Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, hankintapäälliköt, hankintaprosessin avainhenkilöt, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen ja hankinnan projektivalmistelua	
13 § Tietoturvallisuus hankinnoissa	versio 0.95/1.11.2019

13.4 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus
Viranomaisten on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.

Hallituksen esitys HE 284/2018
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Viranomaisen on tunnistettava hankittavaan tietojärjestelmään kohdistuvat tietoturvavaatimukset osana hankinnan vaatimusmäärittelyä. Tietoturvavaatimusten tulee sisältää tiedonhallintalain asettamat tietoturvallisuuden vähimmäisvaatimukset, jotka on lueteltu kortissa **Suositukset tietoturvallisuudesta**. Tietojärjestelmän tietoturvallisuusvaatimukset muodostuvat näistä vähimmäisvaatimuksista sekä **riskiarvioinnin** avulla tunnistetuista muista mahdollisista vaatimuksista. Kunkin vaatimuksen toteuttamisen menettely arvioidaan riskiarviointiprosessin avulla.

Tietoturvallisuudella on keskeinen rooli kaikissa tiedonhallinnan kannalta keskeisissä hankinnoissa, koskivat ne sitten tietojärjestelmiä, tuotteita tai ICT-palveluita. Hankinnoissa tavoitellaan tarkoituksenmukaista ja laadukasta sekä kustannustehokasta tietojärjestelmää, tuotetta tai palvelua, jossa tietoturvallisuus on keskeinen osa laatua. Vastuullinen organisaatio osaa ottaa tämän huomioon kaikissa hankintaprosessin vaiheissa varmistaen hankintaan ja sen kohteeseen liittyen lain- ja vaatimustenmukaisuuden, muuttuvan uhka- ja toimintaympäristön vaikutuksen sekä organisaation asettaman tietoturvatason toteutumisen. Hankinnan kohteen lisäksi myös hankintaprosessiin itseensä liittyy vaatimuksia ja riskejä, jotka tulee huomioida ja hallita osana hankintaa.

Tietoturvallisuus huomioidaan kaikissa hankinnoissa hankinnan suunnittelusta ja valmistelusta alkaen, jotta mahdolliset riskit ja muut vaikutukset tulevat arvioiduksi ja hallituksi hankintaprosessin kautta asianmukaisesti jo heti alusta asti. Hankinnoissa arvioidaan hankittavan tietojärjestelmän, tuotteen tai palvelun merkitys organisaatiolle ja sen toiminnalle suhteuttaen hankintaprosessi sekä riskienhallintakeinot tähän.

Tietoturvavaatimuksia ja suojauskeinoja määritettäessä tarkastellaan tietoturvallisuutta hankittavan tietojärjestelmän, tuotteen tai palvelun koko elinkaaren ajan alkaen hankinnan valmistelusta, jatkuen hankintaprosessin kautta käyttöönotto- ja tuotantovaiheisiin, päättyen lopulta käytöstä poistoon tai palvelun päättymiseen.

Hankintaohjeistus
Tietoturvallisuuden rooli ja sen huomioiminen ovat keskeinen osa organisaation hankintastrategiaa, hankintaohjesääntöä ja muuta hankintoihin liittyvää ohjeistusta. Hankintoihin liittyvä prosessi ohjaa suorittamaan tietoturvallisuuden varmistamisen kannalta keskeiset toimet selkeästi määritetyillä vastuilla ja tehtävillä, joiden toteuttamista tuetaan tarvittavilla malleilla ja työkaluilla. Hankinnan toteuttamisessa noudatetaan hankintaprosessia ja siitä annettuja ohjeita. Hankintaprosessi ja siihen liittyvät toimintatavat on perehdytetty tarvittaville rooleille hankintaprosessin tehokkaan ja asianmukaisen toteuttamisen varmistamiseksi.

Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, hankintapäälliköt, hankintaprosessin avainhenkilöt, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen ja hankinnan projektivalmistelua

13 § Tietoturvallisuus hankinnoissa	versio 0.95/1.11.2019

Hankintaan ja kumppanienhallintaan liittyvät mallit luovat osaltaan viitekehyksen hankinnan ja palvelutoimittajan luokittelemiseksi sekä luokittelun mukaisten käytänteiden muodostumiseksi. Nämä ohjaavat myös tietoturvallisuusvaatimusten asettamista ja riskienhallinnan toteuttamista.

Osana hankintaohjeistusta ja hankinnan tukimateriaalia voi olla lisäksi valmiiksi laadittuja vaatimusmäärittelyitä ja tietoturvavaatimuksia, mutta ne käydään aina tapauskohtaisesti läpi täsmentäen ja täydentäen vaatimukset kyseiseen hankintaan soveltuviksi. Valmiissa ohjeistuksessa ja tukimateriaalissa voidaan ottaa kantaa esimerkiksi ydintoimintajärjestelmien (esim. toiminnanohjausjärjestelmät, asianhallintajärjestelmät, henkilöstöhallinnon), räätälöityjen sovellusten, kaupallisten tuotteiden (laitteet ja valmisohjelmistot), pilvipalveluiden ja tietoturvaratkaisujen hankintaan.

Hankintaprosessiin liittyvissä ohjeistuksissa huomioidaan, että hankinta-asiakirjoja laadittaessa ja käsiteltäessä sekä tarjousten käsittelyssä pitää huomioida niiden julkisuus ja salassa pidettävyys. Hankintaprosessissa käsiteltävät saadut ja luodut salassa pidettävät asiakirjat tai niiden osat tulee suojata niiden edellyttämällä tavalla huomioiden sekä tietoturvan vähimmäisvaatimukset että tarvittaessa turvallisuusluokkaa koskevat vaatimukset.

Hankinnan suunnittelu ja valmistelu
Hankinnan suunnittelu- ja valmisteluvaiheessa määritetään hankintaa koskevat puitteet ja edellytykset, kuten hankinnan tavoitteet, aikataulut, vaadittu resursointi ja organisointi sekä hankinnan vaatimukset ja hyväksymiskriteerit.

Hankintaprosessi noudattaa organisaation hankintamallia ja siihen liittyvää ohjeistusta toteuttaen tarvittavat vaiheet ja tuottaen määritetyn dokumentaation. Hankinnan suunnittelu- ja valmisteluvaiheen perusteellisuus suhteutetaan hankinnan laajuuteen ja merkittävyyteen.

Hankinnan suunnittelun ja valmistelun käynnistyksen yhteydessä tunnistetaan lähtökohdat hankinnalle sekä kuvataan ja vahvistetaan organisaation hankintaan kohdistamat vaatimukset ja odotukset. Hankinnan tavoitteet pohjautuvat organisaation toiminnasta lähtöisin olevaan tarpeeseen ja sen täyttämiseen. Organisaation on tunnettava omaan toimintaansa ja hallinnoimaansa tietoon kohdistuvat ulkoiset vaatimukset ja sisäiset määritykset sekä toiminnastaan muodostuvat tarpeensa ja kyettävä välittämään ne toimittajalle osana hankintaa. Lisäksi suunnittelun ja valmistelun käynnistyksen yhteydessä perustetaan ja resursoidaan hankinnan suunnittelu- ja valmistelutyö sekä siihen liittyvä organisaatio.

Hankinnan tavoitteista muodostetaan tietojärjestelmälle, tuotteelle tai palvelulle vaatimusmäärittely, joka sisältää myös tietoturvallisuutta koskevat vaatimukset. Vaatimusmäärittelyn tarkoituksena on määrittää vaatimukset hankinnan kohteen tavoiteltavalle lopputulokselle eli tietojärjestelmän tai tuotteen toiminnallisuuksille, teknisille reunaehdoille ja laadullisille ominaisuuksille sekä palvelun palvelutasolle ja laadulle. Vaatimusmäärittelyssä huomioidaan muun muassa hankinnan kohteeseen liittyviä tekijöitä, kuten suorituskyky ja palvelutaso, kapasiteetti, jatkuvuus- ja toipuminen, skaalautuvuus, yhteensopivuus sekä turvallisuus. Tietoturvavaatimusten tunnistaminen ja kohdentaminen tapahtuvat siis osana hankinnan vaatimusmäärittelyä.

Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, hankintapäälliköt, hankintaprosessin avainhenkilöt, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen ja hankinnan projektivalmistelua

13 § Tietoturvallisuus hankinnoissa	versio 0.95/1.11.2019

Tiedonhallintalain asettamien **vähimmäisvaatimusten** ylittäviä vaatimuksia määritettäessä ja asetettaessa on kyettävä arvioimaan niiden soveltuvuus ja sovellettavuus hankinnan kohteeseen, koska ylimitoitetut ja turhat vaatimukset voivat aiheuttaa lisäkustannuksia sekä vaikuttaa hankittavan tietojärjestelmän, tuotteen tai palvelun käytettävyyteen ja tehokkuuteen. Vaatimusten on oltava perusteltuja ja asianmukaisesti määriteltyjä. Tähän liittyy keskeisesti organisaation laatimien standardisopimuslausekkeiden ja vaatimuslistojen asianmukaisuuden ja kyseiseen hankintaan soveltuvuuden arvioiminen sekä tarvittavien täsmennysten ja muutosten tunnistaminen.

Vaatimusmäärittelyä ohjaavat organisaation tarve ja tavoitteet, ulkoiset vaatimukset (kuten erityislainsäädäntö, määräykset ja muiden sidosryhmien asettamat vaatimukset), sisäisesti asetetut vaatimukset (kuten määritetty tietoturvataso ja siihen liittyvät suojauskeinot, linjaukset ja periaatteet) sekä tunnistetut riskit ja niille määritetyt hallintakeinot. On keskeistä, että hankinnan suunnittelu- ja valmistelutyössä tunnistetaan hankinnan kohteena olevan tietojärjestelmän tai tuotteen sekä palvelutoimittajan käsiteltäväksi tulevat tiedot ja niihin kohdistuvat vaatimukset.

Vaatimusmäärittelyssä huomioidaan sekä hankinnan kohteena olevaan tietojärjestelmään tai tuotteeseen että sitä toimittavaan tai palvelua tarjoavaan organisaation kohdistuvat vaatimukset. Osana hankintaa asetetaan hallinnollisia ja teknisiä tietoturvavaatimuksia. Tietojärjestelmä ja tuotehankinnan kohdalla vaatimusmäärittelyssä keskeisessä roolissa ovat laadun muodostavien ominaisuuksien, kuten ratkaisun toiminnallisen sopivuuden, tehokkuuden, yhteensopivuuden käytettävyyden, luotettavuuden, turvallisuuden, ylläpidettävyyden ja siirrettävyyden sekä näihin liittyvien laatupiirteiden, käsittely. Tiedon käsittelyä koskevat vaatimukset määritetään kattaen tiedon elinkaaren kaikki vaiheet ja toimittajan toimintaa koskevat vaatimukset ottavat huomioon muun muassa tärkeät tietoturvallisuutta koskevat käytänteet, kuten tietoturva-arkkitehtuuriperiaatteet, tietoturvallisen sovelluskehityksen periaatteet ja operatiiviset tietoturvallisuusperiaatteet.

Riskien arviointi on keskeistä hankinnan suunnittelussa ja siihen liittyvässä vaatimusmäärittelyssä. Hankinnan kohteeseen liittyvän toiminnan ja siinä käsiteltävien tietojen kriittisyyden ja tärkeyden sekä riskien arviointi tulee tehdä useasta näkökulmasta, huomioiden muun muassa toiminnan kriittisyyden, jatkuvuuden ja tietoturvallisuuden sekä toiminnalliset vaatimukset. Riskien arvioinnin avulla varmistetaan myös hankinnan kohteessa mahdollisesti käsiteltävien henkilötietojen ja salassa pidettävien tietojen käsittelyn edellytykset sekä asetetaan hankinnan kohteelle tietoturvallisuuden ja tietosuojan täsmälliset vaatimukset sekä käsittelyn ehdot. Jos hankinnan kohteeseen liittyy henkilötietojen käsittelyä ja käsittelystä saattaa aiheutua korkea riski rekisteröidylle, riskien arviointiin voi olla edellytyksenä sisällyttää myös EU yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi. Joka tapauksessa tietosuojariskit arvioidaan aina osana riskien arviointia, jos hankinnan kohteeseen liittyy henkilötietojen käsittelyä.

Arvioinneissa huomioidaan lisäksi aina hankinnan kohteen riippuvuudet muusta toiminnasta ja toimintaympäristöstä sekä suunnitella sen suhde olemassa oleviin muihin palveluihin, tukipalveluihin ja tietojenkäsittely-ympäristöihin, jotta varmistetaan luottamuksellisuus, eheys ja saatavuus sekä käytettävyys.

Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, hankintapäälliköt, hankintaprosessin avainhenkilöt, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen ja hankinnan projektivalmistelua

13 § Tietoturvallisuus hankinnoissa	versio 0.95/1.11.2019

Arvioinneissa sekä vaatimusmäärittelyissä hyödynnetään laajasti niin toiminnan ja tiedon omistajia, kuin riskienhallinnan, tietoturvallisuuden ja tietosuojan asiantuntijoita, jotta hankinnan kohteelle asetettavat vaatimukset vastaavat asianmukaisesti toimintaan ja hankinnan kohteeseen tunnistettuja riskejä, vaatimuksia ja hyviä käytäntöjä. Tarvittavat asiantuntijat kytketään osaksi hankintaprosessia jo alkuvaiheessa, jotta tarvittavat näkökulmat otetaan huomioon riittävän ajoissa. Mikäli organisaatiolla ei ole jollain tarvittavalla osa-alueella itsellään tarvittavaa osaamista tai muuten resursseja, voidaan käyttää ulkopuolista asiantuntemusta hankintaprosessin tukena.

Hankinnan kohteen tietoturvallisuuden varmistamiseen varaudutaan ennakolta myös alustavalla budjetoinnilla hankinnan valmistelun yhteydessä. Hankinnan mitoituksen suunnittelussa muodostetaan kuva hankinnan laajuudesta, kustannuksista, työmäärästä ja aikataulusta luoden myös tarvittavat edellytykset onnistuneen hankinnan toteuttamiselle.

Keskeisiä hankinnan suunnitteluun ja valmisteluun liittyviä tietoturvatehtäviä ovat:

- Suunnitella hankinnan läpivienti hankinnalle asetettujen tavoitteiden saavuttamiseksi,
- suunnitella, miten varmistetaan hankinnan kohteen lainmukaisuus muun muassa tietoturvallisuuden ja tietosuojan osalta,
- määrittää, miten hankinnan kohteen tietoturvallisuus mitoitetaan organisaation vaatimusten ja tarpeiden sekä tunnistettujen riskien mukaisesti,
- suunnitella, miten huolehditaan hankinnan kohteessa käsiteltävän ja palvelutoimittajan käsittelemän tiedon riittävästä tietoturvallisuudesta, sekä
- määrittää, miten varmistetaan kohteen palvelutaso organisaation tarpeita vastaavaksi.

Tarjousprosessi sekä tietojärjestelmän ja toimittajan valinta
Tarjouspyyntöprosessissa organisaatio laatii ja lähettää tarjouspyynnön, johon toimittajat vastaavat. Tarjouspyynnöstä käy ilmi suunnittelu- ja valmisteluvaiheessa määritetyt vaatimukset, jotka kaikki kirjataan osaksi tarjouspyyntöä ja siihen kuuluvaa dokumentaatiota. Tähän sisältyvät myös tietoturvallisuutta koskevat vaatimukset, jotka yksilöidään osaksi tarjouspyyntöä, ja joihin vastaamista edellytetään tarjouspyynnössä. Kun tietoturvavaatimukset määritellään huolellisesti ja ilmoitetaan jo tarjouspyyntövaiheessa, varmistetaan että palvelutoimittaja ottaa nämä asiat huomioon tarjousta tehdessään.

Tarjouspyynnössä voidaan asettaa ehdottomia vaatimuksia ja toivottavia ominaisuuksia. Ehdottomien vaatimuksien täyttyminen on edellytys, mutta toivottavia ominaisuuksia voidaan esimerkiksi pisteyttää tarjouksien vertailussa. Ehdottomia vaatimuksia ja toivottavia ominaisuuksia voidaan käyttää myös tietoturvavaatimusten osalta, mutta niiden käyttö ja pisteyttäminen on suunniteltava huolellisesti.

Toimittajat vastaavat esitettyihin vaatimuksiin tarjouspyyntöprosessin mukaisesti tarjouksin ottaen kantaa myös tietoturvaa koskeviin vaatimuksiin. Tässä huomioidaan myös mahdolliset palvelun tuottamiseen osallistuvat alihankkijat sekä vaatimusten edellyttäminen myös heiltä.

Tarjouspyynnöissä sekä tarjouksissa on huomioitava, että tiukat tietoturvallisuutta koskevat vaatimukset saattavat aiheuttaa toimittajalle kustannuksia ja erityisjärjestelyitä vakiomuotoisiin palvelutuotantomalleihin, mikä voi vaikuttaa tietojärjestelmän, tuotteen tai palvelun kustannuksiin.

Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, hankintapäälliköt, hankintaprosessin avainhenkilöt, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen ja hankinnan projektivalmistelua

13 § Tietoturvallisuus hankinnoissa	versio 0.95/1.11.2019

Tarjousten vertailun ja neuvotteluiden pohjalta tehdään päätös tietojärjestelmän, tuotteen ja/tai palvelun hankinnasta. Osana tarjousten vertailua ja neuvotteluita käytetään hankinnan suunnittelu- ja valmistelutyön tapaan tarvittavia asiantuntijoita, jotta vaaditut näkökulmat tulee huomioitua riittävällä asiantuntemuksella.

Tarjousvaiheen päätteeksi tehdään päätös tietojärjestelmän, tuotteen ja/tai palvelun toimittajasta ja edetään tämän kanssa sopimusvaiheeseen.

Sopimuksen teko
Kaikissa hankinnoissa tehdään osapuolten välillä kirjallinen sopimus. Sopimuksella määritetään osapuolten vastuut ja velvoitteet. Turvallisuutta koskevat asiat on hyvä määrittää erillisessä turvallisuussopimuksessa, jonka laajuus ja sisältö riippuvat hankinnan kohteesta. Turvallisuussopimuksen lisäksi sopimuksessa on keskeistä määrittää mahdolliseen hankittavaan palveluun liittyvät vaaditut palvelutasot koskien muun muassa toimitusvarmuutta, asiantuntijaresursseja ja tukea.

Sopimusdokumentaatioon kuvattavat tietoturvallisuusvaatimukset ovat samat, jotka ovat määritetty hankinnan suunnittelu- ja valmisteluvaiheen vaatimusmäärittelyssä ja jotka ovat olleet osana tarjouspyyntöä. Vaatimusten täyttämistä edellytetään sopimuksessa, koska muutoin toimittajalla ei ole velvollisuutta huomioida niitä lukuun ottamatta lakisääteisiä vaatimuksia. Jos vaatimukset muuttuvat myöhemmin, toimittaja ei ole velvoitettu muutoksiin, joita ei ole kirjattu sopimuksiin. Tällöin on seurattava sopimusmuutoksia koskevaa prosessia vaatimusten päivittämiseksi ja tämä voi aiheuttaa muutoksia myös kustannuksiin.

Turvallisuussopimuksen lisäksi voi olla tarpeen edellyttää sopimuksen toteuttamiseen liittyviltä toimittajan työntekijöiltä vielä erillisiä turvallisuusselvityksiä ja vaitiolositoumusta, joiden käyttöön liittyvät periaatteet on hyvä määrittää esimerkiksi osaksi hankintaohjeistusta.

Osana sopimuksen tekoa on myös huomioitava hankinnan kohteeseen liittyvistä immateriaalioikeuksista sopiminen eli sopia palvelun tai toimituksen lopputulokseen liittyvistä immateriaalioikeuksista.

Sopimukseen kirjattavia vaatimuksia on kyettävä myös valvomaan ja seuramaan, mikä edellyttää tarvittavien suorituskykymittarien luomista ja auditointioikeutta sekä näiden molempien kirjaamista osaksi sopimusta. Mittareiden ja niihin liittyvän raportoinnin avulla valvotaan sopimuskauden aikana muun muassa palvelutasoa. Auditointien avulla on mahdollista arvioida toimittajan sopimusvaatimustenmukaisuutta sopimuskauden aikana ja joissain tapauksissa se voi olla tarpeellista jo ennen sopimuksen allekirjoittamista.

Vaatimusten ja palvelutasojen määrittämisen lisäksi osaksi sopimusta kuvataan niissä esiintyvistä poikkeamista seuraavat sanktiot ja sanktioiden kumuloituminen.

Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, hankintapäälliköt, hankintaprosessin avainhenkilöt, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen ja hankinnan projektivalmistelua

13 § Tietoturvallisuus hankinnoissa	versio 0.95/1.11.2019

Ennen sopimuksen viimeistelyä ja allekirjoittamista sen asianmukaisuus varmistetaan tarvittavilta asiantuntijoilta, kuten riittävän sopimuslainsäädännön ja tietoturvaosaamisen omaavilta henkilöiltä.

Sopimuksen teossa keskeistä tietoturvanäkökulmasta on:

- Kuvata tarvittavat suojaustoimet ja kontrollit tietoturvavaatimuksiksi,
- määritellä tarvittavat mittarit sekä niitä tukeva raportointi ja valvonta, mukaan lukien auditointioikeus, sekä
- määritellä sanktiot poikkeamille vaatimuksista ja palvelutasoista.

Hankinnan kohteen toteutus ja käyttöönotto
Hankinnan kohteena olevan tietojärjestelmän tai tuotteen toteutusvaiheen sekä palveluun liittyvän projekti- ja käynnistysvaiheen aikana varmistetaan prosessin eteneminen ja tulosten laatu. Päätöksentekopisteissä arvioidaan toteutusvaiheen aikaansaannokset ja niiden vastaavuus suhteessa asetettuihin vaatimuksiin joko hyväksyen, hyläten tai palauttaen ne korjattavaksi. Tavoitteena on, että toteutusvaiheen jälkeen on käyttöönotettavissa hankinnalle asetettujen tavoitteiden ja määritettyjen vaatimusten mukainen tietojärjestelmä, tuote ja/tai palvelu.

Jos toteutusvaihe sisältää tietojärjestelmän tai ohjelmiston kehitystyötä, on tärkeää sopia ja varmistaa kehitysmallin asianmukaisuus sekä tietoturvatoimenpiteiden huomioiminen osana kehitysmallia. Käytännöt sovitaan yhdessä toimittajan kanssa.

Tietoturvallisuuden varmistamiseksi suunnitellaan ja päätetään tietoturvatestauksen ja -arviointien toteuttamisen laajuus, sisältö ja aikataulu niin, että ne toteutuvat riittävässä laajuudessa jo tuotannon aikana sekä ennen käyttöönottoa tai suojattavien tietojen käsittelyn aloittamista. Vähintään merkittävissä hankinnoissa hankittavan tietojärjestelmän, tuotteen ja/tai palvelun vaatimustenmukaisuus on hyvä varmistaa auditoinnilla ennen käyttöönottoa. Hankinnan kohteen tietoturvallisuuden suunnitelmalliseen varmistamiseen sisältyy hankinnan kohteesta riippuen tarvittava määrä tietoturvatestauksia, tietoturva-arviointeja sekä muuta varmistamista. Näihin voi lukeutua muun muassa koodi- ja arkkitehtuurikatselmoinnit, penetraatiotestaukset, konfiguraatiotarkastukset ja hallinnolliset auditoinnit.

Kun asetettujen vaatimusten toteutuminen on todennettu hyväksymistarkastuksessa ja hyväksymiskriteerit täyttyvät, voidaan tehdä hyväksyntä- ja käyttöönottopäätös. Päätöksen tekemisestä vastaa organisaation tähän määrittämässä roolissa toimiva henkilö ja päätös dokumentoidaan. Toteutuksen edettyä hyväksytysti käyttöönottovalmiuteen edetään hankintaprosessin viimeistelyyn ja päättämiseen. Tässä vaiheessa muun muassa arvioidaan ja todetaan, ovatko kaikki hankinnan kohteena olevat tietojärjestelmät, tuotteet ja/tai palvelut toimitettu ja käyttöönotettu asetettujen vaatimusten mukaisina ja hyväksytysti.

Tuotanto ja käytöstä poisto tai sopimuksen päättyminen
Osana hankinnan suunnittelua ja valmistelua sekä tarjous- ja sopimusprosesseja huomioidaan myös vaatimusmäärittelyt koskien tuotannon aikaista toimintaa sekä tietojärjestelmän tai tuotteen käytöstä poistoa ja palvelusopimuksen päättymistä. Asetetut vaatimukset varmistavat sen, että tiedosta, tietoturvallisuudesta ja toiminnan jatkuvuudesta huolehditaan myös tuotannosta poistamisessa sekä

korvaavan ratkaisun käyttöön siirtymisessä. Vastaavasti sama varmistetaan myös palvelusopimuksen päättymisen ja uudelle toimittajalle siirtymisen osalta.

Sopimuksen päättymisen lähestyessä organisaatiolla on olemassa olevat toimintamallit ja suunnitelmat sopimuksen päättämisestä ja palveluiden siirtämisestä tai sopimuksen uusimisesta ja uudelleen neuvottelusta. Tämä huomioidaan muun muassa määrittämällä tarvittavat vaatimukset koskien avustusvelvollisuutta sekä tietojen ja tietojärjestelmien siirtoa toiselle palvelutoimittajalle. Ohjelmistohankintojen osalta voi olla myös perusteltua escrow-järjestelyistä sopiminen, missä ohjelmiston lähdekoodi ja muu tärkeä aineisto tallennetaan kolmannelle osapuolelle toimittajan mahdollisen vakavan häiriön tai toiminnan lakkaamisen varalta.

Auditointeja on hyvä suorittaa organisaation auditointisuunnitelman ja kumppanienhallintamallin mukaisesti myös sopimuskauden ja jatkuvan tuotannon aikana ja varsinkin suurempien hankinnan kohteeseen liittyvien ympäristömuutosten yhteydessä.

Hankinnan kohteen auditointi
Hankinnan kohteeseen kohdistuvien auditointien auditointikriteeristönä käytetään hankinnan kohteelle määritettyä vaatimuslistaa ja muuta keskeistä sopimusdokumentaatiota, jota voidaan täydentää yksityiskohtaisemmaksi tarkistuslistaksi tai auditointimalliksi muun muassa vaatimuskohtaisin tulkintaohjein. Auditoinnit suoritetaan tietojärjestelmä-, tuote- tai palvelutoimituskohtaisesti siihen liittyvien rajausten mukaisesti. Esimerkiksi palvelutoimitusta auditoitaessa, ei ole välttämättä perusteltua ja tarpeen arvioida toimittajan kaikkea palvelutuotantoa, vaan nimenomaan hankittua palvelua.

Tietoturvallisuuden varmistamiseen liittyvien auditointien ja kumppaninhallinnan yhteydessä esille nousseiden havaintojen ja riskien käsittelyssä sovittujen hallintatoimenpiteiden toteutus ja seuranta vastuutetaan ja aikataulutetaan. Toimenpiteiden toteutumista sekä mahdollisia jäännösriskejä seurataan ja arvioidaan säännöllisesti.

Laki julkisista hankinnoista ja käyttöoikeussopimuksista
EU:n yleinen tietosuoja-asetus

Kortti Suositukset tietoturvallisuudesta

ENISA, Security Guide for ICT Procurement
https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement
VAHTI-ohje 2/2014, Tietoturvallisuuden arviointiohje
https://www.vahtiohje.fi/web/guest/2/2014-tietoturvallisuuden-arviointiohje
VAHTI-ohje 1/2013, Sovelluskehityksen tietoturvaohje
https://www.vahtiohje.fi/web/guest/vahti-1/2013-sovelluskehityksen-tietoturvaohje
VAHTI-ohje 3/2011, Valtion ICT-hankintojen tietoturvaohje
https://www.vahtiohje.fi/web/guest/3/2011-valtion-ict-hankintojen-tietoturvaohje

Sanasto

Kyberturvallisuussanasto
https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf
Kokonaisturvallisuussanasto
http://www.tsk.fi/tiedostot/pdf/Kokonaisturvallisuuden_sanasto_2.pdf
Valtionhallinnon tietoturvasanasto
https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto
VAHTI-ohjeen 2/2014, Tietoturvallisuuden arviointiohje, käsitteistö
https://www.vahtiohje.fi/web/guest/2/2014-tietoturvallisuuden-arviointiohje

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

Auditointi on riippumattoman tahon suorittama kohteen, sen toiminnan ja toiminnan tulosten yleensä määräajoin tapahtuva tutkiminen sen selvittämiseksi, vastaako kohde siihen kohdistuvia vaatimuksia.

Escrow-menettelyssä ohjelmiston lähdekoodi talletetaan kolmannen osapuolen, nk. escrow-agentin, haltuun. Ohjelmiston toimittaja ja hankkija tekevät sopimuksen, jossa määritellään ehdot, joiden mukaan escrow-agentti on velvollinen luovuttamaan ohjelmiston lähdekoodin hankintayksikölle. Tällaisia tilanteita voivat olla esimerkiksi toimittajan konkurssi tai ohjelman ylläpidon päättyminen. Escrow-sopimuksen perusteella escrow-agentti säilyttää luotettavalla tavalla ohjelmistotoimittajan sille antamaa lähdekoodia (sen kopiota) ja luovuttaa sen asiakkaalle tietyissä ennalta määritellyissä ohjelmistotoimittajan liiketoiminnan häiriötapauksissa.

Hyväksymistarkastus kattaa toimet, joilla todetaan, täyttääkö tuote tai työn tulos asetetut vaatimukset.

Immateriaalioikeudet ovat aineettomia oikeuksia, mm. tekijänoikeus, patentti-, malli-, tavaramerkki ja toiminimioikeus.

Katselmointi on kohteen tilan arviointi, jonka tarkoituksena on tunnistaa eroavuudet tavoitetilaan nähden ja tuottaa kehitysehdotuksia.

Kontrolli on riskien hallinnan tavoite, keino tai menetelmä, suunnitelmallinen jatkuva toiminta, kertaluonteinen tai toistuva toimenpide, jolla varaudutaan tai suojaudutaan (tieto)turvaloukkauksia tai haitallisia tapahtumia vastaan. Kontrollit ovat ehkäiseviä, havaitsevia (ilmaisevia) tai korjaavia. **Suojauksella** tarkoitetaan haitallisen ulkopuolisen vaikutuksen torjumista tai ennalta ehkäisyä.

Kriteeri on arviointiperuste, jolla todetaan tavoitteen täyttyminen.

Lähdekoodi on tietokoneohjelma ohjelmoijien kirjoittamassa ja ylläpitokelpoisessa muodossa.

Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, hankintapäälliköt, hankintaprosessin avainhenkilöt, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen ja hankinnan projektivalmistelua

13 § Tietoturvallisuus hankinnoissa	versio 0.95/1.11.2019

Suojattava kohde on organisaation toiminnan kannalta merkityksellinen kohde, joka halutaan suojata riskien varalta. Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä, prosessi, fyysinen tila, yksittäinen asiakirja tai työasema.

Testaus on järjestelmän toimivuuden, käytettävyyden, suorituskyvyn, määritysten mukaisuuden tai muun ominaisuuden selvittämiseksi tehtävä toimenpidesarja.

Tietojärjestelmä on ihmisistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi sekä abstrakti systeemi, jonka muodostavat tiedot ja niiden käsittelysäännöt.

Vaatimus on kohteelle asetettu yksittäinen tavoite, joka kohteen tulee pystyä toteuttamaan.