henkilöiden ja elinkeinonharjoittajien luotettavuuden selvittämisestä. Viestintävirasto toimii Suomen määrättynä turvallisuusviranomaisena ja kansallisena tietoliikenneturvallisuusviranomaisena (National Communications Security Authority, NCSA), joka vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. Viestintävirasto toimii viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen hyväksyntäviranomaisena sekä vastaa tietoturvallisuuden arviointilaitosten hyväksymisestä, ohjaamisesta ja valvonnasta. Lisäksi Viestintävirasto laatii yritysturvallisuusselvitystä varten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen.

6.3 Valtiovarainministeriö ja VAHTI

Valtiovarainministeriö vastaa valtion tietoturvallisuuden yleisestä ohjauksesta ja koordinoi hallinnon organisaatioiden toimintaa kansallisessa ja kansainvälisessä tietoturvayhteistyössä. Valtiovarainministeriön ohjausroolia on vahvistettu viimeaikaisen lainsäädännön, kuten valmiuslain (1552/2011), lain julkisen tietohallinnon ohjauksesta (634/2011) sekä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuuden arviointia koskevan lain myötä. Valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämistä koskeva laki (1226/2013) ja asetus (132/2014) sekä eduskunnan käsiteltävänä oleva hallituksen esitys eduskunnalle laiksi julkisen hallinnon turvallisuusverkkotoiminnasta (HE 54/2013) täsmentävät ja vahvistavat tätä. Niin ikään yhteiskunnan turvallisuusstrategia ja kyberturvallisuusstrategia sekä muut valtioneuvoston päätökset vahvistavat tätä roolia. Valtiovarainministeriössä näistä tehtävistä vastaa ylimmän johdon alaisuudessa toimiva Julkisen hallinnon tieto- ja viestintätekninen toiminto (JulkICT).

Valtiovarainministeriö voi tietoturvallisuuden arviointilain 5 § mukaan pyytää Viestintävirastoa laatimaan selvityksen valtionhallinnon viranomaisten tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta. Selvityksen piiriin tulevat

tietojärjestelmät voidaan määritellä tietojärjestelmien käyttötarkoituksen, niihin talletettavien tietojen laadun tai muun vastaavan yleisen tekijän mukaan. Valtionvarainministeriö on kartoittanut selvityksen piiriin otettavat tietojärjestelmät, ja Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI tukee ministeriötä arviointikohteiden valinnassa ja priorisoinnissa.

Valtionvarainministeriön pyytämissä arvioinneissa ensisijaisina kohteina ovat keskeiset valtion johtamiseen tarkoitetut järjestelmät ja tietoverkot, keskeiset tietovarannot sekä hallinnon yhteiset, keskeiset salausratkaisut.

7 Arviointien suorittaminen

7.1 Hankkeiden elinkaaren aikaiset arvioinnit

7.1.1 Tietojärjestelmähankkeiden arviointi

Tietojärjestelmähankkeiden arviointiin on luotu valtionhallinnon yhteinen arviointikehikko[19]. Sen mukainen arviointi on tarkoitettu tehtäväksi esiselvitysvaiheen jälkeen, kun toteutettavasta ratkaisusta ja toteutukseen liittyvästä kokonaisuudesta on olemassa vähintään alustava suunnitelma.

Arviointikehikossa arvioitavia osa-alueita ovat:

1. Vaikuttavuus ja asiakashyödyt
2. Tehokkuus, tuottavuus ja taloudellisuus
3. Osaaminen ja resursointi
4. Yhteentoimivuus
5. Toteutettavuus

Arviointikehikon liitteeksi on tuotettu yhteinen mallipohja kustannus-hyötyanalyyseille[20]. Tarkoituksena on ollut laatia yksinkertainen ja helppokäyttöinen malli, joka samalla asettaa minimivaatimukset. Myös laajempia ja täydellisempiä kustannus-hyötyanalyysejä voi hankevalmistelun yhteydessä tehdä, kunhan mukana on vähintään yhteisen mallin sisältämät asiat. Kustannus-hyötyanalyysin lisäksi arviointikehikon liitteeksi tarvitaan yleensä hanke- tai projektisuunnitelma. Myös muita liitteitä voi olla, koska ideana on se, ettei arviointikehikkoon tarvitse kuvata uudelleen asioita, jotka on jo kuvattu jossain muualla.

Arviointialueeseen 5 (Toteutettavuus) sisältyy tietoturvallisuus. Siellä arvioidaan miten tietoturva-, varautumis- ja tietosuojavaatimuksia on hankkeen valmistelun yhteydessä selvitetty, ja miten ne näkyvät hankkeen suunnittelussa.

---

19 https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20110527Valtio/name.jsp.

20 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20131023Mallip/name.jsp

Hankkeen valmisteluvaiheessa tehtävän hankearvioinnin tavoitteena on osaltaan varmistaa, että

- käynnistetään vain sellaisia hankkeita, joilla on onnistumisen edellytykset,
- kustannukset ja hyödyt on realistisesti arvioitu ja hyötyjen realisointi suunniteltu ja
- kehitettävät ratkaisut ovat yhteentoimivia.

Virastoja suositellaan arvioimaan kehikon avulla kaikki sellaiset toiminnan kehittämishankkeet, joihin sisältyy tietojärjestelmien kehittämistä. Arviointi voidaan toteuttaa ulkoisena tai itsearviointina, mutta merkittäville hankkeille suositellaan ulkoista arviointia. Tietohallintolaki[21] edellyttää, että merkittävistä tietojärjestelmähankinnoista on pyydettävä valtiovarainministeriön lausunto. Koska hankintoja tehdään yleensä hankkeissa, niin tällöin lausuntomenettelyssä on mielekästä tarkastella koko hanketta eikä vain pelkkää hankintaa. Lausunnon edellytyksenä on yhteisen arviointikehikon mukainen arviointi ja arviointiraportti.

7.1.2 Tietoturvallisuuden arviointi järjestelmähankkeissa

Tietojärjestelmähankkeissa auditointimahdollisuus tulee varmistaa etukäteen jo ennen hankkeen käynnistämistä. Hallinnollinen ja tekninen auditointioikeus tulee ulottaa koko suojattavaa tietoa käsittelevään ja sen turvallisuuteen vaikuttavaan kokonaisuuteen tiedon ja järjestelmän koko elinkaaren ajan. Jos toteutustyö ostetaan ulkopuoliselta toimittajalta, auditointioikeus on kirjattava kilpailutusasiakirjoihin ja sopimuksiin. Tarpeen mukaan toimittajan tietoturvamenettelyitä voidaan auditoida jo ennen sopimuksen allekirjoittamista jolloin se on huomioitava kilpailutusasiakirjoissa. Tietoturvallisuuden varmistamisessa etupainotteisuus on tärkeää ja kustannustehokasta. Tarkempaa ohjeistusta aiheesta antaa VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje.

Uusien tietojärjestelmien vaatimusmäärittelyissä on tärkeää määritellä järjestelmien kriittisyys ja niissä käsiteltävien tietojen luokitus. Niillä on merkittävä vaikutus toteutukselle asetettaviin vaatimuksiin ja sitä kautta sen sisältöön ja kustannuksiin. Lisäksi on huomioitava, että joissakin teknisissä ratkaisuissa, esim. salaustuotteissa ja hajasäteilyssä, kansalliset ja kansainväliset vaatimukset poikkeavat toisistaan. Toteutuksen arvioinnissa kriteeristönä tulee käyttää sille hankintavaiheessa asetettuja vaatimuksia.

Tietojärjestelmähankkeissa auditointeja tulee tehdä monessa eri vaiheessa, auditointien määrä ja laajuus päätetään sovelluksen kriittisyyden ja tavoiteltava tietoturvatason mukaan organisaatiokohtaisten menettelytapojen ja ohjeistuksen mukaisesti. Tyypillisiä auditointikohteita ja vaiheita ovat:

- Vaatimusmäärittelyn auditointi/arviointi
- Toteutuksen auditointi valituissa tarkistuspisteissä
- Auditointi käyttöönottovaiheessa tehtävä ennen tuotantoon siirtoa

[21] Laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011).

- Merkittävissä muutoksissa tehtävä auditointi
- Säännöllinen, auditointisuunnitelman mukaan tehtävä uusinta-auditointi.

VAHTI 1/2013 Sovelluskehityksen tietoturvaohje kuvaa käyttöönottovaiheessa tehtävää tietoturva-auditointia seuraavasti: Korotetun tason sovelluksen tietoturvallisuus on auditoitava ennen käyttöönottoa. Tämä on pakollinen vaatimus korotetulla ja korkealla tietoturvatasolla. Auditoinnissa on käytettävä sekä automaattisia että manuaalisia menetelmiä. Auditoijan on oltava ulkoinen, riippumaton osapuoli. Auditointi koostuu seuraavista vaiheista:

- Tekninen auditointi, jossa testataan tietoturvakontrollien toimivuus tunkeutumistestauksen keinoin
- Hallinnollinen auditointi, jossa tarkastetaan sovelluksen operointi- ja ylläpitoprosessit jne.
- Arkkitehtuurin auditointi, jossa tarkastetaan sovelluksen arkkitehtuuri tietoturvanäkökulmasta.

Jos tuotetaan korkean tason sovellusta, niin sen tietoturvallisuus on auditoitava myös sovelluskehityksen aikana sille määriteltyjen tarkastuspisteiden yhteydessä. Näin varmistutaan siitä, että kriittiset tietoturvaongelmat havaitaan ja korjataan jo hyvissä ajoin ennen järjestelmän käyttöönottoa.

Luonnollisesti auditoinnit jatkuvat tuotantovaiheessa organisaation laatiman auditointisuunnitelman mukaisesti. Auditointisuunnitelmaa päivitetään vuosittain ja lisätään siihen uudet järjestelmät, joiden auditointisykli valitaan järjestelmän tai sovelluksen tietoturvatason ja kriittisyyden mukaan.

7.2 Arviointia koskeva toimeksianto ja valmistautuminen arviointiin

Arviointi perustuu aina toimeksiantoon, jossa on olennaista määritellä mahdollisimman tarkasti arvioinnin kohde, mukaan lukien arviointiin sisällytettävät alihankkijat tai sidosryhmät (esimerkiksi tietojärjestelmäarvioinnissa eri käyttäjäorganisaatiot). Kohteen laajuudella on luonnollisesti vaikutusta arviointiin kuluvaan aikaan ja kustannuksiin. Lisäksi toimeksiannossa tulisi määritellä sovellettava arviointiperuste sekä tietoturvallisuuden taso. Kun arvioinnin suorittajana on yksityinen yritys, sovitaan arviointiin liittyvistä ehdoista erillisellä sopimuksella. Tilattaessa arviointi tai selvitys viranomaiselta, noudatetaan kyseisen viranomaisen tilausmenettelyjä. Arvioinnin tehostamiseksi voidaan tehdä etukäteinen itsearviointi, jossa arvioinnin kohde vastaa itse tietoturvallisuutta koskeviin vaatimuksiin ja kriteeristöissä esitettyihin kysymyksiin. Huolellinen etukäteisvalmistautuminen lyhentää arviointiin kuluvaa aikaa sekä pienentää arvioinnin kustannuksia[22].

[22] Viestintäviraston tietojärjestelmätarkastuksista lisätietoa ja työkalu tietoturvallisuuden arviointiin tietojärjestelmissä www.viestintavirasto.fi. Viestintävirasto perii arvioinnista maksun valtion maksuperustelain (150/1992) perusteella. Arvioinnin toimeksiantajalla on oikeus saada Viestintävirastolta arvio kustannuksista ennen arvioinnin tilaamista.

7.3 Tietoturva-arviointien suunnittelu ja toteuttaminen

Tietoturva-arvioinnilla selvitetään, täyttääkö valittu kohde sille asetetut vaatimukset, esim. täyttääkö virasto hallinnollisen tietoturvallisuuden perustason vaatimukset tai täyttääkö tietojärjestelmä sille asetetut tekniset tietoturvavaatimukset. Arviointi voi perustua siihen, noudatetaanko arvioinnin kohteessa ennalta annettuja kriteereitä (esimerkiksi tiettyjä säädöksiä, tietyn standardin vaatimuksia tai sisäisiä ohjeita). Arviointi voi ottaa myös kantaa siihen, onko jokin asian tila hyvä tai huono, kuinka merkittävä jokin poikkeama on (esim. uhan todennäköisyys tai vakavuus) jne. Arvioija antaa myös yleensä suosituksia poikkeaman korjaamiseksi.

Arviointiprosessi kattaa tarvittavat toimet arvioinnin suunnittelusta tulosten raportointiin ja seurantaan saakka. Arvioinnin tulosten perusteella voidaan tehdä päätökset siitä mitä toimenpiteitä tulee toteuttaa sekä laatia niille toteuttamissuunnitelmat. Lisäksi tulokset toimivat lähtökohtana seuraavalle arviointikierrokselle. On hyvin tärkeää, että tietoturvallisuuden arviointi on jatkuvaa toimintaa, koska yksittäisen arvioinnin tulos kuvaa arvioitavan kohteen tilaa ainoastaan tietyllä hetkellä.

Kuvio 4. tietoturvallisuuden arviointiprosessi

SFS-EN ISO 19011[23] standardi antaa ohjeistuksen erilaisten johtamis- ja hallintajärjestelmien auditointien toteuttamiseen. Kyseistä ohjeistusta ja siinä määriteltyjä auditointien vaiheita voidaan soveltaa myös tietoturvallisuuden arviointiin kuten luvuissa 7.6 – 7.9 on tehty.

7.4 Tietoturvallisuuden arvioinnin suunnittelu

7.4.1 Arvioinnin suunnittelun aloittaminen

Jokaisella arvioinnilla on tilaaja, joka on useimmiten arvioinnin kohteen omistaja. Arvioinnin suunnittelu aloitetaan yleensä määrittelemällä sen kohde ja suorittaja.

Erilaisia arviointityyppejä on kuvattu luvussa 7.1. Tyypistä riippumatta arviointi kannattaa tehdä ryhmätyönä. Ryhmän kokoonpano riippuu arvioitavasta alueesta; esimerkiksi tehdäänkö arviointi koko organisaation tietoturvallisuudesta vai jostakin rajatusta kohteesta. Tärkeää kuitenkin on, että ryhmässä ovat kattavasti mukana kaikki tarvittavat

[23] SFS-EN ISO 19011 Johtamisjärjestelmän auditointiohjeet, 2011.

tahot ja riittävä kohdealueen osaaminen. Arvioinnin onnistumisen edellytyksenä on, että sille on nimetty vastuullinen vetäjä.

7.4.2 Ensimmäinen yhteydenotto arvioitavaan tahoon

Arvioinnin alkaessa arviointityöryhmän vetäjällä on päävastuu sen suunnittelusta ja läpiviemisestä. Hänen on ryhdyttävä myös konkreettisiin toimiin arviointitapahtuman onnistumisen edellytysten luomiseksi. Käytännössä tämä tarkoittaa yhteydenottoa arvioitavaan tahoon esim. valmistelukokouksen pitämiseksi.

Kokouksen tuloksena laaditaan arviointisuunnitelma, josta näkyvät mm. arvioitavat osa-alueet, täsmälliset päivämäärät, kellonajat ja paikat, arvioitavien osa-alueiden edustajat sekä arvioijat.

7.4.3 Asiakirjojen katselmointi ja arviointiin valmistautuminen

Ennen varsinaista arviointia kohteeseen on perehdyttävä tarkemmin, jotta itse arviointi voidaan viedä tehokkaasti läpi, osataan selvittää merkittävät asiat ja kyetään paremmin ymmärtämään kohdetta sekä saatavien vastausten ja erilaisten havaintojen merkitystä. Samalla saadaan myös yleiskuva dokumentaation kattavuudesta ja pystytään jo tässä vaiheessa havaitsemaan mahdollisia puutteita.

Mikäli samaa kohdetta on arvioitu joskus aikaisemmin, tulee asiakirjojen katselmointiin sisällyttää myös edellisten arviointien loppuraportit ja selvitykset niissä kuvattujen jatkotoimenpiteiden tilasta.

7.4.4 Arviointisuunnitelman laatiminen

Arviointityöryhmän vetäjä laatii saatujen aineistojen ja tietojen perusteella arviointisuunnitelman, joka muodostaa pohjan arvioinnin suorittamiselle. Jos kyseessä on ulkoinen arviointi, suunnitelman laatiminen kuuluu arvioinnin suorittajalle, ei sen tilaajalle.

Arviointisuunnitelma sisältää mm. arvioinnin kohteen ja mahdolliset rajaukset, tavoitteet, käytettävän kriteeristön, aikataulun ja käytettävissä olevat resurssit sekä raportointimenettelyt.

7.5 Tietoturvallisuuden arvioinnin toteuttaminen

7.5.1 Aloituskokouksen pitäminen

Arviointi aloitetaan kokouksella, jossa tyypillisesti esitellään arviointiin osallistuvat henkilöt, arvioinnin kohde ja tarkoitus, käytettävä kriteeristö, aikataulu sekä menettelytavat. Aloituskokoukseen kutsutaan kohteesta vastaava taho ja mahdollisesti kaikki ne henkilöt, joita arvioinnin yhteydessä tullaan haastattelemaan tai joiden aikaa tullaan muuten

merkittävästi käyttämään. Tarkoituksena on varmistaa arvioinnin sujuva läpivienti, kun samoja perusasioita ei tarvitse selvittää uudelleen yksittäisten henkilöiden kanssa.

7.5.2 Tiedon kerääminen ja todentaminen

Arvioijat keräävät tietoa arvioinnin aikana valituilla menetelmillä ja todentavat tietojen paikkansa pitävyyden. Ainoastaan todennettavissa oleva informaatio voidaan hyväksyä arviointinäytöksi.

Tiedonkeruumenetelmiä ovat muun muassa haastattelut, asiakirjojen katselmointi ja havainnointi. Viestintäviraston tai sen hyväksymän tietoturvallisuuden arviointilaitoksen suorittaessa tietojärjestelmän tai tietoliikennejärjestelyn arviointia, arviointimenetelmät perustuvat Viestintäviraston ohjeeseen tietoturvallisuuden arviointilaitoksille, jossa on kuvattu muun muassa hallinnolliselle ja tekniselle todentamiselle asetetut vähimmäisvaatimukset.

Haastatteluissa arvioija voi käyttää ns. avoimia tai suljettuja kysymyksiä. Avoimilla kysymyksillä (esimerkiksi miten, mitä, kuka), saadaan kattavampi kuva siitä, miten kohteessa kysytyn asian osalta toimitaan. Suljetut ”onko”-kysymykset antavat usein vain suppeata kyllä/ei -tietoa ja sisältävät samalla suositeltavan vastauksenkin. Hyvin usein arvioinneissa voidaan hyödyntää tarkistus- ja kysymyslistoja haastattelujen tukena.

Asiakirjakatselmoinnissa sekä tarkastetaan vaatimustenmukaisuuden täyttyminen suhteessa arvioinnissa käytettävään kriteeristöön että kerätään tietoa arvioinnin toteuttamiseksi.

Havaintoja tehtäessä päähuomio kiinnitetään arvioinnin tavoitteiden saavuttamiseen – mitä piti selvittää tai arvioida. Havaintoja voidaan tehdä arvioitavasta kohteesta riippuen esim. asiakirjojen perusteella, haastattelemalla, tutustumiskierroksella näköhavaintoja tekemällä, tietojärjestelmää kokeilemalla ja testaamalla.

Kun havaitaan ilmeinen puute tai poikkeama, on tämä asia hyvä todeta saman tien arvioitavalle, jotta mahdolliset väärinymmärrykset voidaan heti selvittää. Arvioinnin aikana voidaan myös todeta sellaisia pienehköjä puutteita, jotka arvioitava voi laittaa heti kuntoon.

Jos poikkeama on arvioijan mielestä syytä korjata välittömästi, ei ole tarkoituksenmukaista odotuttaa arvioinnin kohdetta virallisen raportin valmistumisella. Kaikki arvioinnin aikana havaitut ja korjatuksi tulleet asiat on kuitenkin kirjattava arviointiraporttiin.

7.5.3 Kriteeristöjen vaatimusten tulkinta

Tietoturvallisuuden viranomaisarvioinneissa käytettävissä kriteeristöissä esitetään usein kysymyksiä toimintaan kohdistuvien lakisääteisten vaatimusten täytäntöönpanosta. Niitä koskevat kysymykset voivat olla yleisellä tasolla olevia ja tulkinnanvaraisia. Tästä johtuen vastauksetkin voivat jäädä yleisellä tasolla oleviksi ja tulkinnanvaraisiksi. On huomioitava, että lainsäädännön täytäntöönpano edellyttää laaja-alaista tulkintaa, joka ei ole välttämättä yksiselitteinen.

Yksittäisten kriteereissä esitettyjen vaatimusten täyttymisen merkitys riippuu siitä, haetaanko arvioinnin perusteella viranomaishyväksyntää. Jos tietojärjestelmälle haetaan

Viestintäviraston todistusta, on käytettävän arviointiperusteen ja kriteeristön mukaisten vaatimusten täytyttävä. Jos hyväksyntä ei ole tarpeen, voidaan arvioinnissa todettu tietoturvallisuuden taso todeta järjestelmää hallinnoivan tahon toimesta riittäväksi, vaikkeivät kaikki yksittäiset vaatimukset täyttyisikään. Jos jotain yksittäistä vaatimusta ei voida esimerkiksi teknisestä syystä täyttää, puutteen korjaamiseksi voidaan toteuttaa ns. korvaavia kontrolleja. Hallinnoiva taho (omistaja) voi riskienhallinnan perusteella päättää, että tietoturvallisuus kokonaisuudessaan on riittävällä tasolla suhteessa suojattaviin intresseihin.

Silloin kun riskienarvioinnin perusteella todetaan, että kaikkien yksittäisten vaatimusten täyttäminen ei ole tarpeellista ja tarkoituksenmukaista, arvioinnista täytyy tuottaa kirjallinen raportti, joka organisaation johdon tulee hyväksyä. Tämä menettely on kuvattu esimerkiksi tietoturvatasojen osalta VAHTI 2/2010 –ohjeen liitteessä 6, Korvaava menettely.

7.6 Tietoturvallisuuden arvioinnin raportointi

7.6.1 Arviointiraportin laatiminen

Arvioijan tulee laatia valmistuneesta arvioinnista raportti, jossa kuvataan arvioinnin kohde, rajaukset ja kulku pääpiirteissään. Tärkein osuus raportissa ovat yksittäiset havainnot ja niiden perusteella annetut suositukset. Lisäksi laaditaan lyhyt yhteenveto, jossa tiivistetyssä muodossa kerrotaan tärkeimmät havainnot. Tämä osuus voidaan esitellä esim. organisaation johdolle.

Raporttiluonnos on hyvä antaa arvioinnin kohteelle etukäteen ennen loppukokousta tutustumista sekä asiavirheiden ja väärinkäsitysten korjaamista varten.

7.6.2 Yksittäisten havaintojen raportointi ja käsittely

Havaintojen kattava ja yhteneväinen raportointi lisää arviointityön ja yksittäisten havaintojen luotettavuutta. Hyvin perusteltu esitys on myös ratkaisevaa kohteen vastuuhenkilön suhtautumisessa tilanteen korjaamiseen. Kattavan raportoinnin osat on esitetty seuraavassa taulukossa.

Kuvattava seikka	Selite
Havainto	Mitä havaittiin, millainen puute tai poikkeama löydettiin
Luokitus	Merkittävyys ja vaikuttavuus
Kriteeri	Mihin velvoitteeseen ja velvoitekohtaan verrattuna havaintoa voidaan pitää puutteena tai poikkeamana
Merkitys	Mitä puutteen tai poikkeaman johdosta voi sattua tai mitä on jo sattunut
Suositus	Mitä puutteen tai poikkeaman korjaamiseksi suositellaan tehtäväksi
Toimenpiteet	Miten arvioinnin kohde suhtautuu havaintoon ja mitä se aikoo asialle tehdä (huom. tekstin laatii arvioinnin kohteen edustaja)

Arvioinnin yksittäiset havainnot (poikkeamat) voidaan sisällyttää arviointiraporttiin omina kokonaisuuksinaan tai ne voidaan raportoida erillisille lomakkeille tai tietojärjestelmään. Tällöin raportissa voidaan viitata poikkeamalomakkeisiin tai järjestelmään.

7.6.3 Arvioinnin johtopäätösten valmistelu

Arviointityöryhmän on hyvä käydä yhdessä läpi arvioinnin havainnot ja verrata niitä arvioinnin tavoitteisiin. Samalla ryhmän tulee päättää annettavista toimenpidesuosituksista sekä seurantatoimenpiteistä, mikäli arviointisuunnitelmassa on näin määritelty. Johtopäätökset pitää valmistella ennen lopetuskokousta.

7.6.4 Lopetuskokouksen pitäminen

Lopetuskokouksessa arviointityöryhmän vetäjä esittelee arvioinnin havainnot, tulokset ja johtopäätökset arvioitavan kohteen edustajille sekä arvioinnin tilaajalle (jos eri kuin kohde). Lisäksi voidaan esittää jatkotoimenpidesuosituksia sekä seurantatoimenpiteitä. Lopetuskokouksessa pyritään hankkimaan arvioinnin kohteen hyväksyntä havainnoille ja sitoutuminen korjaaviin toimenpiteisiin.

7.6.5 Arviointiraportin viimeistely ja jakelu

Raporttiin voidaan lisätä vielä maininta jatkotoimenpiteiden seurannasta ja niiden ajankohdista. Vasta tässä vaiheessa arviointiraportti on viimeistelty ja lopullinen. Virallinen arviointiraportti toimitetaan sovitun jakelun mukaisesti ja myös arkistoidaan.

Arviointien tuloksena syntyneet raportit pitää säilyttää sähköisessä muodossa sovitussa, hyvin suojatussa paikassa. Koska tallennetuilla raporteilla on tärkeä rooli riskienhallinnassa, niihin pitäisi olla pääsy erityisesti organisaation johdolla, arvioidun järjestelmän turvallisuudesta vastaavilla tahoilla sekä tarpeen mukaan tietohallintojohdolla, sisäisellä ja ulkoisella tarkastuksella. Arviointiasiakirjat pitää kirjata diaariin samaan asiaryhmään niin, että ne ovat helposti löydettävissä.

7.7 Arvioinnin seuranta

Arvioinneista on hyötyä vain jos raportissa kuvatut toimenpiteet toteutetaan. Toimivaan arviointiprosessiin kuuluu toimenpiteiden vastuuttaminen, aikatauluttaminen ja seuranta. Jos organisaatiolla on toimiva riskienhallinnasta tai tietoturvallisuudesta vastaava ryhmä, niin toimenpiteiden seuranta voidaan vastuuttaa tälle ryhmälle.

Seurannassa valvotaan, että arvioinnissa havaitut puutteet korjataan. Täyden hyödyn saaminen arvioinnista edellyttää havaittujen puutteiden korjaamista ja arvioinnin toistamista suunnitelmallisesti määrävälein.

Jos kyseessä on organisaation sisäinen arviointi, arviointikohteelta voidaan pyytää arviointiraporttiin kirjallinen vastine. Vastineessa arvioitavan kohteen omistaja ottaa kantaa arvioijan havaintoihin ja suosituksiin sekä kuvaa mitä havaituille puutteille tai poikkeamille aiotaan tehdä. Korjaaminen on kuitenkin aina arvioinnin kohteen ja viime kädessä sen omistajan vastuulla.

Ulkoisen arvioinnin ollessa kyseessä, organisaatio laatii toimenpidesuunnitelman arvioinnin tulosten pohjalta.

Liite 1 Käsitteistö

arviointi (evaluation, assessment)
sen selvittäminen, täyttääkö tietty kohde eri osiltaan sille asetetun tavoitetilan (vaatimukset, suositukset ja parhaat käytännöt). Arviointiprosessi on usein hyväksyntäprosessin osaprosessi.

tarkastus/auditointi (audit)
riippumattoman tahon suorittama kohteen, sen toiminnan ja toiminnan tulosten yleensä määräajoin tapahtuva tutkiminen sen selvittämiseksi, vastaako kohde siihen kohdistuvia vaatimuksia

katselmointi (review)
Kohteen tilan arviointi, jonka tarkoituksena on tunnistaa eroavuudet tavoitetilaan nähden ja tuottaa kehitysehdotuksia. Katselmointi on aina henkilötyötä (toisin kuin tarkastus, johon voi sisältyä myös automatisoituja osia).

hyväksyntä/akkreditointi (accreditation)
prosessi, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen antaa virallisen lausunnon siitä, että kohde täyttää sille asetetut vaatimukset.

Esim. järjestelmä on hyväksytty käytettäväksi määritellyssä turvaluokassa, tiettyä turvallisuuden takaavaa toimintatapaa noudattaen käyttöympäristössään ja hyväksyttävällä riskitasolla, sen pohjalta, että hyväksytyt tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvatoimet on toteutettu.

sertifiointi (certification)
arvioinnin tuloksena annettu lausunto tai todistus vaatimustenmukaisuudesta, esimerkiksi akkreditointi tai turvallisuustodistus

itsearviointi
Arvioinnin kohteen vastuuhenkilön tai työryhmän toteuttama arviointi.

sisäinen arviointi
Organisaation tietoturvahenkilöstön tai asiantuntijoiden toteuttama arviointi.

ulkoinen arviointi
Organisaation ulkopuolisen, riippumattoman toimijan suorittama arviointi

vertaisarviointi
Arvioijina toimivat henkilöt, jotka työskentelevät samankaltaisen kohteen parissa toisessa organisaatiossa tai yksikössä.

sisäinen valvonta
organisaation valvonta on johdon vastuulla oleva toiminto, jonka tarkoituksena on tuottaa kohtuullinen varmuus toiminnan tehokkuudesta, tarkoituksenmukaisuudesta sekä säädösten mukaisuudesta.

sisäinen tarkastus
Organisaation oma järjestelmällinen ja kohteesta riippumaton arviointi. Organisaation oma (tai ulkoistettu) toiminto suorittaa sisäisen valvonnan toimenpiteitä.

riippumaton tarkastus
riippumaton toiminto, joka on erillään linjaorganisaatiosta, joka voi suorittaa tarkastuksensa ja arviointinsa yleisesti hyväksyttyjen standardien ja suositusten mukaisesti sekä voi raportoida sellaiselle organisaatiotasolle, joka voi tehokkaasti puuttua tarkastuksen esille nostamiin asioihin

omistaja (owner)
nimetty taho, jolla on valta tai valtuudet tehdä päätöksiä suojattavan kohteen osalta (esim. järjestelmä tai palvelu). Valtionhallinnossa voidaan käyttää myös termiä toimivaltainen viranomainen.

vaatimus (requirement)
kohteelle asetettu yksittäinen tavoite, joka kohteen tulee pystyä toteuttamaan

kriteeri (criterion)
arviointiperuste, jolla todetaan tavoitteen täyttyminen

poikkeama (exception)
kohteelle asetettu tavoitetila ei täyty tai täyttyy vain osittain

benchmarking
ulkoisten esikuvien löytäminen ja oman toiminnan vertaaminen näihin edelläkävijöihin, joka antaa mahdollisuuden omaksua parhaita käytäntöjä toiminnan kehittämiseen

erityissuojattava tietoaineisto
EU turvasäännön mukaan kansainvälisen tietoturvallisuusvelvoitteen mukaisesti turvallisuusluokitellut asiakirjat

tietoturvallisuusvaltiosopimus (GSA, General Security Agreement)
Suomen ja toisen valtion välinen tietoturvallisuussopimus

Liite 2 Muut arviointeja ja tarkastuksia suorittavat viranomaiset

Eduskunnan tarkastusvaliokunta
Eduskunta valvoo valtion taloudenhoitoa ja valtion talousarvion noudattamista (perustuslaki 90.1 §). Tätä varten eduskunnassa on tarkastusvaliokunta, jonka tulee saattaa eduskunnan tietoon merkittävät valvontahavaintonsa. Sen pääasiallisena tehtävänä on tehdä valtion taloudenhoitoa ja valtion talousarvion noudattamista koskevaa parlamentaarista jälkivalvontaa. Tehtävässään tarkastusvaliokunta keskittyy valtiontalouden yleiseen tilaan ja hoitoon sekä kysymyksiin, joiden saattaminen eduskunnan tietoon on perusteltua. Se käsittelee ja valmistelee muun muassa valtiontaloutta koskevat kertomukset täysistunnolle. Se voi ottaa käsiteltäväkseen toimialaansa kuuluvia asioita, joista sillä on oikeus antaa mietintö täysistunnolle. Tarkastusvaliokunta voi valvontatoimessaan tehdä oma-aloitteisesti selvityksiä, pyytää niitä valtioneuvostolta tai ministeriöiltä sekä kuulla asiaan osallisia ja asiantuntijoita. Se voi tilata myös ulkopuolisia tutkimuksia päättämistään aiheista.

Valtiontalouden tarkastusviraston rooli ja tehtävät tietoturvallisuuden arviointitoiminnassa Valtiontalouden tarkastusviraston tehtävänä on toimia valtion taloudenhoidon ja talousarvion sekä Euroopan Unionin taloudenhoidon ulkoisena ammattitarkastajana. Tämän tarkastusvirasto toteuttaa tekemällä tilintarkastusta, laillisuustarkastusta ja tuloksellisuustarkastusta sekä näitä tarkastusmenetelmiä yhdistävää tarkastusta. Tarkastusvirasto vahvistaa itse tarkastustaan koskevat ohjeet, jotka määrittävät hyvän tarkastustavan. Niiden perustana sovelletaan ylimpien tarkastusviranomaisten kansainvälisen järjestön INTOSAIn vahvistamia kansainvälisiä ISSAI-tarkastusstandardeja.

Valtiontalouden ylimpänä ulkoisena tilintarkastajana valtiontalouden tarkastusvirasto tarkastaa osaltaan myös sisäisen valvonnan ja siihen kuuluvan riskienhallinnan ohjauksen riittävyyttä ja asianmukaisuutta. Tietoturvallisuuteen kohdistuva tarkastus toteutetaan sisäisen valvonnan tarkastuksilla, tietojärjestelmien järjestelmätarkastuksilla, hallinnonalojen ohjausjärjestelmätarkastuksilla ja turvallisuutta koskevilla tuloksellisuustarkastuksilla. Turvallisuutta koskevissa tuloksellisuustarkastuksissa arviointi kohdistetaan tietoyhteiskuntaan, hallinnollisiin, lainsäädännöllisiin ja tekniseen infrastruktuuriin liittyviin asioihin. Turvallisuus voi olla tarkastuksen perusteema tai sen osa-alue. Näille tarkastuksille on tyypillistä poikkihallinnollisuus.

Tietosuojavaltuutettu
Tietosuojavaltuutettu on ylin tietosuojasta vastaava viranomainen Suomessa. Tässä tehtävässä tietosuojavaltuutettu valvoo henkilötietojen käsittelyä ja suorittaa siihen liittyviä tarkastuksia. Tarkastustoiminnan tarkoituksena on arvioida tietojenkäsittelyn lainmukaisuutta, opastaa rekisterinpitäjiä, parantaa järjestelmien tasoa sekä ennaltaehkäistä tietosuojaloukkaukset. Tarkastusten sisältö voi vaihdella yksittäisen yhteydenoton tutkimisesta laajaan tietojenkäsittelyprosessin selvittämiseen. Tietoturvallisuuden tasoa tarkastetaan osana tietosuojavaatimusten toteutumista.

Arkistolaitos
Arkistolaitoksen SÄHKE-normit ohjaavat julkishallinnon asiakirjahallintaa sähköisessä toimintaympäristössä. Määräykset antavat reunaehdot asiakirjallisten tietojen käsittelyprosessien sähköistämiselle ja tiedon luotettavalle sähköiselle säilyttämiselle. SÄHKE-normit määräävät niistä vaatimuksista ja ominaisuuksista, jotka ovat edellytyksenä tietojärjestelmiin sisältyvien tietojen säilyttämiselle pysyvästi yksinomaan sähköisessä muodossa.

Arkistolaitos edellyttää riittävää tietoturvallisuutta niiltä organisaatioilta, jotka hakevat SÄHKE2-normin mukaista sähköisen säilyttämisen lupaa. Osoituksena riittävästä tietoturvallisuudesta on suoritettu tietoturvallisuuden perustason arviointi. Lisäksi arkistolaitos suorittaa omia katselmointejaan siitä, täyttävätkö organisaation asiakirjahallinnolliset prosessit niille asetetut vaatimukset.

Sosiaali- ja terveysministeriön arvioinnit
Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007) säädetään tietoturvallisuutta ja tietosuojaa koskevista vaatimuksista, joita sovelletaan erityisesti sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä varten suunnitelluissa asiakas- ja potilasasiakirjojen ja niissä olevien tietojen käsittelyyn tarkoitetuissa ohjelmistoissa ja järjestelmissä. Sosiaali- ja terveydenhuollon tietojärjestelmät jaotellaan käyttötarkoitustensa ja ominaisuuksien perusteella ja luokan A kuuluvien palveluiden ja järjestelmien osalta tietoturvallisuutta ja tietosuojaa koskevat vaatimukset on todennettava tietoturvallisuuden arviointilaitoksen suorittamalla arvioinnilla.

Valtori
Valtion tieto- ja viestintätekniikkakeskus Valtori edellyttää tietoturvallisuuden perustason saavuttamista sen palveluihin liittyviltä asiakkailta eli valtionhallinnon viranomaisilta. Perustason täyttyminen todennetaan ulkoisella arvioinnilla.

Viranomainen voi myös tilata arviointeja kaupallisilta toimijoilta silloin kun arvioinnin kohteelle ei haeta viranomaishyväksyntää. Näiden arviointien tuloksia voidaan hyödyntää esimerkiksi tietojärjestelmän kehittämisessä, arvioitaessa tietoturvallisuuden toteutusta järjestelmän kehittämisvaiheessa, sekä haettaessa kohteelle myöhemmin ulkoista arviointia ja viranomaishyväksyntää.

Valtori on kilpailuttanut valtionhallinnon viranomaisten käyttöön tietoturvallisuuden konsultointi- ja arviointipalveluja, joita voidaan hyödyntää esimerkiksi tietojärjestelmien arviointiin tai tietoturvallisuusasetuksen mukaisen tietoturvatason ohjattuun itsearvioin-

tiin. Valtorin asiakkaat voivat hankkia tietoturvapalveluita ilman, että niitä tarvitsee itse kilpailuttaa. Palvelun tuottajina on useita konsulttiyrityksiä ja alihankkijoita, joiden konsulteilta löytyy osaamista hyvinkin erityyppisiin toimeksiantoihin.

Liite 3 CASE-esimerkkejä

1. Puolustusvoimien elinkaarimalli

Tietohallintapäätösmenettely sisältää tietoturvallisuuden osalta seuraavat päävaiheet:

THP -käynnistämisvaiheessa (THP 1) hankkeen/projektin tarvitsemat tietoturvaresurssit määritellään ja tarvittaessa hankkeeseen/ projektiin osoitetaan lisäresursseja. Käynnistämis-vaiheen jälkeen hankkeella/projektilla on riittävät tiedot ja resurssit laatia tietoturvallinen hankintaehdotus.

Suunnittelusta rakentamiseen -vaiheessa (THP 3) suoritetaan tietoturva-arviointi. Arvioinnissa varmistetaan, että järjestelmälle suunnitteluvaiheessa asetetut tietoturvavaatimukset ovat riittävät. Arvioinnin voi suorittaa Pääesikunnan johtamisjärjestelmäosaston hyväksymä tarkastusorganisaatio. Arvioinnista tiedotetaan puolustusvoimien SAA-toimijaa. Hyväksytyn arvioinnin jälkeen hanke/projekti saa luvan edetä rakentamisvaiheeseen.

Rakentamisesta operointiin -vaiheessa (THP 4) suoritetaan tietoturva-arviointi perustuen kehitystyön dokumentaatioon ja tekniseen toteutukseen. Tarkastuksissa todetaan suunnittelusta rakentamiseen -vaiheessa asetettujen tietoturvavaatimusten toteutuminen ja todennetaan järjestelmän tuotantokäytön vaatimien prosessien riittävyys tietoturvamielessä kuten esim. käyttövaltuushallinta, toipumissuunnittelu, muutoshallinta, elinkaarenhallinta, lakimääräiset rekisteriselosteet, varmuuskopioinnin järjestelyt. SAA:n asettamat vaatimukset tietoturvatarkastustoiminnalle kuvataan DSA -normissa

Järjestelmä voidaan ottaa operatiiviseen käyttöön hyväksytyn akkreditointipäätöksen jälkeen. Akkreditointi suoritetaan SAA:n (puolustusvoimien tai Viestintäviraston) toimesta ja akreditointi pohjautuu suoritettuun tietoturva-arviointiin. Akkreditointi voi olla määräaikainen tai ehdollinen. Määräaikainen akkreditointi edellyttää uutta akkreditointia määräajan umpeutuessa. Ehdollinen akkreditointi edellyttää uutta akkreditointia, jos akkreditoinnin perusteet oleellisesti muuttuvat.

Operointivaiheessa (THP 4.N) suoritetaan teknisiä tietoturvatarkastuksia ja -auditointeja osana kehityskohteen tuotantokäytön aikaista toimintaa. Tekninen tietoturvatarkastus voi ajoittua tietojärjestelmän tuotantokäytön aikaisen ohjelmistoversion (-oiden) päivityksen yhteyteen tai määräaikaisena (1-3v). Kehitystyön omistaja määrittelee tuotantokäytön aikaisten tarkastusten ajoittamisen kehitystyön elinjakson aikana. Tarkastus- ja auditoinnit suoritetaan puolustusvoimissa hyväksytyn tarkastustoimijan toimenpitein.

Operoinnista purkuun -vaiheessa (THP 5) arvioidaan kehitystyön purkamis- ja luopumissuunnitelmien vaikutus palveluympäristön tietoturvaan. Osana THP 5-päätöstä annetaan teknisen tietoturvan osalta purkamislupa. Arviointi suoritetaan puolustusvoimissa hyväksytyn tarkastustoimijan toimenpitein.
Tietoturvatarkastustoimintaa voidaan tarvittaessa suorittaa myös erillään THP-menettelystä, esimerkiksi yllätystarkastuksina, pistokokeina tai osana hankintaprosessin suunnittelua. Puolustusvoimien johtamisjärjestelmäkeskus (PVJJK), Viestikoelaitos (VKOEL), Puolustusvoimien tiedustelukeskus (PVTK) sekä puolustushaarat tukevat tätä tarkastustoimintaa tarvittaessa.

Liite 4 Tietoturvallisuuden perustaso tietoturvallisuusasetuksen 5 §:n mukaan

5 § Tietoturvallisuuden perustason toteuttaminen

Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, että:

1) viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan;
2) viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään;
3) asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään;
4) tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi;
5) asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi;
6) tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä;
7) asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;
8) henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;
9) henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä;
10) annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

Valtionhallinnon viranomaisen velvollisuudesta huolehtia tietojen suojaamisesta annettaessa salassa pidettäviä tietoja toimeksiantotehtävän suorittamista varten säädetään viranomaisten toiminnan julkisuudesta annetun lain 26 §:n 2 momentissa. Henkilörekisteriin talletettujen henkilötietojen antamisesta säädetään lisäksi henkilötietolain 32 §:n 2 momentissa.

Liite 5 Voimassa olevat VAHTI –julkaisut

VAHTI 2/2014	Tietoturvallisuuden arviointiohje
VAHTI 1/2014	VAHTIn toimintakertomus vuodelta 2013
VAHTI 5/2013	Päätelaitteiden tietoturvaohje
VAHTI 4/2013	Henkilöstön tietoturvaohje
VAHTI 2/2013	Toimitilojen tietoturvaohje
VAHTI 1/2013	Sovelluskehityksen tietoturvaohje
VAHTI 3/2012	ICT-teknisen ympäristön tietoturvataso-ohje
VAHTI 2/2012	ICT-varautumisen vaatimukset
VAHTI 3/2011	Valtion ICT-hankintojen tietoturvaohje
VAHTI 2/2011	Johdon tietoturvaopas
VAHTI 4/2010	Sosiaalisen median tietoturvaohje
VAHTI 3/2010	Sisäverkko-ohje
VAHTI 2/2010	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
VAHTI 7/2009	Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009	Kohdistetut hyökkäykset
VAHTI 3/2009	Lokiohje
VAHTI 9/2008	Hankkeen tietoturvaohje
VAHTI 8/2008	Valtionhallinnon tietoturvasanasto
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen
VAHTI 3/2008	Valtionhallinnon salauskäytäntöjen tietoturvaohje
VAHTI 2/2008	Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 3/2007	Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 1/2007	Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006	Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006	Tietoturvakouluttajan opas
VAHTI 9/2006	Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 7/2006	Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006	Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006	Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 2/2006	Electronic-mail Handling Instruction for State Government
VAHTI 3/2005	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005	Information Security and Management by Results

VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002	Valtionhallinnon etätyön tietoturvaohje
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje

Ohjeisto löytyy VAHTIn Internet-sivuilta www.vm.fi/vahti sekä www.vahtiohje.fi

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
Telefaksi 09 160 33123
www.vm.fi

2/2014
VAHTI
Joulukuu 2014

ISSN 1455-7606 (nid.)
ISBN 978-952-251-622-0 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251- 623-7 (pdf)