Hyvärinen Liisa VM

Lähettäjä: Jalava Maarit [Maarit.Jalava@formin.fi]
Lähetetty: 6. elokuuta 2014 8:46
Vastaanottaja: Valtiovarainministerio VM
Kopio: NSA-00
Aihe: Lausuntopyyntö VAHTI arviointiohjeen luonnokseen
Liitteet: Tietoturvallisuuden_arviointiohjeluonnos 2.pdf

Ohessa NSA:n kommentit tietoturvallisuuden arviointiohjeluonnokseen. Kommentit on merkitty ohjeluonnokseen ja ne kohdistuvat lähinnä osioihin, joissa käsitellään kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista.

Terveisin,

Maarit Jalava
Deputy Director, National Security Authority
tel +358 295 351 843
mobile +358 50 3831361
e-mail maarit.jalava@formin.fi
nsa@formin.fi

VAHTI

OHJE-LUONNOS

13.06.2014

Tietoturvallisuuden arviointiohje

LUONNOS

VALTIOVARAINMINISTERIÖ

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

Johdanto

Tämä ohje on tarkoitettu valtionhallinnon viranomaisille, joiden tulee säännöllisesti arvioida organisaationsa tietoturvallisuuden tilaa sekä toteutettujen tietoturvatoimenpiteiden asianmukaisuutta ja riittävyyttä.

Tietoturvatyön lähtökohtana tulee olla tietoisuus organisaation turvallisuuden tasosta, mutta se on myös lainsäädännöllinen velvoite. Lisäksi turvallisuuden arviointia tulee suorittaa aina merkittävien muutosten yhteydessä.

Ohjeen liitteessä 1 on sanasto, joka pyrkii selventämään mitä tässä ohjeessa käytetyillä termeillä tarkoitetaan.

Tausta

Ohje on suositukseksi 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 erilaisia tarkistuslistoja arvioimisen tueksi. Ohjeistuksesta on ollut tarjolla, mutta siitä huolimatta arviointi- ja auditointitoiminta on ollut satunnaista useimmissa valtionhallinnon organisaatioissa, lähinnä sitä ovat tehneet tietoturvatyötä muutenkin järjestelmällisesti kehittäneet viranomaiset.

Valtionhallinnon tietoturvallisuuden kehittämistä koskeva periaatepäätös[1] ohjaa valtionhallinnon tietoturvallisuuden kokonaisuutta, ja siinä päätetään tietoturvallisuuden kehittämisen periaatteista ja painopisteistä sekä linjataan keskeiset suuntaviivat viranomaisten tietoturvatyölle. Kehittämisen painopisteisiin kuuluvat esimerkiksi tietoturvallisuuden hallintajärjestelmän, mittareiden ja seurannan sekä palvelu- ja hankintaketjujen tietoturvallisuuden ja 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

---

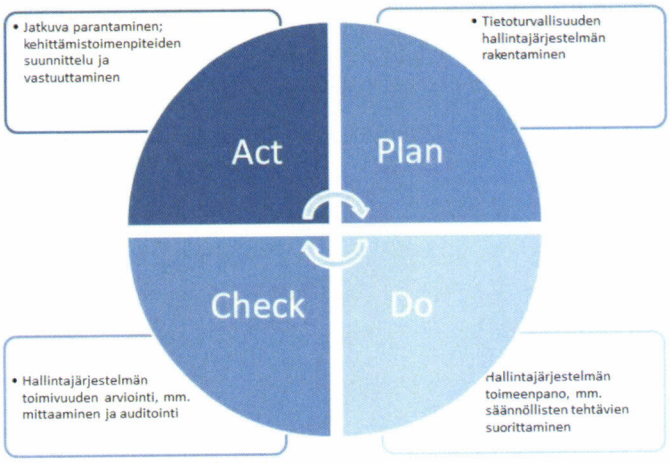
1 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä, VAHTI 7/2009, 26.11.2009

arviointeja merkittävästi asetuksen voimaantulon jälkeen. Lisäksi tietoturvatietoisuuden kasvu ja tietoturvauhkien lisääntyminen ovat kasvattaneet tarvetta arvioinneille.

Auditoinnit ja arvioinnit ovat lisääntyneet merkittävästi, mutta viranomaisilla on paljon epätietoisuutta siitä milloin arviointeja tulisi tehdä, miten, kenen toimesta ja mitä viitekehyksiä arviointiin pitää käyttää. Tämä ohje pyrkii selventämään näitä kysymyksiä sekä antamaan suosituksia arviointien suorittamiseen.

Arvioinnin hyödyt organisaatiolle

Tietoturvallisuuden arviointi on apuväline organisaation tietoturvallisuuden johtamiseen ja kehittämiseen. Se tukee organisaation tavoitteiden toteuttamista kun arvioinnin kohteet valitaan organisaation toiminnan kannalta oikein, eli kohdentamalla arvioinnit merkittäviin 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 suunnittele – tee – arvioi/mittaa – paranna -periaatetta (PDCA). Sisäisten ja ulkoisten arviointien avulla organisaatio saa tarvittavaa tietoa toiminnan jatkuvan parantamisen toteuttamiseen.



Kuva 1. Tietoturvallisuuden PDCA-malli

Edellytykset tietoturvallisuuden arvioinnille

Jotta tietoturvallisuuden arviointi olisi mahdollista, organisaation tulee ensin huolehtia tietyistä tietoturvallisuuden perusasioista. Tietoturvallisuuden keskeiset viitekehykset perustuvat sille vaatimukselle, että tietoturvatyö on hallittua, säännöllistä ja dokumentoitua. Muun muassa tietoturvatasojen tai ISO/IEC27001-standardin vaatimukset voidaan toteuttaa hallintajärjestelmän avulla. Organisaation tulee laatia oman tietoturvallisuuden hallintajärjestelmänsä kuvaus, jonka keskeiset dokumentit ovat mm. tietoturvapolitiikka ja –strategia, tietoturvakäytännöt, -periaatteet ja ohjeet, kehittämissuunnitelma, tietoturva-arkkitehtuurit, riskienhallinnan kuvaus, jatkuvuus- ja valmiussuunnitelmat, tietoturvaraportointi ja audi-

tointisuunnitelma. Hallintajärjestelmän sisältöä on kuvattu tarkemmin VAHTI:n yleisohjeessa[2].

Ennen arviointien tilaamista ulkopuoliselta arvioijalta, on suositeltavaa, että organisaatio tekee arvioinnin kohteeseen itsearvioinnin. Tämän 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 vastuutaho, jonka toimintaa ja tietojenkäsittelyä suojattava kohde palvelee. Vastuutahoa voidaan kutsua myös termillä "omistaja". Hän vastaa tietojärjestelmän kehittämisestä ja on siten vastuussa myös suojattavan kohteen tietoturvallisuudesta ja siihen liittyvistä kustannuksista.

Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä tai palvelu. 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.

Tietoturvallisuuden arviointiin liittyvä lainsäädäntö

Tietoturvallisuutta koskeva lainsäädäntö

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. Asiakirjojen ja tietojärjestelmien sekä niihin liittyvien 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] Tietoturvallisuudella tuloksia, yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007

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 suojaan sekä tietojärjestelmien turvallisuuteen vaikuttavat uhat sekä niiden vähentämiseksi ja poistamiseksi käytettävissä olevat keinot ja 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.

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[3]. Laissa säädetään turvallisuusviranomaisten tehtävistä ja erityissuojattavan aineiston suojaamista koskevista tietoturvallisuustoimenpiteistä.

Tietoturvallisuustoimenpiteillä tarkoitetaan salassapito- ja vaitiolovelvollisuutta sekä hyväksikäyttökieltoa. Lisäksi erityissuojattavaan aineistoon on merkittävä turvallisuusluokkaa koskeva merkitä ja noudattaa vastaavaa luokkaa koskevia käsittelyvaatimuksia. Tietoja käsittelevien henkilöiden ja elinkeinonharjoittajien luotettavuuden arvionniksi on laadittava henkilö- ja yritysturvallisuusselvitykset, joiden perusteella turvallisuusviranomainen antaa turvallisuustodistuksen. Yritysturvallisuusselvitys voidaan tehdä elinkeinonharjoittajista, jotka ovat osapuolena kansainvälisessä turvallisuusluokitellussa sopimuksessa tai osallistuvat julkisista puolustus- ja turvallisuushankinnoista annetussa laissa tarkoitettuun tarjouskilpailuun, jossa käsitellään luokiteltuja tietoja.

---

[3] 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.fi kohdasta: Etusivu – Palvelut - Kansallinen turvallisuusviranomainen (NSA) - Voimassa olevat tietoturvasopimukset) (http://formin.finland.fi/Public/default.aspx?nodeid=47189&contentlan=1&culture=fi-FI)

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 tietojärjestelmien, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja, on läpikäytävä hyväksymisprosessi, jossa pyritään varmistumaan siitä, että kaikki asiaankuuluvat turvatoimet on pantu täytäntöön ja että riittävä suojaustaso on saavutettu[4]. Lisäksi Suomea sitovat turvallisuusluokitellun tiedon suojaamista koskevat valtiosopimukset edellyttävät pääsääntöisesti henkilöiden ja yritysten turvallisuusselvityksiä turvallisuusluokasta III ylöspäin sekä määrättyjen turvallisuusviranomaisten (Designated Security Authority, DSA) välistä sopimusta, jos tietoa siirretään valtioiden välillä sähköisessä muodossa.

Tietoturvallisuuden viranomaisarviointia edellytetään myös julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (HE 54/2013, 31 §). Turvallisuusselvityksistä annetun lain mukaan valtioneuvoston asetuksella voidaan säätää valtionhallinnon viranomaisen velvollisuudesta hakea yritysturvallisuusselvitys niistä yrityksistä, jotka käsittelevät suojaustasoille I-III luokiteltuja asiakirjoja (HE 57/2013, 34 §).

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. Viranomainen voi pyytää Viestintävirastolta sen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tietoturvallisuuden arviointia ja vaatimukset täyttävälle järjestelmälle hyväksymistä osoittavan todistuksen antamista. Lisäksi lain 5§ mahdollistaa sen, että Viestintävirasto voi valtiovarainministeriön pyynnöstä tehdä selvityksiä valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta.

Lain tarkoituksena muun muassa se että viranomaiset voivat saada Viestintävirastolta ulkopuolisen arvion korkeamman tason kriittisistä järjestelmistä, joiden arviointi yksityisten arviointilaitosten toimesta on ongelmallista.

Laki tietoturvallisuuden arviointilaitoksista

Tietoturvallisuuden arviointilaitostoiminnasta säädetään tietoturvallisuuden arviointilaitoksia koskevassa laissa (1405/2011), jossa määritellään arviointilaitosten hyväksymiskriteerit ja tehtävät. Lailla on luotu järjestelmä, jonka avulla voidaan kehittää tietoturvallisuutta yhteisten kriteerien ja viranomaisvalvonnassa olevien arviointilaitosten avulla sekä osoittaa

[4] Euroopan unionin neuvoston päätös (2013/488/EU)

toiminnan tietoturvallisuuden taso ulkopuolisen, luotettavan arvioinnin avulla. 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 yritysturvallisuusselvitystä tai tietojärjestelmän hyväksyntää koskeva todistus annetaan arviointilaitoksen tekemän arvioinnin pohjalta. Myös viranomaiset voivat käyttää hyväksytyn arviointilaitoksen suorittamaa arviointia tietoturvallisuuden tason arvioinnissa.

Arviointilaitoksen 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.[5] Hyväksyntäprosessia kuvataan tarkemmin Viestintäviraston antamassa ohjeessa[6].

Tietoturvallisuuden arviointilaitosten toiminta rinnastetaan julkisen hallintotehtävän hoitamiseen, minkä vuoksi hyväksytyn laitoksen tulee noudattaa hyvää hallintoa koskevia viranomaisvaatimuksia. Tämä tarkoittaa muun muassa hallintolain menettelymääräyksiä sekä julkisuuslain salassapitomääräyksiä.

Turvallisuusselvityslaki

Turvallisuusselvityslain (.../...) 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. Lisäksi laissa säädetään näiden etujen suojaamiseksi toteutettavista turvallisuusjärjestelyistä, joita ovat erityisesti henkilö- ja yritysturvallisuusselvitykset. Henkilöturvallisuusselvityksellä tarkoitetaan henkilön luotettavuuden varmistamista koskevaa selvitystä ja yritysturvallisuusselvityksellä yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimista koskevaa selvitystä. Laissa luetellaan henkilöturvallisuusselvitysmenettelyn piiriin kuuluvat tehtävät sekä yritysturvallisuusselvityksen hakemiseen oikeutetut tahot.

---

5 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.

6 NCSA:n suorittama tietojärjestelmien tietoturvallisuushyväksyntä ja –arviointi, 8.1.2013.

Yritysturvallisuusselvitystä voi hakea taho, 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.[7] Yritysturvallisuusselvitys toteutetaan turvallisuusselvityslain 37 §:n mukaisten tietolähteiden sekä yritykseen ja sen toimitiloihin sekä sen tietojärjestelmiin ja tietoliikennejärjestelyihin kohdistuvan tarkastuksen avulla.

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. Kilpailutettaessa hankintoja julkisista hankinnoista annetun lain mukaisin menettelyin hankinnan tietoturvavaatimusten on liityttävä hankinnan kohteeseen. Toimittajan organisaatiolle ei siis voida hankintalain perusteella asettaa tietoturvavaatimuksia muuten kuin hankinnan kohteen osalta. Jos kyse on puolustus- tai turvallisuushankintalain alaisesta hankinnasta[8], hankintayksikkö voi asettaa tietoturvavaatimuksia sekä tarjouskilpailuvaiheen (54 §) että hankinnan (41 §) toteuttamiseksi. Tällöin turvallisuustoimenpiteitä voidaan toteuttaa jo ennen sopimussuhteen syntymistä, kun tarjouksen laatiminen edellyttää pääsyä salassa pidettäviin tietoihin. Tietoturvavaatimusten on puolustus- ja turvallisuushankintalain mukaan perustuttava viranomaiselle asetettujen tietoturvallisuusvelvoitteiden toteuttamiseen, mutta puolustus- ja turvallisuushankintalaki ei edellytä, että tietoturvavaatimusten olisi suoraan liityttävä hankinnan kohteeseen. Vaatimusten tulee kuitenkin olla syrjimättömiä ja niistä on ilmoitettava tarjouspyynnössä.

Puolustus- ja turvallisuushankintaan liittyvistä salassa pidettävistä tiedoista ja niihin kohdistuvista suojausvaatimuksista riippuen hankintayksikkö voi edellyttää henkilö- ja yritysturvallisuustodistusta tai muita sitoumuksia tai tietoja, jotka liittyvät turvallisuusluokitellun tiedon käsittelyyn, säilyttämiseen, tuhoamiseen sekä luovuttamiseen. Tarjoajan tai alihankkijan sitoumukseen liittyy usein tilojen, toimintatapojen ja prosessien tarkastus turvallisuusselvityslain tai kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan. Hankintayksikkö voi tehdä omia tarkastuksia tai selvityksiä tai pyytää muilta hankintayksiköiltä tietoja tarjoajan kyvystä suoriutua tietoturvallisuusvaatimuksista.

---

[7] 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).

[8] Puolustushankinnoilla tarkoitetaan muun muassa puolustustarvikkeita sekä erityisesti sotilaalliseen käyttöön tarkoitettuja rakennusurakoita ja palveluita. Turvallisuushankinnoiksi katsotaan tavara- ja palveluhankinnat sekä rakennusurakat ja niiden osakokonaisuudet, jotka ovat tarkoitettu käytettäväksi turvallisuustarkoituksiin ja joiden toteuttamiseksi annetaan, laaditaan tai muutoin käsitellään turvaluokiteltuja asiakirjoja.

Kun hankinnan kohteena on tietojärjestelmä tai tietoliikennejärjestely, määrittelee hankintayksikkö tarpeen mukaan tarjouspyyntö- ja hankintasopimusasiakirjoihin liittyvissä teknisissä kuvauksissa tietojärjestelmää koskevat tietoturvallisuusvaatimukset, jotka määräytyvät tietojärjestelmässä käsiteltävien salassa pidettävien tietojen tai ICT-varautumistarpeiden perusteella. Tällöin hankinnan yhteydessä on suositeltavaa sopia myös niistä menettelyistä, joilla järjestelmän tietoturvallisuusvaatimukset todennetaan.

Edellä mainituissa hankintalaeissa on säädetty yleisistä ja erityisistä soveltamisalaa koskevista poikkeuksista, 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 tietoturvallisuusvaatimukset sen mukaisesti, mitä salassa pidettävää tietoa palveluntoimittajalle luovutetaan.

Kappaleessa 5 käsitellään tietoturvallisuusvaatimusten vaatimuksenmukaisuuden arviointia toimeksiantosuhteissa.

Tietoturvallisuuden ohjausta koskeva lainsäädäntö

Valtiovarainministeriöstä annetun asetuksen[9] mukaan valtiovarainministeriö vastaa julkisen hallinnon tietoturvallisuuden yleisestä kehittämisestä sekä valtionhallinnon tietoturvallisuuden ohjauksesta. Valtiovarainministeriön tehtävänä on lisäksi julkishallinnon viranomaisten tietohallinnon yleinen ohjaus[10] sekä valtion yhteisten tieto- ja viestintäteknisten palvelujen varautumisen, valmiuden ja turvallisuuden ohjaus[11]. Tällaisia palveluja 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) 5§ mukaan valtiovarainministeriö voi pyytää valtionhallinnon tietoturvallisuudesta annettujen säännösten täytäntöönpanon seuraamiseksi ja kehittämiseksi Viestintävirastolta selvitystä valtionhallinnon viranomaisten tietojärjestelmien yleisestä tietoturvallisuuden tasosta. Valtiovarainministeriöllä on salassapitosäännösten estämättä oikeus saada tiedon arvioinnin lopputuloksista.

Tietoturvallisuuden arviointiperusteet

Tietoturvallisuuden arviointiperusteilla tarkoitetaan niitä tietoturvallisuutta koskevia vaatimuksia, joiden perusteella tietoturvallisuuden arviointi suoritetaan. Arviointiperusteina voidaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annetun lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti käyttää:

---

[9] Valtioneuvoston asetus valtiovarainministeriöstä (610/2003)
[10] Laki julkisen hallinnon tietohallinnosta (634/2011)
[11] Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013)

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 ennen kaikkea tietoturvallisuusasetuksen 5§ mukaisia tietoturvatasovaatimuksia, joita on täsmennetty valtiovarainministeriön ohjeilla. Asetuksen täytäntöönpanoa koskevaa ohjetta (VAHTI 2/2010) sovelletaan tietoturvallisuuden arviointiperusteena silloin, kun arvioinnin kohteessa käsitellään Suomen viranomaisen salassa pidettävää tietoa jonka salassapito perustuu julkisuuslakiin.

Kun taho, jolla on määräysvalta salassa pidettävään tietoon, on toisen valtion viranomainen tai siellä kotipaikkaansa pitävä yritys, kansainvälinen järjestö tai toimielin, ja Suomella on tietoturvallisuusvaltiosopimus kyseisen valtion tai toimielimen kanssa, sovelletaan tiedon salassapitoon ja tietoturvallisuustoimenpiteisiin lakia kansainvälisistä tietoturvallisuusvelvoitteista. Tiedon käsittelyyn sovelletaan tällöin kansallisten tietoturvallisuusvaatimusten lisäksi aina soveltuvaan valtiosopimukseen tai muuhun Suomea koskevaan velvoitteeseen, eli kansainväliseen tietoturvallisuusvelvoitteeseen, sisältyviä määräyksiä. Erityissuojattavaa tietoaineistoa eli kansainvälisen tietoturvallisuusvelvoitteen mukaisesti turvallisuusluokiteltuja asiakirjoja ja materiaaleja luotaessa, kopioitaessa, siirrettäessä, jaettaessa, säilytettäessä, hävitettäessä tai muutoin käsiteltäessä on pidettävä huolta, että tietoaineiston suojaamisesta voidaan huolehtia sen turvallisuusluokkaa vastaavalla tavalla. Erityissuojattava tietoaineisto on säilytettävä tiloissa, joissa asiakirjojen ja niihin sisältyvien tietojensuojaamisesta voidaan huolehtia valtiosopimuksessa edellytetyllä tavalla. Kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvien tietoturvavaatimusten todentamisessa käytetään kansallista turvallisuusauditointikriteeristöä (KATAKRI). Erityissuojattavan tietoaineiston käsittely edellyttää viranomaishyväksyntää, ja kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvien turvallisuusselvitysten tekemisestä vastaa aina toimivaltainen turvallisuusviranomainen.

Tietoturvallisuuden arviointi voi perustua myös muihin kuin lainsäädännöstä johtuviin vaatimuksiin. Tietoturvallisuuden arviointiperusteina voidaan käyttää julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita taikka vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia. Tällainen vahvistettu standardi on esimerkiksi tietoturvallisuuden hallintajärjestelmiä koskeva kansainvälinen standardi ISO/IEC 27001, joka toimii mallina tietoturvallisuuden hallintajärjestelmän kehittämiselle, toteuttamiselle, käyttämiselle, valvomiselle, katselmoinnille, ylläpitämiselle ja parantamiselle. Lisäksi tietoturvallisuuden arviointi voi perustua organisaation tekemiin sopimuksiin ja niihin kirjattuihin tietoturvavelvoitteisiin.

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

Tietoturvallisuusasetuksen tasovaatimukset

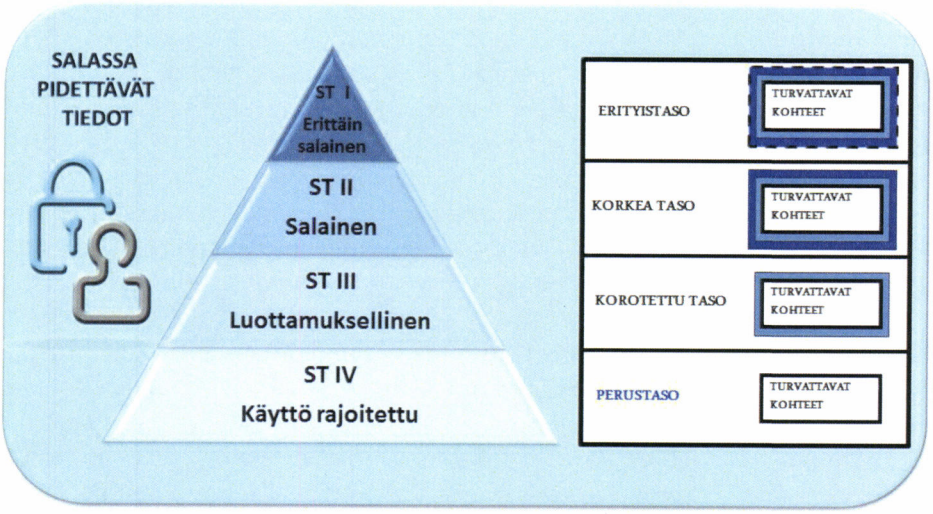
Tietoturvallisuusasetuksen 5 §:ssä on asetettu valtionhallinnon viranomaisille **tietoturvallisuuden perustason** vaatimukset (Liite 3). Niistä konkreettisista toimenpiteistä, joita tietoturvallisuuden perustason toteuttaminen edellyttää, annetaan tarkemmat määrittelyt valtiovarainministeriön ohjeistuksessa (VAHTI 2/2010). Asetuksen 23.3 §:n siirtymäsäännöksen mukaan viranomaisen tietojenkäsittely on saatettava vastaamaan asetuksen 5 §:ssä säädettyjä perustason tietoturvallisuusvaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta. 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 §), kohdistuvat vaatimukset valtionhallinnon viranomaisten tietoverkkoon ja tietojenkäsittelyn kokonaisuuteen.

Asiakirjojen suojaamisen yhteydessä edellytetään, että viranomaisen tietoverkko ja tietojenkäsittelyn kokonaisuus täyttää korotetun tai korkean tietoturvallisuustason vaatimukset. Asetuksen mukaan viranomaiset voivat sallia esim. suojaustasoon ST III kuuluvan asiakirjan tallettamisen ja siirtämisen salaamattomana mikäli tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät korotetun tason vaatimukset. Salaamis- ja suojaamistarvetta ja 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 tietoturvatasovaatimusten toteutumista. Arvioinnin kohteen johto tekee viime kädessä päätöksen riittävän tason saavuttamisesta ja hyväksyy jäännösriskit liittyen yksittäisten tietoturvallisuusvaatimusten toteuttamatta jättämiseen.

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.



Kuva 2. Tiedon luokituksen ja tietoturvatason vastaavuus

Katakri

Kansainvälisen erityissuojattavan tietoaineiston käsittelyssä tulee noudattaa tiedon luovuttaneen viranomaisen asettamia vaatimuksia, joita ovat esimerkiksi:

- EU Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluoki-teltujen 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 ja muiden maiden kahdenväliset bilateraalisopimukset

Edellä mainitut vaatimukset ovat varsin yleisellä tasolla ja ne edellyttävät, että käsittelyssä noudatetaan kansallisen viranomaisen antamia ohjeita.
Suomessa kansallisena turvallisuusviranomaisena (National Security Authority, NSA) toimii ulkoasiainministeriö. NSA on antanut seikkaperäisen ohjeen kansainvälisen luokitellun aineiston käsittelystä [12].

Kansallista turvallisuusauditointikriteeristö (KATAKRI) on tarkoitettu Kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvien tietoturvallisuusvaatimusten todentamiseen. Kriteeristöä käytetään arviointityökaluna niissä arvioinneissa, joiden tarkoituksena on todentaa, täyttävätkö viranomaiset niiltä edellytettävät kansainväliset tietoturvallisuusvaatimukset. Se toimii myös kansallisesti velvoittavana asiakirjana silloin, kun suomalaisten yritysten turvallisuustaso varmennetaan kansallisen turvallisuusviranomaisen toimesta kansainväliseen viranomaispyyntöön pohjautuen ja yritysturvallisuustodistuksen myöntämiseen tähdäten.

[12] Kansainvälisen turvallisuusluokitellun tiedon käsittelyohje, päivitetty 10.2.2014

ICT-varautumisen vaatimukset

Lisäksi VAHTI 2/2012 ICT-varautumisen vaatimukset kuvaa viitekehyksen, jota voidaan käyttää varautumisen 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 turvaaminen. Niiden tasot voivat poiketa toisistaan, sillä joissain toiminnoissa tiedot voivat olla julkisia, mutta palveluilta edellytetään korkeaa käytettävyyttä.

ICT-varautumisen vaatimuksia kannattaa käyttää viitekehyksenä erityisesti silloin kun hankitaan tai tuotetaan itse yhteiskunnan elintärkeiden toimintojen kannalta kriittisiä palveluita.

Muut valtionvarainministeriön antamat ohjeet

Tietoturvaturvallisuusasetuksen 4§ (Liite 3) annetaan kymmenen vaatimusta tietoturvallisuuden perustasolle. Näitä vaatimuksia täsmentää ja täydentää Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta VAHTI 2/2010, jossa tietoturvatasojen kaikkien kolmen tason vaatimukset on kuvattu yksityiskohtaisesti. Nämä vaatimukset kohdistuvat menettelytapoihin ja prosesseihin eikä niiden perusteella tehdä päätöksiä teknisistä yksityiskohdista ja ratkaisuista, joiden avulla tasovaatimukset voidaan täyttää. Tämän vuoksi tietoturvatasot on huomioitu kaikissa asetuksen voimaantulon jälkeen julkaistuissa VAHTI-ohjeissa, joissa annetaan vaatimuksia ja suosituksia eri tietoturvatasoilla sovellettavista ratkaisuista. VAHTIn tekninen jaosto muodostaa tulkintoja linjausten mukaisista 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 7.3. kuvataan tarkemmin ICT-hankintoja ja sovelluskehitystä koskevien ohjeiden käyttöä palveluiden tuottamisessa ja niiden arvioinnissa.

Viranomaisten tietoturvallisuuden arviointi

Viranomaisten 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. Hallinnollisissa arvioinneissa käytetään yleensä viitekehyksenä tietoturvatasoja, mutta hallintajärjestelmän arviointi on mahdollista myös esimerkiksi ISO/IEC 27001 standardin mukaisesti.

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

Hallinnollista arviointia voidaan tehdä myös itsearviointina säännöllisin väliajoin, mikä on tietoturvallisuuden jatkuvan kehittämisen kannalta myös suositeltavaa. ISO/IEC 27001 standardin mukaan sertifioitu hallintajärjestelmä edellyttää vuosittaista itsearviointia. Myös viranomaisten väliset vertaisarvioinnit ovat hyödyllisiä, niissä kaksi tai useampi organisaatio suorittaa toisen viranomaisen tietoturvallisuuden arvioinnin ja hyödyntää näin toisen organisaation osaamista ja resursseja.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden arviointi

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa säädetään viranomaisten tietojärjestelmien arvioinnissa sovellettavista menettelyistä ja perusteista, joita arvioinnissa voidaan käyttää[13]. Lain tarkoituksena on osoittaa viranomaisille sopiva menettely, jonka avulla ne voisivat saada luotettavan arvioinnin käyttämiensä tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasosta. Lain perusteella Viestintävirasto voi arvioida viranomaisten tietojärjestelmiä ja tietoliikennejärjestelyjä sekä antaa todistuksen vaatimukset täyttävistä järjestelmistä. Laki liittyy osaltaan valtionhallinnon tietoturvallisuutta koskevien säännösten täytäntöönpanoon ja niiden kehittämiseen. Tietojärjestelmien arviointimenettelyllä on yleisempääkin merkitystä, koska viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta arvioiva viranomainen kuuluu osana eri maissa noudatettuihin ja useissa kansainvälisissä sopimuksissa ja säädöksissä edellytettyihin järjestelyihin.

Tietojärjestelmien arviointia koskevan lain mukaisia arviointeja voivat tehdä Viestintävirasto sekä sen hyväksymät tietoturvallisuuden arviointilaitokset. Viranomaishyväksynnän voi kuitenkin antaa ainoastaan Viestintävirasto. Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä 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. Tämä on tarpeen sen vuoksi, että valtionhallinnon viranomaisten tietojärjestelmien arvioinnit toteutettaisiin yhtenäisillä menettelytavoilla ja siten toimeksiantaja saisi arvioinnista aiheutuvia kustannuksia vastaavan hyödyn valtionhallinnon tietoturvallisuuden kehittämiseksi yhtenäisellä tavalla ja ilman perustaltaan epäasial-

---

[13] Arviointiperusteilla tarkoitetaan vaatimuksia, joiden perusteella arviointi tehdään. Näitä ovat muun muassa lailla tai asetuksella säädetyt viranomaisen toimintaa koskevat tietoturvallisuusvaatimukset ja valtiovarainministeriön tietoturvallisuutta koskevat ohjeet sekä kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamat kansainvälisten tietoturvallisuusvelvoitteiden toteutumista koskevat säännökset ja ohjeet.

lisia kustannuksia. Viranomaiset voivat kuitenkin osana normaalia toiminnan kehittämistä tehdä itse viranomaisarviointiin valmistavia sisäisiä arviointeja tai itsearviointeja. Erityisesti muutosten yhteydessä toiminnan arvioiminen on tärkeää. Ohjatuissa sisäisissä arvioinneissa ja itsearvioinneissa voidaan myös hyödyntää ulkopuolisia palveluntuottajia.

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 perusteella.

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 perusteella luovutetaan salassa pidettävää tietoa.

Viranomainen voi luovuttaa tietoja ulkopuolisille tahoille 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 päätös. Nämä tilanteet poikkeavat kuitenkin toimeksiantoon perustuvasta tietojen luovuttamisesta ja sopimukseen perustuvien tietoturvallisuusmenettelyiden todentamisesta, joita käsitellään seuraavassa.

Yksityiset yritykset sopijakumppanina

Yksityiset yritykset ja muut vastaavat toimijat eivät ole velvoitettuja noudattamaan julkisuuslain hyvää tiedonhallintatapaa tai tietoturvallisuusasetuksen vaatimuksia ilman erillistä sopimusta. Tietoturvallisuusvaatimukset ovat siis huomioitava hankinta- tai muussa sopimuksessa ja tämä voidaan toteuttaa turvallisuussopimusmenettelyllä VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohjeen ja VAHTI 2/2013 Toimitilojen tietoturvaohjeen mukaisesti. Myös ICT-varautumisvaatimukset on huomioitava sopimuksessa, jos ne liittyvät sopimuksen kohteeseen.

Tietoturvavelvoitteiden noudattaminen voidaan todentaa ulkoisella arvioinnilla tai sopijakumppanin itsearvioinnilla viranomaisen harkinnan perusteella. Tässä tulee huomioida salassa pidettävien tietojen määrä ja suojaustaso. Jos tietoja käsitellään sähköisesti, voi todennukseen liittyä myös tietojärjestelmän auditointi. Jos kyseessä on puolustus- tai turvallisuushankinta, voi hankintayksikkö edellyttää tarjouskilpailuun osallistujalta tai voittajaksi valitulta tarjoajalta yritysturvallisuusselvitystodistusta.

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[14].

Valtionhallinnon viranomaisten välisissä sopimuksissa, joissa sopijapuolet luovuttavat salassa pidettävää tietoa, sopijapuolet toteavat minkä suojaustason mukaista tietoa sopimuksen perusteella luovutetaan, tai jos kyseessä on tietojärjestelmää taikka tietoliikennejärjestelyä koskeva sopimus, minkä suojaustason mukaisia vaatimuksia järjestelmään sovelletaan. Tietoturvallisuusvaatimusten noudattamisen todentamiseksi tietoja luovuttava taho voi pyytää selvityksen siitä, että tietoja vastaanottava taho on tehnyt asiakirjojen luokittelua koskevan päätöksen ja noudattaa soveltuvaa tietoturvallisuuden tasoa. Tietoturvallisuuden tason noudattaminen voidaan tarpeen mukaan osoittaa 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 ole tarvetta suorittaa tietoturvallisuuden arviointia uudelleen.

Koska valtionhallinnon viranomaiset noudattavat suoraan lain perusteella tietoturvallisuusvaatimuksia ja ovat siis lain velvoittamina vastuussa tietoturvatoimenpiteiden toteuttamisesta, ei vaatimusten noudattamisesta ole tarpeen sopia yhtä kattavalla turvallisuussopimus-

---

[14] Valtio on perinteisesti katsottu yhdeksi oikeushenkilöksi, joka muodostuu toimielinten kokonaisuudesta. Näiden yksiköiden voidaan siten katsoa kuuluvan samaan oikeushenkilöön, jolloin niiden välisissä suhteissa ei yleensä ole kysymys hankintalainsäädännön alaan kuuluvista sopimuksista.

järjestelyillä kuin yksityisten yritysten osalta. Viranomaisten välisiin sopimusjärjestelyihin tulee siksi soveltaa kevyempiä tietoturvallisuuden todentamismenettelyjä ja päällekkäisiä turvallisuusselvityksiä sekä tietoturvallisuusarviointeja on vältettävä.

Sopijakumppanina julkisuuslain mukainen viranomainen

Valtionhallintoon kuulumattomat viranomaiset eivät ole velvoitettuja noudattamaan tietoturvallisuusasetusta, mutta niiden on kuitenkin noudatettava julkisuuslakia mukaan lukien sen salassapitomääräykset ja hyvä tiedonhallintatapa. Julkisuuslain soveltamisalaan kuuluvia tahoja ovat muun muassa valtion liikelaitokset, kunnalliset viranomaiset, julkisoikeudelliset laitokset sekä eduskunnan virastot ja 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 riippuen valtionhallinnon viranomaisen harkinnasta.

Sopijakumppanina ulkomainen taho

Viranomaisen tulee varmistua tietoturvallisuusvaatimusten 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.[15] Turvallisuusluokiteltujen tietojen suojaamista koskevissa valtiosopimuksissa voidaan edellyttää henkilö- ja yhteisöturvallisuusselvitysten 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, riippuen tiedon suojaustasosta, yhteisöturvallisuus- ja henkilöturvallisuusselvitykset.[16] Jos käsiteltävä tieto on muuta salassa pidettävää tietoa (esimerkiksi liikesalaisuudet tai arkaluontoiset henkilötiedot), on turvallisuusvaatimusten todentaminen ja mahdollisuudet arvioinnin suorittamiseen ulkomailla arvioitava tapauskohtaisesti viranomaisen harkinnan perusteella. Jos vaatimusten noudattamisesta ei voida riittävällä tavalla varmentua, on harkittava, voidaanko salassa pidettävää tietoa ylipäätään luovuttaa ulkomaille.

---

[15] Turvallisuusselvityslain (HE 57/2013) mukaan valtioneuvoston asetuksella voidaan säätää, että valtionhallinnon viranomaisen on hankittava henkilöturvallisuusselvitys henkilöstä, jolla on muutoin kuin satunnaisesti oikeus käsitellä suojaustasoihin I tai II luokiteltuja asiakirjoja taikka joka muutoin hoitaa sellaisia tehtäviä, joissa hän salassa pidettäviä tietoja paljastamalla tai muulla lainvastaisella teolla voi merkittävällä tavalla vaarantaa valtion turvallisuutta, maanpuolustusta, kansainvälisiä suhteita, poikkeusoloihin varautumista, väestönsuojelua tai yhteiskunnan elintärkeitä toimintoja taikka mainittujen etujen suojaamiseksi toteutettuja turvallisuusjärjestelyjä.

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

Arviointeihin osallistuvat tahot

Tässä luvussa on kuvattu viranomaisarviointeihin osallistuvat tahot ja niiden roolit. Muita tietoturvallisuuteen liittyviä arviointeja ja tarkastuksia suorittavia viranomaisia on kuvattu liitteessä 6.

Kansallinen turvallisuusviranomainen ja määrätyt turvallisuusviranomaiset

Kansallisen turvallisuusviranomaisen 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 kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan. Lisäksi turvallisuusselvityslain mukaisia henkilöturvallisuusselvityksiä voivat tehdä määrätty poliisihallinnon yksikkö sekä henkilö- ja yritysturvallisuusselvityksiä suojelupoliisi ja pääesikunta.

Viestintävirasto toimii määrättynä turvallisuusviranomaisena ja kansallisena tietoliikenneturvallisuusviranomaisena (National Communications Security Authority, NCSA), joka vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. Viestintävirasto toimii myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen hyväksyntäviranomaisena sekä vastaa tietoturvallisuuden arviointilaitosten hyväksymisestä, ohjaamisesta ja valvonnasta. Lisäksi Viestintävirasto laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen.

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, jos kansainvälinen tietoturvallisuusvelvoite edellyttää toimivaltaisen turvallisuusviranomaisen hyväksyntää. Lisäksi arvio ja tarpeen mukaan hyväksyntä voidaan hakea muulle tietojärjestelmälle esimerkiksi, jos sitä edellytetään viranomaisen riskienarvioinnin tai hallinnonalakohtaisen ohjeistuksen perusteella. Turvallisuusviranomaisen arviointi on ulkopuolinen arviointi, jonka perusteella annetaan viranomaistodistus, jos tietoturvallisuutta koskevat vaatimukset täyttyvät.

Tietoturvallisuuden arviointilaitokset

Arviointitoimintaa harjoittava yritys tai palvelutehtäviä julkishallinnolle tarjoava yksikkö voi hakea toiminnalleen Viestintäviraston hyväksynnän. Hyväksyntä ei ole pakollinen arviointitoiminnan harjoittamiseksi, mutta valtionhallinnon viranomaiset voivat käyttää vuodesta 2015 lähtien tietojärjestelmiensä ja tietoliikennejärjestelyidensä arvioinnissa Viestintäviraston lisäksi vain sen hyväksymiä arviointilaitoksia.

Tietoturvallisuuden arviointilaitos arvioi toimeksiannosta arvioinnin kohteen tietoturvallisuustason. Arviointilaitoksen tulee arvioinnissa selvittää, onko arvioinnin kohteen toiminnassa asianmukaisella tavalla toteutettu ne tietoturvallisuutta koskevat vaatimukset, jotka ovat otettu arvioinnin perustaksi. 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 tavoitteena todentaa, että tietojärjestelmälle asetetut tietoturvallisuusvaatimukset ovat 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.

Valtiovarainministeriö ja VAHTI

Valtiovarainministeriö vastaa valtion tietoturvallisuuden yleisestä ohjauksesta ja koordinoi hallinnon organisaatioiden toimintaa laajasti kansallisessa ja kansainvälisessä tietoturvayhteistyössä. Valtiovarainministeriön ohjausroolia on vahvistettu viimeaikaisen lainsäädännön, kuten valmiuslain, lain julkisen tietohallinnon ohjauksesta 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 (HE54/2013) täsmentävät ja vahvistavat tätä. Yhteiskunnan turvallisuusstrategia ja kyberturvallisuusstrategia sekä muut valtioneuvoston päätökset vahvistavat niin ikään tätä roolia. Valtiovarainministeriössä näistä tehtävistä vastaa ylimmän johdon alaisuudessa toimiva Julkisen hallinnon tieto- ja viestintätekninen toiminto (JulkICT).

Valtiovarainministeriö voi tietoturvallisuuden arviointilain (1406/2011) 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 verkot, keskeiset tietovarannot sekä hallinnon yhteiset, keskeiset salausratkaisut.

Arviointien suorittaminen

Arviointityypit

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

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

Erilaiset arviointikohteet

Tietoturvallisuuden arvioinnit voivat kohdistua erilaisiin kohteisiin. Usein arvioidaan menettelytapoja tai teknisiä järjestelyitä. Kohteesta riippuen arvioinnit voidaan jakaa karkeasti teknisiin ja hallinnollisiin. Teknisissä arvioinneissa tarkastellaan teknisten järjestelyiden riittävyyttä ja asianmukaisuutta, hallinnolliset arvioinnit kohdistuvat toimintaprosesseihin tai menettelytapoihin.

Arvioinnit ovat harvoin luonteeltaan täysin teknisiä, koska myös teknisissä arvioinneissa on aiheellista tarkastella teknisen ympäristön hallinta- tai ylläpitoprosesseja – hyväkään teknisen taso ei säily riittävänä elleivät kyseiset prosessit ole kunnossa. Myös 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 lakisääteiset vaatimukset ja sopimukset. Tiedon luokitus on ratkaiseva tekijä silloin kun valitaan esim. sovellettavaa tietoturvatasoa tai Katakrin 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, joista tulisi käydä ilmi sovellettava arviointiperuste. Jos jotain asiaa ei ole osattu vaatia toimittajalta hankintavaiheessa, niin sen toteuttamista on hankalaa vaatia jälkikäteen.

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 hajasäteilysuojauksessa, kansalliset ja kansainväliset vaatimukset poikkeavat toisistaan. Toteutuksen arvioinnissa tulee käyttää sille hankintavaiheessa asetettuja vaatimuksia.

Hankkeiden elinkaaren aikaiset arvioinnit

Tietojärjestelmähankkeiden arviointi

Tietojärjestelmähankkeiden arviointiin on luotu valtionhallinnon yhteinen arviointikehikko. 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. 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.

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
- 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[17] 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.

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 koko tiedon elinkaaren ajan. Jos toteutustyö ostetaan ulkopuoliselta toimittajalta, niin auditointioikeus on kirjattava sopimuksiin. Tarpeen mukaan toimittajan tietoturvamenettelyitä voidaan auditoida jo ennen sopimuksen allekirjoittamista jolloin se on huomioitava kilpailutusasiakirjoissa. Tarkempaa ohjeistusta aiheesta antaa VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje.

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

- Vaatimusmäärittelyn auditointi/arviointi
- Toteutuksen auditointi valituissa tarkistuspisteissä
- Käyttöönottovaiheessa tehtävä auditointi ennen tuotantoonsiirtoa

VAHTI 1/2013 Sovelluskehityksen tietoturvaohje kuvaa käyttöönottovaiheessa tehtävää tietoturva-auditointia seuraavasti: Korotetun tason sovelluksen tietoturvallisuus on auditoitava ennen käyttöönottoa. 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.

---

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

Luonnollisesti auditoinnit jatkuvat tuotantovaiheessa. Auditointisykli valitaan järjestelmän tai sovelluksen tietoturvatason ja kriittisyyden mukaan.

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.[18]

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 (esim. 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 voi antaa myös 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.

---

[18] 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.

Kuva 3. Tietoturvallisuuden arviointiprosessi

SFS-EN ISO 19011[19] standardi antaa ohjeistuksen erilaisten johtamisjärjestelmien auditointien toteuttamiseen. Kyseistä ohjeistusta ja siinä määriteltyjä auditointien vaiheita voidaan soveltaa myös tietoturvallisuuden arviointiin kuten luvuissa 7.6 – 7.9 on tehty mukaan.

Tietoturvallisuuden arvioinnin suunnittelu

Arvioinnin suunnittelun aloittaminen

Jokaisella arvioinnilla on tilaaja, joka useimmiten on arvioinnin kohteen omistaja. Arvioinnin suunnittelu aloitetaan yleensä määrittelemällä arvioinnin kohde ja arvioinnin 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 tahot ja riittävä kohdealueen osaaminen. Arvioinnin onnistumisen edellytyksenä on, että sille on nimetty vastuullinen vetäjä.

Ensimmäinen yhteydenotto arvioitavaan tahoon

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

---

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

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

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 arvioinnin 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 mahdollisuuksien mukaan selvitykset tehdyistä jatkotoimenpiteistä.

Arviointisuunnitelman laatiminen

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

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

Tietoturvallisuuden arvioinnin toteuttaminen

Aloituskokouksen pitäminen

Arviointi aloitetaan kokouksella, jossa tyypillisesti esitellään arviointiin osallistuvat henkilöt, arvioinnin kohde ja tarkoitus, käytettävä kriteeristö, aikataulu sekä menettelytavat arvioinnin suorittamisessa. 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.

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 mm. 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 (esim. 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.

Kriteeristöjen vaatimusten tulkinta

Tietoturvallisuuden viranomaisarvioinneissa käytettävissä kriteeristöissä esitetään tavallisesti 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 esim. teknisestä syystä täyttää, puutteen korjaamiseksi voidaan toteuttaa ns. korvaavia kontrolleja. Hallinnoiva taho (omistaja) voi riskienhallinnan perusteella päättää, että tietojenkäsittely kokonaisuudessaan on riittävällä tasolla suhteessa suojattaviin intresseihin.

Silloin kun riskienarvioinnin perusteella todetaan, että kaikkien yksittäisten vaatimusten täyttäminen ei ole tarpeellista ja tarkoituksenmukaista, niin arvioinnista täytyy tuottaa kir-

jallinen raportti, joka organisaation johdon tulee hyväksyä. Tämä menettely on kuvattu esim. tietoturvatasojen osalta VAHTI 2/2010 –ohjeen liitteessä 6, Korvaava menettely.

Tietoturvallisuuden arvioinnin raportointi

Arviointiraportin laatiminen

Arvioijan tulee laatia valmistuneesta arvioinnista raportti, jossa kuvataan auditoinnin kohde, rajaukset ja auditoinnin 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.

Arvioinnin kohteelle raporttiluonnos on hyvä antaa etukäteen tutustumista sekä asiavirheiden ja väärinkäsitysten korjaamista varten.

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
Vastine	Miten arvioinnin kohde suhtautuu havaintoon ja mitä se aikoo asialle tehdä (huom. vastinetekstin 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.

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.

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.

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 samassa, hyvin suojatussa paikassa. Koska tallennetuilla raporteilla on tärkeä rooli riskienhallinnassa niin, 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.

Arvioinnin seuranta

Osana arviointiprosessia on arviointiraportin tulosten perusteella määriteltyjen jatko- ja kehittämistoimenpiteiden toteutuksen seuranta. 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, niin 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 jatkotoimenpidesuunnitelman arvioinnin tulosten pohjalta.

Liite 1 Käsitteistö

arviointi (evaluation, assessment)
sen seikan selvittäminen, täyttääkö tietty kohde sille asetetut vaatimukset eri osiltaan. 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

hyväksyntä/akkreditointi (accreditation)
prosessi, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen antaa virallisen lausunnon siitä, että 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.

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

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

itsearviointi
arvioinnin kohteen itsensä suorittama kohteen vaatimustenmukaisuuden arviointi.

sisäinen arviointi
Organisaation tietoturvahenkilöstön tai asiantuntijoiden toteuttama arviointi.

ulkoinen arviointi
Organisaation ulkopuolisen, riippumattoman toimijan suorittama arviointi

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

vertaisarviointi

Arvioijina toimivat henkilöt, jotka työskentelevät samankaltaisen kohteen parissa toisessa organisaatiossa

ulkoinen arviointi

poikkeama
vaatimuksen täyttymättä jääminen

omistaja (owner)
nimetty taho, jolla on valta tai valtuudet päättää suojattavasta kohteesta (esim. järjestelmästä)

vaatimus (requirement)

kriteeri (criterion)

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

erityissuojattava tietoaineisto
EU turvasäännön mukaan kansainvälisen tietoturvallisuusvelvoitteen mukaisesti turvallisuusluokitellut asiakirjat

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.

VTV:n 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 ennakolta 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.

STM:n arvioinnit
Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa 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 itsearviointiin. 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§ 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.