Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua, tietoon kohdistuvien riskien tunnistaminen, arviointi ja asianmukainen hallinta.	
13 § Riskienhallinta	versio 0.9/01.11.2019

13.1 § Riskienhallinta

Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

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

Tietoriskien analyysi ja hallinta

Tiedonhallintayksikön hyvänä käytäntönä on toteuttaa tietoaineistojen, tietovarantojen ja tietojärjestelmien riskienhallintaa[1]:

- Tunnistamalla ja arvioimalla olennaisia riskejä, sekä
- Vähentämällä niiden todennäköisyyttä ja/tai vaikutuksia hyväksyttävälle tasolle ja
- Ylläpitämällä saavutettua tasoa tai
- Vaihtoehtoisesti hyväksymällä jäännösriskit tai osa niistä.

Riskienhallinnalla pyritään toteuttamaan tietoturvallisuustoimenpiteiden yhdistelmä, jolla varmistetaan tietoaineistojen ja tietojärjestelmien riittävä tietoturvallisuuden taso ja saadaan aikaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä. Oikeansuhtainen riskienhallinnan taso voidaan saavuttaa, kun tietoon ja/tai tietojärjestelmiin liittyvät vaikutukset on tunnistettu vaikutusanalyysin avulla ja huomioitu riskin realisoitumisen todennäköisyys.

Tietoriskien hallinta on jatkuvaa toimintaa, johon liittyvät tavoitteet, periaatteet, vastuut ja keskeiset menettelyt tiedonhallintayksikön on hyvä kuvata. Johdon vastuulla on tietoriskien hallinnan organisointi ja resursointi. Tietoriskien hallintaprosessin tyypillisesti vaikuttaa tiedonhallintayksikön toiminnan ja tavoitteiden arviointiin ja suunnitteluun. Tietoriskien hallinnassa havaitut riskit yleisesti vaikuttavat tiedonhallintayksikön toimenpiteisiin sen koko toiminnan aikana.

Tietoriskien hallinnassa käytetään tiedonhallintayksikön tehtävien ja tietoaineistojen laajuuden perusteella valittuja menettelytapoja. Pienissä organisaatioissa tietoriskien koordinointi voi olla vastuutettu yhdelle henkilölle ja organisoitu johdon ja muutaman henkilön yhteistyönä toteutettavaksi. Prosessissa voidaan hyödyntää tavanomaisia toimisto-ohjelmistoja.

Laajemmissa organisaatioissa, ja etenkin ICT-tuotannosta vastaavissa organisaatioissa, riskienhallinnassa tarvitaan sekä useiden asiantuntijoiden että keski- ja ylemmän johdon työpanosta, ja erityisiä riskienhallintaohjelmistoja. Kaikissa organisaatioissa tietoturvariskit on käsiteltävä **johdon sisäisen valvonnan ja riskienhallinnan** arviointi- ja vahvistuslausumassa kerran vuodessa.

Tietoriskien käsittelyssä toimenpiteet mitoitetaan hyväksyttävälle tasolle. Jäännösriskejä ja tietoturvallisuustoimenpiteiden toteutumista seurataan säännöllisesti. Tietoriskien seuranta jatkuu tietoaineistojen ja tietojärjestelmien elinkaaren ajan. Seurannassa tarkistetaan riskienkäsittelysuunnitelmien toteutuminen sekä toteutettujen tietoturvallisuustoimenpiteiden vaikuttavuus.

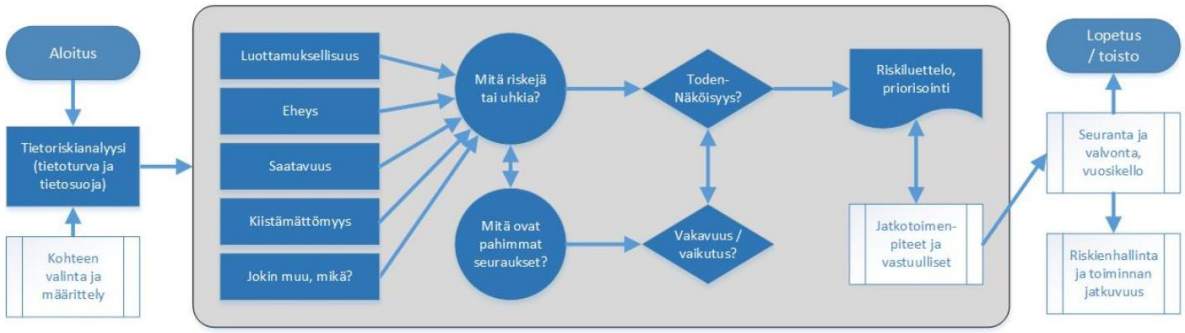
Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua, tietoon kohdistuvien riskien tunnistaminen, arviointi ja asianmukainen hallinta.	
13 § Riskienhallinta	versio 0.9/01.11.2019

Tietoriskien hallinnassa on tärkeää kirjata ylös kaikki potentiaaliset tietoriskit riskirekisteriin ja arvioida ne todennäköisyyden ja vaikutuksen perusteella. Myös tietoriskin syyt ja mahdollisen toteutumisen seuraukset on hyvä kirjata ylös. Usein on helpompaa puuttua riskin syyhyn kuin itse tietoriskiin. Tarkempia ohjeita riskien todennäköisyyden ja vaikutusten arviointiin löytyy tämän ohjeen lopussa viitatusta VM-ohje 22/2017 – Ohje riskienhallintaan.

Tietoriskien kartoittamisen ja arvioinnin lisäksi on hyvä kirjata jo aloitetut tai toteutetut riskinhallintatoimenpiteet sekä potentiaaliset uudet hallintatoimenpiteet. Tietoriskin arvioinnin kohteen omistaja päättää, mitkä hallintatoimenpiteet toteutetaan ja mitkä riskit voidaan hyväksyä sekä kuka vastaa hallintatoimenpiteen toteuttamisesta ja mihin mennessä toteuttamisen tulee olla valmis. Hallintatoimenpiteiden tulee olla suhteutettu riskiarvioinnin perusteella tietoon ja tietojärjestelmään kohdistuviin uhkiin ja seuraksiin.

Riskit ja hallintatoimenpiteet tulee myös huomioida jatkuvuussuunnittelussa, jonka avulla pyritään takaamaan tiedon tai tietojärjestelmän riittävä saatavuus.

Sovittujen hallintatoimenpiteiden toteutumista ja aikataulujen pitävyyttä on hyvä seurata systemaattisesti, esimerkiksi kerran kuukaudessa tai vähintään neljä kertaa vuodessa. Tietoriskin arviointi on hyvä tehdä uudestaan, kun yksi tai useampia hallintatoimenpiteitä on toteutettu.



Kuva 1: Tietoriskianalyysin prosessikaavio[2]

Jäännösriskien hallinta

Hallintatoimenpiteiden jälkeen voimaan jääviä riskejä, joihin ei voida tai haluta enää vaikuttaa, kutsutaan jäännösriskeiksi esimerkiksi hallintakeinojen ollessa riskin vaikutusten suhteen liian kalliitta tai raskaita. Organisaatiolla tulee olla johtoryhmätason hyväksymä menetelmä jäännösriskien käsittelemiseksi ja niiden nostamiseksi tarvittaessa myös johto-ryhmän käsiteltäväksi.

Tietoriskien hallinnassa tarvittavat tietoaineistot

Tietoriskien hallinta perustuu järjestelmälliseen uhkien ja haavoittuvuuksien tunnistamiseen sekä näiden todennäköisyyksien ja vaikuttavuuden arviointiin. Tiedonhallintayksikön on hyvä pitää yllä havainnointikykyään, jotta se voi varautua riskien toteutumiseen etukäteen. Hallinnollisia havainnointitapoja ovat: Poikkeamien hallintatoimenpiteiden toteutumisen seuranta, auditointihavaintojen korjaamistoimenpiteiden seuranta ja riskienhallintatoimenpiteiden seuranta.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua, tietoon kohdistuvien riskien tunnistaminen, arviointi ja asianmukainen hallinta.	
13 § Riskienhallinta	versio 0.9/01.11.2019

Hyvänä käytäntönä tiedonhallintayksikössä on seurata toimintaympäristönsä turvallisuustilannetta viranomaislähteistä sekä viranomaiskontaktien ja mediaseurannan avulla ja valvomalla jatkuvasti tietojärjestelmiänsä ja tietovarantojansa. Mahdollinen erityislainsäädäntö, käytännesäännöt ja muu informaatio-ohjaus sekä tulosohjaus ja taloudelliset voimavarat huomioiden. Traficomin:in Kyberturvallisuuskeskuksen raportit ovat keskeinen viranomaistietolähde, sekä rikosasioissa poliisi.

Julkisen hallinnon on hyvä huomioida tietoturvallisuudesta annetut Vahti-ohjeet, jotka löytyvät liitteinä tämän ohjeen lopusta omassa varautumisessaan. Näihin kuuluu muun muassa tietoturvapoikkeamista mahdollisimman nopeasti tehty ilmoitus Kyberturvallisuuskeskukselle, jotta tietoturvapoikkeaman kohteeksi joutunut viranomainen saa apua tilanteesta toipumiseen. Lisäksi on aina suositeltavaa tehdä rikosilmoitus poliisille, jos rikoksen tunnusmerkit täyttyvät. Oikea-aikainen toiminta koituu sekä julkisen hallinnon että kansalaisten eduksi.

Tietoriskien hallinnassa hyödynnetään tiedonhallintayksikön ylläpitämiä metatietoja koskien tietojärjestelmiä sekä tiedonhallintamallista löytyviä metatietokuvauksia tietoaineistoista ja tietovarannoista ja tietovarantojen ja -järjestelmien tärkeysluokituksista. Erityistä huomiota on kiinnitettävä siihen, missä tietojärjestelmät ja tietovarannot fyysisesti sijaitsevat, ja mitä tietoriskejä tästä toiminta ja kyseessä olevat tietoaineistot huomioiden mahdollisesti aiheutuu.

Tiedonhallintayksikkö ylläpitää riskiarvioiden tuloksista ja riskikäsittelysuunnitelmista muodostuvaa tietoaineistoa sekä arvioi säännöllisesti onko tämä aineisto osin tai kokonaan salassa pidettävä tai turvallisuusluokiteltava. Salassapitosäännösten niin vaatiessa viranomaisen on luokiteltava tietoriskejä koskeva tietoaineisto salassa pidettäviksi sekä turvallisuusluokitteluvaatimusten täyttyessä myös turvallisuusluokiteltava tietoaineisto kokonaan tai osittain.

Yleisiä vaatimuksia

Seuraavat yleiset vaatimukset tulisi huomioida riskienhallinnassa:

- Onko viranomainen tunnistanut, sekä dokumentoinut kaiken tiedon ja tietojärjestelmät joista se on vastuussa?
- Onko näitä ylläpitävät ja käyttävät avainhenkilöt tunnistettu?
- Onko tietoihin, tietojärjestelmiin ja avainhenkilöihin kohdistuvat mahdolliset uhkatekijät tunnistettu?
- Onko tiedolle ja tietojärjestelmille laadittu vaikutusanalyysi, jonka perusteella voidaan arvioida riskienhallinnallisten toimenpiteiden oikeasuhtaisuus?
- Ovatko riskienhallinnalliset toimenpiteet oikeasuhtaiset riskin realisoitumisen vaikutukseen ja todennäköisyyteen nähden?
- Ylläpidetäänkö riskirekisteriä, sekä arvioidaanko riskienhallinnallisten toimenpiteiden toimivuutta säännöllisesti?

[1] ISO31000

[2] VM 22/2017 Ohje riskienhallintaan – Liitteet 1-6

VM Riskienhallinnan järjestäminen

VM Riskienhallintapolitiikkamalli

VM 22/2017 Ohje riskienhallintaan

Riskirekisteri

Riskien arviointityökalu

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua, tietoon kohdistuvien riskien tunnistaminen, arviointi ja asianmukainen hallinta.	
13 § Riskienhallinta	versio 0.9/01.11.2019

Riskienhallintapolitiikka
Riskienhallintaperiaatteet
Yksittäisen kohteen riskienarviointi- ja seurantataulukko
Yksittäisen kohteen tietosuojariskienarviointi- ja seurantataulukko
Riskiprosessin kuvaus, jossa mukana avustavia kysymyksiä
Tietojärjestelmien tärkeysluokittelija

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

Tiedonhallintayksiköitä ovat esimerkiksi organisaatiot, joissa viranomaiset toimivat, kuten valtiovarainministeriö, valtion tieto- ja viestintätekniikkakeskus Valtori, Maanmittauslaitos tai Helsingin kaupunki.

Suojattavien kohteiden tunnistamisella ja dokumentoinnilla tarkoitetaan kaiken tiedonhallintayksikön hallinnassa olevan tiedon sekä järjestelmien ja näihin liittyvien muiden suojattavien kohteiden kuten avainhenkilöiden tunnistamista.

Viranomaisen tulee kyetä tunnistamaan kaikki tieto ja tietojärjestelmät jotka ovat sen vastuulla sekä huomioida näitä ylläpitävät ja käyttävät avainhenkilöt. Jokaiseen tunnistettuun kohteeseen liittyvät riskit ja niiden mahdolliset vaikutukset tulee arvioida ja lisätä organisaation itsensä ylläpitämään riskirekisteriin.

Tietoriskillä tarkoitetaan tietoon kohdistuvaa tai tiedosta aiheutuvaa jonkinlaisen haitan tai vaurion todennäköisyyttä ja sen seurauksia. Tietoriski ilmaistaan tavallisesti riskin lähteiden, mahdollisten tapahtumien, niiden seurausten ja niiden todennäköisyyden yhdistelmänä.

Tietoriskit voivat aiheutua esimerkiksi inhimillisistä virheistä, annettujen ohjeiden puutteista tai noudattamatta jättämisestä, varkauksista tai ilkivallasta, laitteiden, järjestelmien tai ohjelmistojen virheistä ja toimintahäiriöistä, haittaohjelmien leviämisestä, tietoaineistojen tuhoutumisesta taikka alihankkijan tai kumppanuusverkostoon kuuluvan toimijan virheistä tai laiminlyönneistä.

Tietoturvauhkalla tarkoitetaan tietoaineistoihin ja tietojärjestelmiin liittyvällä sellaista tahatonta tai tahallista tekijää, joka vaarantaa tietoaineistojen luottamuksellisuutta, eheyttä tai käytettävyyttä tai tietojärjestelmien käyttöä tai vikasietoisuutta.

Tietoturvauhkat voivat aiheutua esimerkiksi inhimillisistä virheistä, annettujen ohjeiden puutteista tai noudattamatta jättämisestä, varkauksista tai ilkivallasta, laitteiden, järjestelmien tai ohjelmistojen virheistä ja toimintahäiriöistä, haittaohjelmien leviämisestä, tietoaineistojen tuhoutumisesta taikka

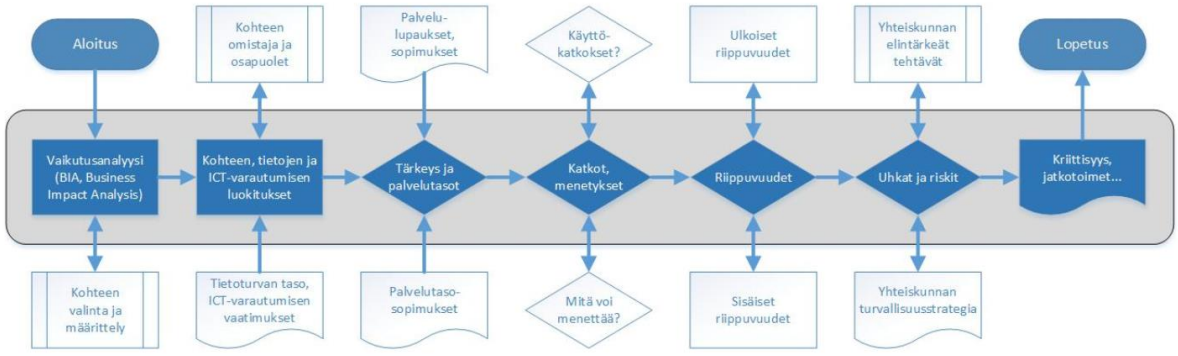
organisaation oman työntekijän, alihankkijan, palveluntoimittajan tai kumppanuusverkostoon kuuluvan toimijan virheistä tai laiminlyönneistä.

Haavoittuvuudet ovat tekijöitä, jotka altistavat tietoaineistot ja tietojärjestelmät uhkille. Esimerkkinä haavoittuvuudesta voi olla vanhentunut järjestelmä joka antaa hyökkääjälle mahdollisuuden hyväksi käyttää teknistä haavoittuvuutta ja saada tätä kautta pääsyn organisaation tietoihin ja täten realisoida tietoturvauhkan.

Tietoturvapoikkeamalla tarkoitetaan tapahtumaa, jossa viranomaisen tietojen ja palvelujen eheys, luottamuksellisuus tai palvelulta vaadittava käytettävyystaso on tai saattaa olla vaarantunut.

Vaikutusanalyysillä tarkoitetaan toiminnan keskeyttävien tai toiminnan jatkuvuutta häiritsevien uhkien tunnistamista sekä toimintaan liittyvien riippuvuuksien tunnistamista. Tieto- ja kyberturvallisuuden näkökulmasta vaikutusanalyysissä erityisesti valtionhallinnon tai muun julkisen sektorin organisaation toiminnan kannalta tarkasteltavia asioita ovat muun muassa:

- Vaikutukset omaan operatiiviseen toimintakykyyn
- Vaikutukset säädösperusteisten tehtävien suorittamiseen (vrt. myös yhteiskunnanelintärkeät tehtävät)
- Vaikutukset yhteiskunnalle
- Riippuvuussuhteet ja niiden vaikutukset:
  - Oman organisaation riippuvuus toisesta osapuolesta tai palvelusta tai toisista organisaatioista tai palveluista
  - Toisen organisaation tai palvelun riippuvuus oman organisaation tuottamasta palvelusta tai toiminnasta



Kuva 2: Vaikutusanalyysin prosessikaavio[2]