DTYT / Reivo Juho (DVV)

9.3.2022

# Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta

## Riskienhallintamallin rakenne

## [LUONNOS]

5.4.2022

DTYT / Reivo Juho (DVV)

9.3.2022

# Sisällysluettelo

DTYT / Reivo Juho (DVV)

9.3.2022

# Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta

Tässä asiakirjassa on kuvattu digitaalisen turvallisuuden strategisten riskien hallinnan prosessia ja kehitystä siltä osin, kuin sitä on suunniteltu toteutettavaksi julkisen hallinnon laajuisesti. Yksittäisen organisaatiokokonaisuuden tavoiteltavaa riskienhallintaprosessia kuvataan standardissa ISO 31000. Siihen verrattuna julkisen hallinnon laajuisessa riskienhallintamallissa digitaalisen turvallisuuden strategisten riskien hallintaan on kolme keskeistä eroa, johtuen sen hajautetusta rakenteesta. Riskienhallintaprosessin perusteella tehtävien hallintatoimien tarkempi suunnittelu ja toteutus tapahtuvat erillisesti, toimivaltaisten viranomaisten toimesta, sekä organisaatiokohtaisten että julkista hallintoa laajemmin koskevissa toimissa. Riskienhallintaprosessissa on huomioitu julkiselle hallinnolle luonteenomainen tarve selkeän päätöksenteon rakenteelle, josta vastaa erillinen koordinaatioryhmä, digitaalisen turvallisuuden strateginen johtoryhmä. Lisäksi prosessiin sisältyvää viestintää painotetaan muodostamalla aiheeseen liittyviä tilannekuvien ja muuta tietoa. Niiden kuvaus ja kehitys perustuvat soveltuvin osin strategisen tiedonhankinnan prosessimalliin, jota toteutetaan osana kokonaisprosessia.

Tämä asiakirja on yleiskatsaus riskienhallinnan asiantuntijoille sekä digitaalisen turvallisuuden kanssa toimiville johtotason päättäjille. Se on taustoittava esitys digitaalisen turvallisuuden riskienhallintaprosessin toiminnasta ja merkityksestä julkisen hallinnon läpäisevien riskien käsittelemiseksi silloin, kun ne ovat luonteeltaan erityisen merkittäviä tai sellaisiksi mahdollisesti kehittymässä. Asiakirjassa on käsitelty riskienhallintamallin ominaisuuksia myös laajemmin, jotta sen kehitystä voidaan arvioida ja tulevaisuudessa suunnata tarvittavalla tavalla.

Esitetty prosessikuvaus ja siihen liittyvät tehtävät muodostavat julkisen hallinnon digiturvallisuuden strategisten riskien hallintamallin, jonka tehtävä on mahdollistaa poikkihallinnollisten ja laajasti jaettujen riskien tunnistaminen, arviointi ja käsittelyyn ohjaus julkishallinnossa. Käytetyssä termistössä pyritään noudattamaan digitaalisen turvallisuuden riskienhallinnalle kehitettyä sanastokokonaisuutta (2022)[1], joka täydentää ISO31000- ja ISO73-sanastoja[2] sekä soveltuvin osin kokonaisturvallisuuden[3] ja kyberturvallisuuden[4] sanastoja.

## 1 Johdanto

Organisaatiot toteuttavat riskienhallintaa kukin omista lähtökohdistaan ja omaan toimintaansa keskittyen, kuten riskienhallinnassa pitääkin. Riskienhallinnan tulee heijastaa organisaation toimintaa ja näkemystä itsestään sekä suhdettaan ympäröivään toimintaympäristöön. Julkisen hallinnon riskienhallintaa varten on laadittu melko

[1] Esittelydokumentin julkaisu VAHTI Hyvä Käytännöt -tukimateriaaleissa https://dvv.fi/digiturvajulkaisut ja sanaston julkaisu Yhteentoimivuusalustan Sanastot-työkalussa https://sanastot.suomi.fi/

[2] ISO 31000:2018 (Riskienhallinta. Ohjeet), SFS-opas 73 (Riskienhallinta. Sanasto; ISO GUIDE 73:2009)

[3] https://turvallisuuskomitea.fi/viestinta/kokonaisturvallisuuden-sanasto/

[4] https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

kattavaa ohjeistusta sekä riskienhallinnan järjestämisen tukemiseksi että keskeisten prosessin osien yhdenmukaistamiseksi, liittyen niin vertailtavuuteen, tarkastusten tehokkuuteen kuin hyviin käytäntöihinkin.

Valtioneuvoston tasolla ei ole ollut velvoitetta säännöllisesti toistettavaan hallinnonalat kattavaan riskitiedon keräykseen, josta tunnistettaisiin ilmiöitä ja laajempia riskejä tai vertailtaisiin näkymiä näihin. Tämä koskee sekä kaikkien riskien kokonaisuutta että erillisiä aihealueita, kuten digitaalista turvallisuutta. Siten muuttuvan toimintaympäristön monimutkaistuvista tai hallinnon rajat ylittävistä riskeistä ei ole ajantasaista ja kattavaa tilannekuvaa. Kokonaiskuvan puuttuessa julkishallinnon riskien hallintatoimenpiteiden tukemiseksi on voitu kohdistaa vain vaillinaiseen tietoon perustuvasti ohjausta ja resursseja. Koska hallintatoimenpiteiden määrittelyä ja seurantaa on toteutettu yksittäisissä organisaatioissa, ei julkishallinnossa tehtyjen kehitystoimenpiteiden vaikuttavuutta ole myöskään voitu arvioida kattavasti[5].

Digitaalisen turvallisuuden toimeenpanosuunnitelman 2020—2023 (Haukka)[6] mukaisesti on asetettu poikkihallinnollinen digitaalisen turvallisuuden strateginen johtoryhmä (DTS-JORY). Sen tehtävänä on muun muassa arvioida julkisen hallinnon digitaalisen turvallisuuden strategisen tason tilannetta, koordinoida riskiarviota, luoda ja koordinoida yhteistoimintamallia sekä arvioida, ohjata, koordinoida ja valvoa keskeisiä kehitettäviä digitaalisen turvallisuuden palveluja. Ryhmä kokoontuu noin neljä kertaa vuodessa.[7] Tässä asiakirjassa esitetyt kuvaukset johtoryhmän roolista sekä toimenpiteistä riskienhallinnan toteuttamisessa vastaavat asetusasiakirjassa ilmaistua ja tulkitsevat näitä tehtäviä siltä osin kuin ne ovat johtoryhmän toiminnan puitteissa. Näiden ulkopuolella vastuu riskienhallinnasta ja siihen liittyvistä tehtävistä on kullakin toimivaltaisella viranomaisella.

Strategiseen riskikuvaan tunnistetaan useista kansallisista ja kansainvälisistä tietolähteistä sellaisia riskejä, jotka toteutuessaan aiheuttaisivat laajasti vakavia haittoja niin valtiolle kuin muillekin julkisen hallinnon toimijoille. Julkisen hallinnon tiedonhallinnan, palvelujen ja palvelutuotannon varautumisen, valmiuden ja turvallisuuden yleinen ohjaus on valtiovarainministeriön (VM) tehtävä. Sen pitää pystyä arvioimaan digitaalisen turvallisuuden yleisohjausta varten turvallisuuden kustannuksia sekä kohdentamaan resursseja mahdollisimman tehokkaasti. Riskien käsittelemiseksi suunniteltuista hallintatoimenpiteistä saatavien hyötyjen (toimenpiteiden vaikuttavuus) on oltava hyväksyttävässä suhteessa toteuttamiskustannuksiin sekä seurattavia.

Tässä asiakirjassa on kuvattu digitaalisen turvallisuuden julkishallinnon tason (strategisen) riskienhallinnan kokonaisprosessia. Tämä kokonaisuus on kehitysvaiheessa ja sen luominen käynnistettiin 2020 osana valtiovarainministeriön Haukka-hanketta. Kokonaisuuden kehittäjänä sekä toteuttajana on Digi- ja väestötietovirasto (DVV), joka tuottaa näkymän digiturvallisuuden riskeihin sekä tukee näiden riskien käsittelyä.

[5] Valtiontalouden tarkastusviraston tuloksellisuustarkastuskertomus 20/2018

[6] Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) VM 33/2020

[7] Digitaalisen turvallisuuden strategisen johtoryhmän asettaminen, 19.12.2019 (VN/13510/2019)

DTYT / Reivo Juho (DVV)

9.3.2022

# 2 Strateginen riskienhallintamalli

Riskienhallintamalli koostuu kattavasta, systemaattisesta, toistettavasta ja kehittyvästä prosessista sekä siihen liittyvistä tehtävistä. Näiden suunniteltujen mallien toteuttaminen – yhdessä muiden riskienhallintaan liittyvien toimien kanssa – muodostavat riskienhallintajärjestelmän, eli niin sanotun käytännön toteutuksen. Mallin suuntaus ja rajat muodostavat siitä digiturvallisuuden strategisen riskienhallintamallin. Sen erityinen tarkoitus on mahdollistaa poikkihallinnollisten ja laajojen jaettujen riskien tunnistaminen, arviointi ja käsittelyyn ohjaus sekä hallintatoimien tehostaminen yhteiseksi hyväksi.

Riskienhallintamallissa painotus on digitaalisen turvallisuuden riskien kokoamisella ja arvioimisella sekä strategisen tason riskianalyysien laatimisella tarvittavassa muodossa, ja toteutuksen maturiteetin rajoissa. Niiden avulla tuotetaan syötettä ja vaihtoehtoja erilaisten hallintatoimien muodostamiseen ja toteutukseen.

## 2.1 Nykytilan kuvaus

Ennen digiturvallisuuden strategisen riskienhallintamallin kehityksen käynnistämistä riskejä ei ole poikkihallinnollisesti arvioitu jatkuvasti, kattavasti ja laajasti. Digiturvallisuuden riskejä on mahdollisesti arvioitu eri tahoilla kertaluontoisesti, tarkoitusperään liittyen ja laajimmillaan rajatun hallinnon alueen sisällä. Aihepiiriä on aiemmin käsitelty ensisijaisesti tieto- ja kyberturvallisuuden näkökulmista.

Tässä esitellyn mallin kehitystyön osana tehtiin syksyllä 2020 valtiovarainministeriön toimesta kunnille ensimmäinen pilotointi riskeihin liittyvän tiedon keräämiseksi yhteistä näkymää varten. Sen taustalla oli vahvasti World Economic Forumin (WEF) tekemän globaali tarkastelu[8], jota on sovellettu verrokkina tiedon keruussa. Riskinäkemyskyselyä kehitettiin ja se toistettiin 2021 koko julkishallintoon[9].

Kysely toteuttaa osaltaan riskienarviointiprosessia, joka on osa riskienhallintaprosessia. Arviointiprosessiin kuuluvat osat ovat riskien tunnistaminen, riskien arviointi sekä riskien analysointi. Analysoinnin oheen kuuluu myös riskienhallintakeinojen alustava luonnostelu. Kyselyt ovat tehokas tapa laajan asiantuntijanäkemyksen kokoamiseen valituista asioista. Vaikka saadut tulokset olivat hyödynnettäviä, tehtyjen pilottien pohjalta voitiin tunnistaa useita kehityskohteita, joilla prosessia ja laatua voidaan kehittää tulevina vuosina.

Esimerkkejä kehityskohteista:

- Riskien tunnistaminen on tehty rajatun asiantuntijaryhmän toimesta, mikä ei takaa kattavuutta.

[8]Pilotti edeltänyt raportti WEF:n raportti: https://www.weforum.org/reports/the-global-risks-report-2019, sekä seuraavat 2020, 2021

[9] https://dvv.fi/documents/16079645/0/Digiturvallisuuden_riskikyselyn_tulokset_syksy2021.pdf/32f991cd-1b0e-9275-fadb-2d5166c2102c/Digiturvallisuuden_riskikyselyn_tulokset_syksy2021.pdf

- Riskien muodostamisen ohjaamiseksi ei oltu määrittelty kattavasti muun muassa toimintaympäristöä ja kriteereitä.
- Vastauksissa arviot perustuivat eri organisaatioissa toimivien virkamiesten asiantuntijanäkemyksiin, mutta tarkempien arvioiden tekemiseksi ja tilastollisen merkittävyyden takaamiseksi vastausten määrän tulisi olla suurempi.
- Analyysi hakee myös muotoaan, sillä se perustuu vielä suppeaan määrään lähteitä, eikä sisällä esim. historiatietoihin perustuvia muutostrendejä.
- Tuotettu tieto perustuu rajalliseen analysointimetodologiaan.

Tarkkaa tai kattavaa strategisiin tavoitteisiin sidottua riskinäkemystä ei myöskään pystytty vielä tarjoamaan riskienhallintamallin ollessa kehitysasteella, vaikka huomiota osattiin kiinnittää tunnettuihin haastaviksi tiedettyihin osa-alueisiin. Laajan ja päivittyvän tietomäärän käsittely perinteisenä kyselynä ei ole käytännöllistä, joten jatkoa varten riskienhallinnan kyselyt toteutetaan kehitettävällä digiturvallisuuden kokonaiskuva -palvelulla, jossa on riskienhallinnan osio. Keskeisimmät pitkän aikavälin kehityskohteet ovat laajemman prosessin rakentaminen sekä siihen liittyvien tukijärjestelmien kehittäminen. Kehitystoimia on otettu esiin enemmän tämän asiakirjan myöhemmissä osioissa.

## 2.2 Riskienhallinnan vuosisuunnittelu

Asetuksessa valtion talousarviosta (11.12.1992/1243) 69 § määritellään että, ”*viraston ja laitoksen johdon on huolehdittava siitä, että virastossa ja laitoksessa toteutetaan sen talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden asianmukaiset menettelyt*”, mihin perustuu vaatimus riskienhallinnasta. Tämä kattaa myös ”*toiminnot ja tehtävät, jotka se on antanut toisten virastojen ja laitosten, yhteisöjen tai yksityisten tehtäväksi tai joista se muuten vastaa*”. Tämän lisäksi, laki julkisen hallinnon tiedonhallinnasta (9.8.2019/906) 13 § määrittelee että, ”*tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti*”. Nämä säädökset ohjaavat toteuttamaan riskienhallintaa laajasti, mihin kuuluu myös tietoisuus ympäröivän toimintakentän sekä tarvittaessa laajemman globaalin tilanteen vaikutuksista ja muutoksista.

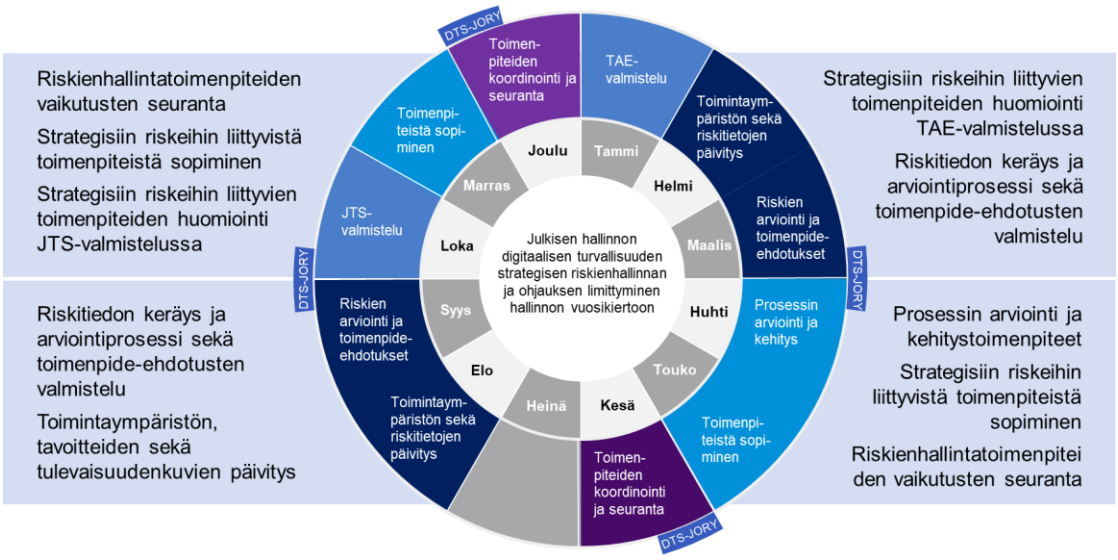
Riskienhallinta on prosessi, jonka vaiheita toistetaan syklisesti sekä muutosten havaitsemiseksi että pyrkimyksenä kehittyä paremmaksi. Riskienhallinnan syklejä, ja joissain tapauksissa yksittäisiä vaiheita, voidaan toteuttaa tasaiseen rytmiin tai tarpeeseen perustuen (ns. dynaamisesti). Tarve voi olla esimerkiksi eteen tuleva uhka, säännöllisesti toistuessaan prosessi, joka on sidottu toimintaa ohjaaviin rakenteisiin, kuten suunnittelun ja raportoinnin prosesseihin. Yleisesti ottaen riskienhallinnassa pitää kyetä molempiin, mutta riippuu organisaation toiminnasta missä suhteessa näitä kahta käytetään – kumpi tukee toiminnan tarpeita parhaiten missäkin tilanteessa.

Digitaalisen turvallisuuden strategisessa riskienhallintamallissa painotus on ohjauksellisten tarpeiden ja tarkastelutason vuoksi painottunut miltei täysin säännöllistä ennalta sovittua aikataulua toteuttavaan prosessiin. Sen aikataulutus suhteessa valtiovarainministeriön toteuttamaan ohjausprosessiin (Julkisen talouden suunnitelma, JTS) sekä organisaatioiden omiin ohjausprosesseihin (talousarvioesitys, TAE) on

DTYT / Reivo Juho (DVV)

9.3.2022

esitetty pääkohdittain alla olevassa. vuosikellossa. Riskienarviointiprosessin mallin tavoiteltu sykli on toteuttaa se kahdesti vuodessa, jotta tuetaan vuosisuunnittelua sekä kehitystarpeita niin organisaatioiden omassa toiminnassa kuin julkisen hallinnon yhteisissä tarpeissa.




*Kuva 1: Digitaalisen turvallisuuden strategisen riskianalyysin tavoiteltu vuosikello. Riskinarviointiprosessi on tarkoitus toteuttaa kahdesti vuodessa, alkukeväästä ja -syksystä. Arviointeja seuraavat raportointi sekä siihen perustuvat toimien kehittämisen tehtävät. Syklin lopuksi on tarkoitus tarkastella toimenpiteiden edistymistä, mikä sisältää laajojen kehityshankkeiden kestosta johtuen useamman aiemman syklin tehtäviä. Vuosikellossa on huomioitu suurpiirteisesti julkisen talouden suunnittelun valmistelu syksyllä, organisaatioiden talousarvioesitysten valmistelu alkuvuodesta sekä heinäkuun lomakausi. Riskienhallintamallin kokonaisuuden kehittämiseen liittyvät suuremmat suunnitellut muutokset on aikataulutettu pääosin tapahtuvaksi keväisin siten, että niitä voidaan tarvittaessa tarkastella digiturvallisuuden strategisen johtoryhmän (DTS-JORY) kokouksessa alkukesästä.*

Ensimmäisen ja kolmannen vuosineljänneksen aikana käynnistetään riskien analysointiprosessi keräämällä riskien tunnistamisen tueksi tarvittavat taustatiedot, muun muassa toimintaympäristöstä ja julkishallinnon strategisista tavoitteista. Prosessi jatkuu riskeihin liittyvän tiedon keräämisellä, riskien arvioinnilla ja analysoinnilla. Kerätyn riskitiedon luokittelun ja kokoavan analysoinnin jälkeen kootaan analyysiraportti asiantuntijaryhmän verifioitavaksi sekä sopivien hallintatoimenpiteiden tarkentamiseksi.

Verifioinnin jälkeen strateginen johtoryhmä arvioi riskejä ja toimenpide-ehdotuksia, tehden päätöksen riskien seuraamisesta, tarkentamisesta tai hallintatoimenpiteiden suosittelemisesta. Toimenpiteet voidaan tehdä koko julkisen hallinnon laajuisesti tai niiden toteutus voi olla organisaatiokohtaista. Yhteisesti tehtävissä toimissa strateginen johtoryhmä määrittää hallintatoimenpiteille vastuutahon. Riskitietoon perustuen tuotetaan myös raportti ja viestitään riskeistä julkishallintoon organisaatioiden omien toimenpiteiden käynnistämiseksi. Toisen ja neljännen vuosineljänneksen lopuksi kootaan tilannekatsaus, jossa tarkastellaan kokonaistilannetta sekä aiemmin aloitettujen yhteisten hallintatoimenpiteiden edistymistä.

## 2.3 Strategisen tason riskienhallintaprosessin kuvaus

Julkisen hallinnon digitaalisen turvallisuuden strategisessa riskienhallintamallissa painotetaan tiedon keräystä ja tilannekuvan luomista riskien arviointiprosessissa (tunnistetaan riskejä, arvioidaan niiden merkitystä sekä tarvittaessa analysoidaan tarkemmin niiden luonnetta). Sitä kuvataan prosessina, jossa tuodaan esiin tiedon siirtyminen ja eri osioiden toteutusvastuut toimijoiden välillä. Prosessi näkyy eri toimijoille vain osin, riippuen heidän roolistaan. Kokonaisuutta voidaan siis kutsua hajautetuksi prosessiksi.

### 2.3.1 Prosessin toimijat ja roolit

Riskienhallintamallin prosessin toteutuksessa ja erityisesti riskienarviointiprosessin eri vaiheissa tarvitaan seuraavia rooleja:

| Rooli | Kuvaus |
|---|---|
| **Riskienhallintapäällikkö** | Digi- ja viestintävirastoon (DVV) sijoitettu julkisen hallinnon digiturvallisuuden tehtävä, jonka vastuualueeseen kuuluu riskienhallintamallin mukaisen järjestelmän kehitys, prosessin ylläpito sekä koostavien tilannekuvien muodostaminen ja raportointi. Tähän sisältyy digitaalisen turvallisuuden valittujen riskien koonti, luettelointi sekä tietojen ylläpito ja seuranta riskirekisterissä. Tehtävässä tuotetaan arvioita ja analyysejä riskeistä sekä riskienhallinnasta itsenäisesti sekä asiantuntijaryhmän avulla. |
| **Asiantuntijaryhmä** | Asiantuntijoiden tehtävänä on tuottaa näkemystä riskeistä ja riskienhallinnasta arvioiden ja analyysien muodossa. Asiantuntijoita käytetään muun muassa varmistamaan strategisten riskien merkityksellisyys ja yhteismitallisuus sekä kehittämään hallintatoimia. |
| **Toimivaltaiset viranomaiset** | Toimivaltaiset viranomaiset ovat asiakkaina tuotetulle tiedolle, minkä perusteella ne voivat alallaan ohjata toimia ja omaa toimintaansa. Prosessissa ne toimivat oman toiminta-alueensa mukaisesti vastuullisena toimijana, joka tuottaa tarpeelliseksi ja tarkoituksenmukaisiksi katsottuja toimia riskien hallitsemiseksi. Laajoissa julkisen hallinon strategisissa riskeissä tämä voi tarkoittaa myös yhteishankkeita useiden osapuolten kesken. |
| **Digitaalisen turvallisuuden strateginen johtoryhmä (DTS-JORY)** | Toimivaltaisia viranomaisia edustaa digitaalisen turvallisuuden strategisen johtoryhmä (DTS-JORY), jonka tehtävänä on käsitellä riskitilannekuva sekä siihen mahdollisesti sisältyvät toimenpide-ehdotukset julkishallinnon poikkileikkaavan koordinaation toteuttamiseksi. Näin se ohjaa perustamaan tarvittavat digitaalisen turvallisuuden kehityshankkeet toimivaltaisten viranomaisten toimesta sekä seuraa niiden toteutumista ja yhteensovittamista. DTS-JORY osallistuu riskienhallintamallin kehittämiseen palautteen ja asiantuntijuuden muodossa. |
| **Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä** | Vuoden 2020 alusta Digi- ja väestötietovirasto vastuulle siirretty toiminto, joka toimii julkisen hallinnon keskeisten operatiivisten organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä. VAHTI-johtoryhmä käsittelee säännöllisesti sille tuotettua |

| | |
|---|---|
| **sekä riskienhallinnan kehittämisen työryhmä (VAHTI)** | riskiraportointia ja digitaalisen turvallisuuden tilannetta. Johtoryhmä kokoontuu viisi kertaa vuodessa. VAHTI-johtoryhmän alaisuuteen on asetettu viisi VAHTI-työryhmää, joista yhden työryhmän tehtävänä on digiturvallisuuden eri osa-alueiden riskienhallinnan kehittäminen. |
| **Julkisen hallinnon organisaatiot ja näiden keskeiset asiantuntijat** | Organisaatioiden riskienhallinnan ja/tai digiturvallisuuden asiantuntijat tuottavat, siirtävät ja (uudelleen)arvioivat tietoa riskeistä ja riskienhallinnastaan kokonaiskuvan muodostamista varten. He myös saavat siihen perustuvaa tietoa oman organisaationsa riskienhallinnan tilasta suhteessa muihin toimijoihin sekä julkisen hallinon yleisestä riskinäkymästä. Niiden perusteella he voivat kehittää omaa riskinäkemystään, riskienhallintatoimiaan sekä antaa syötteitä ylemmälle johtotasolle organisaation toiminnan ohjaamiseen. Organisaatiot voivat myös asiantuntijoidensa välityksellä osallistua toteutettaviin yleisiin hallintatoimiin ja niiden soveltamiseen omassa organisaatiossaan. |
| **Kokonaiskuvapalvelun tuoteomistaja** | Digi- ja väestötietoviraston tuottaman tilannekuvatietojärjestelmän kehittämisestä, yhteensovittamisesta sekä tiedon hyödyntämisestä vastaava rooli, jonka vastuulla on palvelun kehittämisessä huomioida tämän riskienhallintaprosessin tarpeet yhteistyössä riskienhallintapäällikön kanssa. |
| **Hallintatoimia toteuttavat asiantuntijat** | Erityisten kehityshankkeiden kautta riskienhallintatoimia toteuttavat asiantuntijat toimivaltaisissa viranomaisissa ja näiden yhteistyökumppanit. Kyseessä voi olla usean toimijan eri alueilla toteuttama kokonaisuus. |

*Taulukko 1: Digitaalisen turvallisuuden riskienhallinnan prosessin keskeiset toimijaroolit*

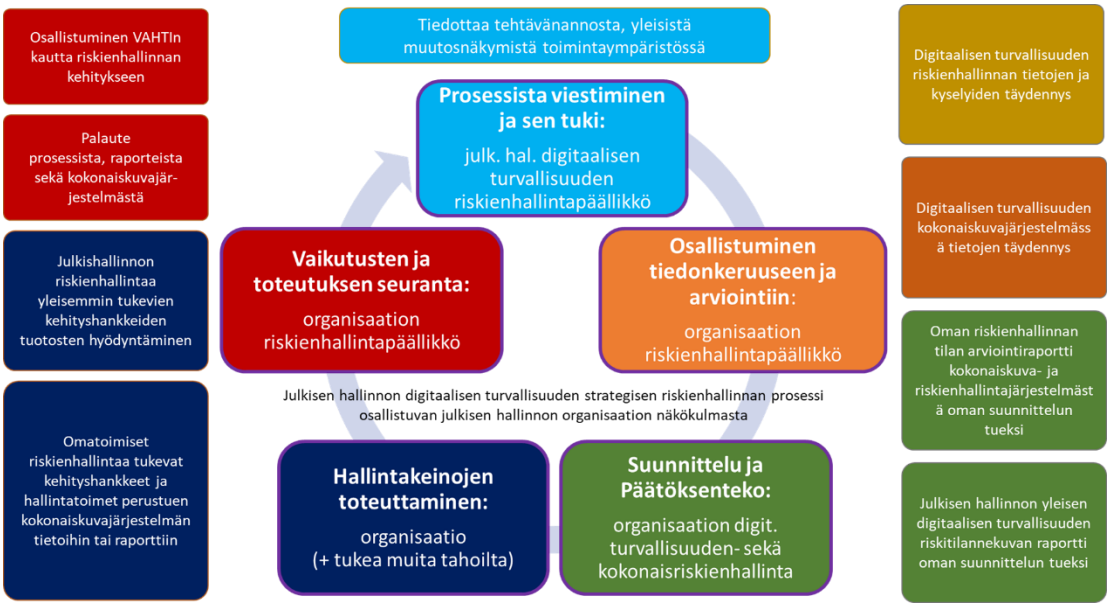
### 2.3.2 Prosessin osat ja vaiheet

Riskienhallinnan prosessiin on laadittu kolme keskeistä näkymää, sillä kokonaisprosessissa tuotetaan vastaus kolmeen tarpeeseen. Ensimmäinen näkymä on julkishallinnon organisaatioille, jotka pääsevät kokonaiskuvapalvelun riskienhallintaosion kautta vertaamaan omaa riskien ja riskienhallinnan tilannettaan verrokkiorganisaatioihin sekä saamaan kootun julkisen hallinnon riskitilannekuvan kautta tietoa omatoimiseen riskienhallintaan. Toinen on digitaalisen turvallisuuden strategisen johtoryhmän ja hallinnonalojen johdon näkymä, joka palvelee ohjaukseen ja päätöksentekoon tarvittavan tiedon tuottamisen tarpeita. Kolmas näkymä palvelee strategisen tiedonhallinnan prosessia, jossa on pysyväisluonteinen ”tietopyyntö” (niin sanottu RFI) tarkastella digitaaliseen turvallisuuteen vaikuttavia riskitekijöitä. Tähän prosessiin liittyy oma näkökulmansa, mutta sen tarkoitus on tuottaa oikein kohdistettuja tietotuotteita.

Päätöksenteko julkisessa hallinnossa ja erityisesti käytetyssä hallintorakenteessa, jossa digitaalisen turvallisuuden strateginen johtoryhmä koordinoi yhteistoimintaa, edellyttää sen lisäämisen klassiseen neliosaiseen kehitysprosessiin. On huomattava, että kaikki prosessin osat sisältävät useampia toimenpiteitä ja osaprosesseja, mikä myös mahdollistaa rakenteen säilymisen ennallaan, vaikka sisältöjä täydennettäisiin tulevaisuudessa. Kokonaisuuden kuvaamisesta tekee haasteellista myös se, että prosessin syklit ovat vain teoriassa peräkkäisiä, todellisuudessa hallintatoimien toteutus ja loppuun saattaminen voi kestää useita syklejä, joten toteutus sisältää limittäisyyttä.

Kokonaisprosessia voidaan kuvata hajautetuksi, sillä sitä toteuttavat eri toimijat eri vaiheissa ja eri päämääriä varten, mutta kokonaisuus tuottaa riskienhallintaa standardoitua prosessirakennetta soveltaen. Oheisista prosessia avaavista rakennekuvista voidaan tunnistaa yhtenevyydet.


*Kuva 2: Yleiskuva riskienhallinnan kokonaisprosessin mallista pääkohtien osalta.*




*Kuva 3: Julkisen hallinnon digitaalisen turvallisuuden strategisen riskienhallinnan prosessi osallistuvan julkisen hallinnon organisaation näkökulmasta. Painotus on julkisen hallinnon strategisen riskienhallinnan merkityksessä organisaation oman riskienhallinnan tukemiseksi. Suuntaa antava vertailutieto on anonymisoitu ja perustuu erilaisiin ryhmittelyihin.*


*Kuva 4: Julkisen hallinnon digitaalisen turvallisuuden strategisen riskienhallinnan prosessi julkisen hallinnon ohjauksen näkökulmasta. Painotus on riskienhallintatoimien sekä muun ylemmän tason päätöksenteon tarvitseman tiedon tuottamisessa. Ohjaukselliset tarpeet myös suorasti tai epäsuorasti liittävät prosessin osaksi laajempiakin ohjauksen rakenteita, jolloin se toimii syötteenä riskienhallinnan ulkopuolelle.*


*Kuva 5: Julkisen hallinnon digitaalisen turvallisuuden strategisen riskienhallinnan prosessi tiedonhallinnan toteutuksen näkökulmasta. Painotus on tiedon tuottamisen prosessissa, joka jatkuu toisten toimijoiden tietoa hyödyntävillä toimilla. Tiedon tuottamisen prosessissa tuotetaan ennakointitietoa sekä vaihtoehtoja ja ehdotuksia päätöksenteon syötteiksi, mutta se, miten näitä hyödynnetään, on riippuvainen riskienhallinnan prosessin ulkopuolisista asioista (muut strategiset tavoitteet, resurssit jne.).*

Prosessin ensimmäisessä vaiheessa kootaan lähtötiedot digitaalisen turvallisuuden strategisen tason riskiarvioprosessia varten. Tässä määritetään sekä digitaalisen

turvallisuuden että laajemmat strategiset tavoitteet, jotka vaikuttavat julkiseen hallintoon ja sen digiturvallisuuden järjestämiseen. Näiden kautta tapahtuu erilaisten riskien tunnistus ja arviointi. Sisäisten suuntaviivojen lisäksi tietoa kerätään ulkoisesta toimintaympäristöstä sekä sen muutossuunnista. Näitä näkemyksiä välitetään tarvittavissa määrin arviointiprosessiin osallistuville yhtenäisen arviointinäkemyksen tukemiseksi.

Osallistuvien organisaatioiden tiedonkeruu (taustatiedot organisaatiosta, perustiedot digiturvallisuudesta ja riskienhallinnasta) tapahtuu Digi- ja väestötietoviraston (DVV) ylläpitämän digitaalisen turvallisuuden kokonaiskuva -palvelussa, jossa on oma riskienhallinnan osionsa. Kokonaiskuvapalvelu toimii riskienhallinnan työkaluna, varmistaen kerätyn tiedon luottamuksellisuuden, yhdenmukaisuuden sekä pitkäjänteisen käytön. Tätä täydentävinä lähteinä analyysin kokoamisessa voidaan hyödyntää muita kansallisia ja kansainvälisiä tietolähteitä (raportit, tutkimukset, tietokannat, tietotuotteet yms.). Kokonaiskuvapalvelu tuottaa osallistuville organisaatioille vertailutietoa riskeistä ja riskienhallinnasta julkisessa hallinnossa toiminnan itsenäiseksi kehittämiseksi.

Riskinarvioprosessiin sisältyy myös raportin muodostaminen julkisen hallinnon digitaalisen turvallisuuden keskeisistä riskeistä, jossa saatu informaatio muokataan kohdeyleisöille relevanttiin muotoon. Siihen sisältyvät alustavat hahmotelmat hallintatoimille, perustuen lähinnä näkemykseen riskeistä ja riskienhallinnan kuvasta. Raportointi ja siinä tehdyt arviot riskeistä tulee laadunhallinnan vuoksi ohjata asiantuntija-arvioon, jossa otetaan huomioon sekä sisäiset että ulkoiset tavoitteet, muutostekijät, rajoitteet ja mahdollisuudet. Tämän jälkeen asiantuntijat laativat hallintakeinoille hahmotelmat projekteista, laajemmista hankkeista tai muista toteuttamistavoista päätösehdotuksiksi jatkokäsittelyyn.

Päätöksenteon ja koordinaation vaiheessa toimivaltaiset viranomaiset käyvät läpi raportoituja tietoja, arvioivat niitä laajempiin hallinnollisiin tarpeisiin nähden sekä päättävät niiden jatkokäsittelystä. Jatkotoimet voivat koskea muun muassa riskin seurantaa, lisäselvitystarpeita tai hallintakeinoja ja -toimia. Päätöksenteossa huomioidaan riski- ja riskienhallintatietojen sekä digiturvallisuuden tietojen ja arvioiden lisäksi johtoryhmän käytössä olevia muita, kuten toiminnallisia ja taloudellisia seikkoja, jotka voivat ohjata vaihtoehtoja. Digitaalisen turvallisuuden strategisen johtoryhmä voi tehdä päätöksiä sille osoitetuissa puitteissa. Julkishallinnon organisaatioiden tulee huomioida laajemmat riskinäkymät osana organisaation kokonaisriskienhallintaa.

Riskienhallinnan hallintakeinojen toteuttaminen sisältää eri toimenpiteiden tarkentamisen tarvittavilta osin toimivaltaisten viranomaisten toimesta. Tähän voi kuulua hankkeistaminen, mahdollisten yhteistyötahojen kanssa sovittavat työnjaot, rahoituksen, toimintakehyksen tai projektin tavoitteiden ja aikataulun selventäminen. Lisäksi sovitaan toimenpiteiden etenemisen seurannasta ja vaikutusten arvioinnista sekä varmistetaan jälkiseuranta. Hallintatoimenpiteiden toteutuksen etenemisestä raportoidaan DTS-JORY:lle vähintään puolivuosittain (Q2 ja Q4 lopussa).

Organisaatioiden omaan kontekstiinsa riskinarvioprosesseissa tuottamat tiedot toimivat pohjatietona strategisen tason riskianalyysille. Tämän tiedon jakaminen tuottaa vertailutietoa riskien ja riskienhallinnan tilanteesta julkisessa hallinnossa, jolla voidaan kehittää organisaatioiden yhteistä näkymää digitaalisen turvallisuuden tilasta.

Organisaatiot hyötyvät laajemmista julkishallintoon tuotettavista riskienhallintatoimenpiteistä, joita toteutetaan poikkihallinnollisesti merkittävien, laajojen tai jaettujen riskien käsittelemiseksi.

Hallintatoimista, niiden vaikutuksista, riskienhallintaprosessista sekä siinä tuotetusta tiedosta ja käytetyistä välineistä kerätään huomioita ja palautetta, jotta kokonaisuutta voidaan kehittää eteenpäin sekä laadullisesti, mutta myös vastaamaan tarpeita. Palautetta tarvitaan jokaiselta kokonaisuuteen osallistuvalta toimijalta. Palautteeseen sekä kehityssuunnitelmaan perustuen prosessia kehitetään kohti tasoa, jossa sen tuottaman riskienhallintatiedon laatu, luotettavuus, kattavuus ja oikea-aikaisuus tuovat merkittävää lisäarvoa digitaalisen turvallisuuden ohjaamiseen ennakoivasti.

# 3 Riskienhallintamallin taustaoletukset

Taustaoletukset ja niiden ymmärtäminen on olennaista, jotta ymmärretään tuotettu tieto ja pystytään suhteuttamaan sen merkitys oikein. Kaikessa tiedossa on rajoituksensa ja kontekstisidonnaisuutensa. Tämän lisäksi, kokonaisuuden kehittämisen kannalta nämä ominaisuudet ovat niitä, joilla voidaan tehdä strategisia muutoksia ja kohdennuksia prosessin toiminnassa. Nämä suoraan, tai näiden päälle rakentuvat tarkennusmahdollisuudet, antavat strategisen tason toimijoille mahdollisuuksia ymmärrettävästi ja määritellysti kohdentaa riskienhallintaa tarpeiden mukaan.

## 3.1 Digitaalisen turvallisuuden riskienhallintamallin taustaa

Vaikka riskienhallintaa tehdään julkisessa hallinnossa laajasti ja hallintaprosessi on kuvattu siihen sovitetusti[10], on strategisten riskien arvioinnissa tunnistettu[11] asioita, joita käytetyissä riskienhallintamalleissa ei ole riittävästi määritelty. Tästä syystä julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmaan vuosille 2020-2023 (Haukka)[12] on kirjattu toimenpiteet julkisen hallinnon strategisen tason digitaalisen turvallisuuden riskianalyysin toteuttamiseksi.

Riskienhallintamallin lähtökohtana on valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta 8.4.2020 (VM 2020:23)[13]. Päätöksessä on listattu kuusi kehittämisen periaatetta, joista riskienhallintamallin laatimisen taustalla on periaate: ”johdamme digitaalisen yhteiskunnan turvallisuutta yhdessä tilannetietoon ja riskiarvioon perustuen”.

## 3.2 Käyttötarkoitukset ja toimijat

Tämä asiakirja on laadittu kuvaamaan riskienhallintamallissa käytettyä rakennetta ja prosesseja yleisellä tasolla. Kokonaisuudesta voidaan kerralla valmistella vain osia, sillä sen on välttämättä kyettävä mukautumaan muuttuviin ja kehittyviin vaatimuksiin,

[10] Ohje riskinhallintaan VM 22/2017

[11] Tuloksellisuustarkastuskertomus - Valtionhallinnon riskienhallinta ja toimintojen jatkuvuus (20/2018)

[12] https://julkaisut.valtioneuvosto.fi/handle/10024/162191

[13] Julkisen hallinnon digitaalinen turvallisuus

joten mallin osioista on luonnosteltu eri kehitysvaiheita. Niitä voidaan tarvittaessa muuttaa tarpeiden, teknologian ja toimintaympäristön kehittyessä.

Riskienhallintamallin tehtävä on toimia tukena ennakoitaessa digiturvallisuuden tulevia haasteita, muun muassa tuottamalla yhteisesti jaettua tietoa. Lisäksi mallin sisällä olevien prosessien tehtävänä on varmistaa pyrkimys luotettavaan laatuun ja jatkuvuuteen. Tarkoitus on luoda strategisen tason riskeistä ja riskienhallinnasta tilannekuvaa, jonka avulla pystytään vaikuttamaan muun muassa digitaalisen turvallisuuden kehitystoimintaan ja budjetointiin.

Tästä asiakirjasta ja digiturvallisuuden riskienhallintamallista vastaa Digi- ja väestötietovirasto (DVV), perustuen lakiin Digi- ja väestötietovirastosta (304/2019, § 3). Riskienhallintamallin tavoitteet ovat sidoksissa digiturvallisuuden toteutuksen keskeisiin osa-alueisiin (johtaminen ja riskienhallinta, kyberturvallisuus, tietoturvallisuus, tietosuoja sekä jatkuvuudenhallinta). Näitä, sekä muita osa-alueita, toteuttaa kukin organisaatio itsenäisesti, mutta osa-alueilla toimii myös vastuuviranomaisia. Riskienhallintamallin erityinen tarkoitus on palvella näiden viranomaisten päätöksenteon ja toiminnan tarpeita tuottamalla yhteistä tietoa digiturvallisuuden osa-alueiden kehittämiseksi.

Riskienhallintamallia ja sen tuottamaa tietoa voidaan käsitellä ja arvioida kootusti viranomaisten yhteistyöelimissä. Valtiovarainministeriön asettama julkisen hallinnon digitaalisen turvallisuuden strategisen johtoryhmän (DTS-JORY), jonka ensimmäinen toimikausi on 1.1.2020 - 31.12.2024, yhtenä tehtävänä on arvioida ja koordinoida toimenpiteitä koskien strategisia julkisen hallinnon digitaalisen turvallisuuden riskejä. Sen tehtävänä on siten tarkastella digiturvallisuuden hallinnan, tietoturvan, tietosuojan, kyberturvallisuuden sekä jatkuvuuden ja varautumisen riskitilannetta, jonka perusteella DTS-JORY:ssä voidaan sopia jatkotoimista. Oleellista on, että johtoryhmä myös seuraa jatkotoimia sekä antaa palautetta päätöksentekoa tukevasta tiedosta, jotta sitä voidaan tukea tehtävässään ja tuottaa merkityksellistä tietoa riskeistä ja riskienhallinnasta.

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI-johtoryhmä), jonka nykyinen toimikausi on 01.03.2020 - 31.12.2024, on julkisen hallinnon digitaalisen turvallisuuden kehittämisen yhteistyö-, valmistelu- ja koordinaatioelin. Sen toiminnassa kehitetään digiturvallisuuden riskienhallintaa ja siten se voi kommentoida riskienhallintamallin rakenteita ja toteutusta, osana toiminnan tavoitteena kuvattua tukea julkisen hallinnon digitaalisen turvallisuuden kehittämiselle. VAHTI-johtoryhmän tehtäviin kuuluu myös koordinoida ja edistää julkisen hallinnon palvelutuotannosta ja turvallisuudesta vastaavien organisaatioiden yhteistyötä digitaalisen turvallisuuden eri osa-alueilla sekä edistää ja osallistua valtiovarainministeriön laatimien julkisen hallinnon digitaaliseen turvallisuuteen liittyvien periaatepäätösten, kehittämisohjelmien ja hankkeiden toimeenpanemiseen. VAHTI-johtoryhmän kautta strategiseen riskienhallinta-kokonaisuuteen osallistuvat organisaatiot voivat vaikuttaa sen kehittämiseen.

Tuotetun riskejä, riskienhallintaa ja riskienhallintajärjestelmiä koskevan tilannekuvatiedon sekä laajempien hallintatoimien kautta julkishallinnon organisaatioiden on tarkoitus saada tukea omaan riskienhallintatyöhönsä. Vertailutieto voi myös mahdollistaa itsearvioinnin sekä itseohjautuvuuden digiturvan järjestämisessä. Asiaa yleisemmin tarkasteltuna, julkishallinnon laajuisen kokonaisuuden riskienhallintaprosessi toteutuu virtuaalisesti ja loogisesti eri toimijoiden toteuttaessa eri osia, kun ne

toteuttavat omaa sisäistä riskienhallintaansa tai osallistuvat yhteisen hallinnan tuottamiseen. Organisaatioiden tasolla tuen voi tosin olettaa olevan kuitenkin pääosin soveltamista vaativaa tai epäsuoraa. Seurausten odotetaan olevan positiivisia vaikutuksia organisaatioiden asiakkaiden ja sidosryhmien luottamukseen ja digiturvallisuuden tasoon.

## 3.3 Perusoletukset ja rajaukset

Riskienhallintamallin suunnittelussa ja toteutuksessa on sovellettu kansainvälisiä riskienhallinnan standardeja[14]. Mallissa käytetyn prosessin osana pyritään tunnistamaan rakenteessa keskeiset sisältyvät kontekstit, rajaukset ja valinnat - sen lisäksi mitä oletuksia ja määrityksiä tehdään toimintaympäristöön ja sen muutoksiin, kun prosessia toistetaan.

### 3.3.1 Sisäinen näkymä ja tarkastelulle merkityksellinen näkökulma

Tarkastelussa toinen pääasiallisista rajauksista on Suomen julkishallinnon organisaatiot. Tämän katsotaan sisältävän laajasti valtion virastot, liikelaitokset, ministeriöt ja muut toimijat sekä kunnat ja erilaiset kuntayhtymät. Mukaan luetaan myös eri viranomaiset ja toiminnot, jotka voivat toimia laajempien organisaatioiden osana, kuten tiedonhallintayksiköt joissain tapauksissa.

Julkishallinto-rajauksen ulkopuolelle jäävät tarkastelussa muun muassa kansalaiset ja yritykset. Valinta johtuu valtiovarainministeriön ohjauksesta, joka suuntaa näkökulmaa suhteessa muuhun hallintoon. Tarkastelussa kuitenkin heijastuvat kansalaisten tarpeet palvelurakenteiden kautta ja yrityksillä on roolinsa erilaisten palveluiden tuotannossa. Tuotettava voi olla sovellettavissa myös julkishallinnon ulkopuolella ja antaa kansalaisille osaltaan kuvaa julkishallinnon kyvystä huolehtia digiturvallisuudesta, mikä voi olla merkittävää demokratian ja valvonnan kannalta. Riskeille kehitettävissä hallintatoimissa on myös mahdollista pyrkiä huomioimaan julkishallinnon alihankintaketjut sekä sen ulkopuolella toimivat tahot.

Digiturvallisuus on valittu erityiseksi tarkastelun aiheeksi, jolta käytetään poikkileikkaamaan julkisen hallinnon alueita. Se on otettava sisäisenä määrittelynä, vaikka itse termi on asetettu kaikenkattavaksi. Tämä johtuu digiturvallisuuden toteuttamisessa tehtäviin määrittelyihin ja valintoihin, eli niihin keinoihin ja lähestymiskulmiin mitä julkishallinnossa on sovittu käytettäväksi. Osa tästä määrittelystä tehdään esimerkiksi lainsäädännössä, mutta keskeisiksi määritellyt toteuttamisen osa-alueet ovat johtaminen ja riskienhallinta, kyberturvallisuus, tietoturvallisuus, tietosuoja sekä jatkuvuudenhallinta. Historiallisesti katsottuna, käytetty kattokäsite on muuttunut digitalisaation historiassa niin termiltään kuin sisällöltäänkin, eikä tälle muutokselle ole odotettavissa loppua. Digiturvallisuuden sisällä voidaan ottaa kapeampia tai kattavampia näkökulmia siihen luettaviin asioihin, mikä heijastuu merkityksellisinä pidettäviin riskeihin, joita sisällytetään tarkasteluun ja seurantaan.

Käsitys julkisen hallinnon digiturvallisuuden tilasta ja tavoitteista perustuu sekä prosessissa tuotettuun tietoon että myös muilla tahoilla tuotettaviin asiakirjoihin.

[14] ISO 31000:2018 (Riskienhallinta. Ohjeet), IEC 31010:2019 (Riskienhallinta. Riskien arviointimenetelmät), ISO/TR 31004 (Riskienhallinta. Ohjeita standardin ISO 31000 soveltamisesta)

Keskeisiä asiakirjoja ovat digitalisaation, julkisen hallinnon kehittämisen, turvallisuuden sekä digi- ja kyberturvallisuuden strategisen tason suunnitelmat, raportit ja selonteot. Näistä muodostuvat strategiset kiintopisteet, joiden kautta digiturvallisuuden riskienhallintamallissa tehtävä arviointi ja analysointi tapahtuu.

### 3.3.2 Toimintaympäristöt, joiden sisällä tarkastelu tehdään

Määritettävä toimintaympäristö riskienhallinnalle tässä mallissa koostuu useista risteävistä alueista, joista yksi keskeisin on digitaalinen toimintaympäristö. Digiturvallisuuden määritelmän mukaisesti, toimintaympäristöön kuuluvina voidaan tarkastella asioita, jotka vaikuttavat digitaaliseen toimintaympäristöön tai siellä toimimiseen, sekä asioita, joihin digitaalisella toimintaympäristöllä ja siellä tapahtuvalla toiminnalla on vaikutusta. Digitaalisuuden rajat ylittävät vaikutukset voivat olla negatiivisia (esimerkiksi kaapeleiden katkeaminen, osaajien puute, hyökkäykset) tai ne voivat olla asioita, joiden estyminen olisi negatiivinen asia (esimerkiksi energia, komponentit, palvelut). On myös huomattava, että digitaalinen toimintaympäristö on jatkuvasti kehityksessä ja uudelleenmäärityksessä, johtuen osittain sen yhteyksistä muihin toiminta-alueisiin, joiden kanssa se on vuorovaikutuksessa. Tämä muokkaa ja luo uusia uhkia ja mahdollisuuksia, joista voi muodostua riskejä.

Fyysisessä ympäristössä olemme tarkastelussa sidotut Suomen valtion alueelle. Vaikka digitaalinen toimintaympäristö on globaali, useat järjestelmät, käytetyt kielet, asiakkaat, palvelut, asiantuntijoiden sijoittuminen, tietoverkot sekä muut toiminnallisuudet ja liitospisteet reaalimaailman kanssa määrittelevät alueellisen toimintaympäristön. Julkishallinnon toimintaympäristö koostuu näistä. Tämän rinnalla sijaitsee julkishallintoon ja valtioon liittyvä poliittinen toimintaympäristö, johon ovat liitoksissa muun muassa naapurivaltiot ja muut kansainväliset toimijat, kuten EU.

Abstraktimmassa tarkastelussa, kehityskulkuja laajassa sosio-teknisessä todellisuudessa kuvataan käsitteellä VUCA (volatility, uncertainty, complexity, ambiguity). Näillä kuvataan miten asiat ovat jatkuvassa muutoksessa, tulevaisuus on epävarma, merkitykset ja yhteydet ovat kompleksisia sekä monimerkityksellisiä. Pysyvät, selkeät, rajatut ja yksiselitteiset näkymät eivät siten ole todennäköisiä strategisella tasolla.

Digitaaliseen toimintaympäristöön liittyviä kehityskulkuja voidaan seurata tiedotusvälineistä, raporteista ja selvityksistä, mutta muutoksia on syytä tarkastella myös pidempien aikajaksojen tarkasteluista. VUCA:n huomioivaa näkymää tulevaisuuden ilmiöiden kehittymiseen voidaan saada eri organisaatioiden tuottamista ennusteista ja ennakointityöstä. Edellä mainitut sisältävät myös muun muassa fyysiseen ja poliittiseen ympäristöön liittyviä näkymiä.

### 3.3.3 Aikaikkuna

Riskienhallinnan strategisessa tarkastelussa on määriteltävä aikaikkuna, jossa tarkastelua tehdään. Perinteisen ajattelutavan mukaan, strateginen näkymä on noin 2-5 vuotta eteenpäin, mutta tämä määrittyy usean tekijän mukaan. Hyvin nopeidenkin päätösten vaikutukset voivat olla kauaskantoisia ja vaikutusten erottaminen muista tapahtumista voi kestää tuon aikaikkunan tai pidemmällekin. Asioiden kehittyminen merkittäviksi voi viedä aikaa, mutta digi-aikakaudella ne voivat skaalautua yllättävän

nopeasti. Aikaikkuna asettuu, määrittelystä riippuen, keski-pitkälle tai pitkälle tähtäimelle.

Aikaikkunan maksimi on raja, jonka yli näkeminen riskienhallinnassa käytettävillä menetelmillä ei tuota kuvaa sillä varmuudella, että sitä voidaan hyödyntää toiminnan ohjaamisessa. Erityisen kauaskantoiset arviot voivat tukea vaihtoehtojen arvioimista sekä yleistä tulevaisuuteen liittyvää ennakointityötä, mutta niiden käyttö konkreettisiin toimiin ei välttämättä ole perusteltua. Kuten riskienhallinta, ennakointityö on systemaattista, jäsenneltyä, osallistavaa ja kehittyvää, mutta painottuu pidempään aikaväliin, mahdollisien tulevaisuuksien hahmottamiseen ja voidaan nähdä tukevan enemmän strategioiden luomista, kuin niiden toteutumisen varmistamista. Aikaikkunan maksimin määrittelyyn voi liittyä tilannekohtaista harkintaa ja joissain tilanteissa hyvin lyhyenkin aikavälin yli näkemiseen voi liittyä merkittäviä epävarmuustekijöitä.

Aikaikkunan minimi on raja, joka muodostuu siitä, miten ajantasaista ja oikea-aikaista tuotettu näkymä on. Riskienhallintaan liittyvän tiedon tuottamisen tavoitteena on tuottaa riittävä ennakkovaroitus, jotta voidaan tehdä tarvittavat toimet kehityskulun ehkäisemiseksi tai muuttamiseksi. Ennakkovaroituksen on oltava niin ajoissa, että tarvittavat toimet ehditään tehdä, sillä muussa tapauksessa muodostuva tilanne on käsiteltävä olemassa olevalla kyvyllä ja kapasiteetilla – mahdollisesti tukien sitä poikkeavilla, kiireellisillä ja vaillinaisilla (mutta tarpeellisilla) toimenpiteillä. Voidaan argumentoida, että pienikin varoitus on tarpeellinen, mutta tavoiteltavaa olisi tuottaa riskienhallinnassa ennakointitieto, joka kyetään käsittelemään normaalien hallintarakenteiden kautta, osana normaalia johtamista ja työskentelyä.

Aikaikkuna ei siis ole tarkkarajainen kumpaankaan suuntaan, mutta ohjaa keskittymään tiettyihin rajoihin. Prosessin kaikkien osien läpimenon syklin kestosta tuleva viive määrittelee lyhimmän mahdollisen ajan, jossa mallilla voidaan tuottaa tukea riskienhallintaan. Se on riippuvainen erilaisista taustajärjestelmistä, mutta myös tarvittavasta arvioinnin ja analysoinnin laajuudesta ja syvyydestä. Prosessi on lisäksi sidottu osaksi hallinnollista vuosikelloa, mikä tahdistaa sen toimintaa muiden prosessien kanssa, pyrkien tuottamaan tietoa oikea-aikaisesti.

### 3.3.4 Suhde standardeihin

Riskienhallintajärjestelmien riskienhallintaprosessien luominen standardia noudattaviksi julkishallinnossa ja muissa suurissa monimutkaisissa organisaatioissa on haasteellista. Näin etenkin, edellä mainittuja vielä laajempien hallinnon- ja toimialat yhdistävissä järjestelyissä (esimerkiksi aihealueen ympärille, kuten digiturvallisuus tai toimiala), joita luodaan eri riskienhallintakokonaisuuksia tukemaan. ISO31000:ssa kuvattuun mallirakenteeseen ei ole valmiiksi sisällytetty laajan organisaation tai vielä suuremman kokonaisuuden tarvitsemia toiminnallisuuksia, joilla rönsyilevää organisaatiorakennetta tai laajaa tietomäärää voidaan käsitellä tehokkaasti eri vaiheissa. Tätä varten on eri vaiheisiin luotava tarvittavat mekanismit käsittelyn jakamiseksi osiin tai kokoaviksi luokitteluiksi ja tilastoinniksi.

Keskeistä on huomioida, että kukin organisaatio tai sen osa toteuttaa riskienhallintaa sekä tunnistaa ja arvioi riskejä ensisijaisesti omasta näkökulmastaan, vaikka pyrkisivät huomioimaan muita. Nämä näkökulmat eivät useinkaan ole sellaisenaan siirrettävissä organisaatiokontekstista toiseen. Siirrettäessä riskitietoa organisaatioiden välillä

niin sivuttain kuin myös hierarkisten tasojen välillä, tulee tieto aina uudelleenarvioida suhteessa uuteen näkökulmaan ja organisaatioon. Tätä voidaan tehdä tietoa lähettävässä tai vastaanottavassa päässä, mutta se perustuu tulkintaan. Laajempaa tarkastelua varten tehtävissä koonneissa ja strategisemman tason näkemystä tuotettaessa on oletusarvoisesti hyväksyttävä, että ne perustuvat epätarkasti tulkittavaan indikoivaan tietoon ja viittaaviin signaaleihin, vaikka taustalla oleva data olisi laadukasta.

Niillä organisaatioilla tai organisaatioiden järjestelmillä, joiden hallinnan tukena käytetään ISO27000-sarjan mukaisesti suunniteltua toimintaa, riskienhallinta siltä osin edellyttää organisaatiolta standardin noudattamista. Koska ISO27000-sarjassa käytetty riskienhallintaprosessi perustuu ISO31000:een, löytyy tästä tarvittaessa rajapinta ja mahdollisuus kytkeä ne osaksi laajempaa riskienhallintaa. Vastaavuuksia voi löytyä myös muista prosessimalleista. Organisaation oma kokonaisriskienhallinta on ensisijaisin yksittäisiin osa-alueisiin tai tähän julkisen hallinnon laajuiseen riskienhallintamalliin nähden.

Valtiovarain controller-toiminto on laatinut ohjeita riskienhallintaan[15] sekä riskienhallintapolitiikkamallin, joka sisältää politiikan suositellut vähimmäisvaatimukset sekä eräitä muita mallia ohjaavia ominaisuuksia.[16] Suositukset pohjautuvat ISO 31000 -riskienhallintastandardiin.

## 3.4 Kustannuksista ja vaikuttavuudesta

Julkisen hallinnon strategisen riskienhallinnan vaikutukset ja vaikuttavuus ovat laajoja kokonaisuuksia, joiden mittaamista hankaloittavat hajautettu toteutus, kohdistuksen ja kontekstin määrittely yksittäisen organisaation sijaan myös asiakkaisiin ja muihin sidosryhmiin sekä toteutumattoman vaikutuksen arvon mittaamisen haaste – eli hallintatoimilla vältetyn riskin vaikutuksen käänteinen arvo. Niiltä osin kuin tämän riskienhallintamallin toteuttamisen vaikutuksia tarkastellaan, mikä on yksinkertaisemmin arvioitavissa, voidaan nähdä tärkeiden panostusten olevan pieniä suhteessa potentiaalisiin haittoihin ja menetyksiin, joita toteutuneet laajat riskit voisivat tuoda.

Kokonaisprosessia ylläpitävä, kehittävä ja tietotuotteista vastaava riskienhallintapäällikkö toimisi Digi- ja väestötietovirastossa vakituisena johtavana asiantuntijana. Tämän henkilön palkkaus sivukuluineen sekä kehittämiseen ja viestintään tarvittava alustava budjetti olisivat yhteensä arviolta 140000€ vuodessa. DVV:n kuluiksi on myös huomioitava digitaalisen turvallisuuden asiantuntijoiden sekä konsulttien hyödyntäminen mahdollisuuksien mukaan osana riskienarvioitiprosessin tehtäviä, mikä arvioidaan tässä vaiheessa olevan yhteensä noin yksi henkilötyökuukausi. Erityisiä riskejä arvioitaessa ja niiden hallintatoimia suunniteltaessa on asiantuntijoina käytettävä myös muiden julkisen hallinnon toimijoiden asiantuntemusta, mitä ei tässä laskelmassa huomioida. Tämän päälle tulevat järjestelmien ylläpitokulut, jotka nivoutuvat muihin DVV:n kuluihin, mukaan lukien digitaalisen turvallisuuden kokonaiskuvapalvelu, johon riskienhallinnan tiedot ovat yhteydessä.

[15] https://vm.fi/riskienhallinnan-ohjeita

[16] https://vm.fi/riskienhallinta/riskienhallintapolitiikka

Riski- ja riskienhallintatiedon tuottamiseen osallistuvat organisaatiot tulisivat käyttämään tähän noin 1 htp vuodessa, tiedonsyöttöön käytettävän ajan voidaan olettaa laskevan selvästi ensimmäisten prosessisyklien jälkeen. Saatujen raporttien käyttö omassa riskienhallinnassa vie käsittelytavasta riippuen saman verran aikaa, minkä päälle luonnollisesti tulevat välilliset vaikutukset mahdollisista hallintatoimista. Kokonaiskuvapalvelun kautta riskienhallinnan tiedonjakoon osallistumattomat organisaatiot tulisivat hyötymään yleisestä julkisen hallinnon laajuisesti digitaalisen turvallisuuden riskienhallinnan raportoinnista sekä mahdollisista yleisistä digitaalisen turvallisuuden riskienhallintatoimista, vaikkakin toimien kohdistus voi kärsiä kattavuuden puutteesta, mikäli osallistujia on vähän.

Riskienhallintaprosessissa tuotettu tieto tuottaa tehtäviä sekä digitaalisen turvallisuuden strategiselle johtoryhmälle että niille toimivaltaisille viranomaisille, joille erilaisia riskienhallintatoimia ohjautuu. DTS-JORY:n suhteen pääasiallinen ajankäyttö sisältyy jo suunniteltuihin kokouksiin. Toteuttavien viranomaisten kohdalla vaikutukset ovat tapauskohtaisia ja osin normaalien prosessien puitteissa tehtäviä, mutta laajemmissa hankkeissa vaativat erillistä resursointia. VAHTI-johtoryhmällä ja VAHTI riskienhallinnan kehittämisen työryhmällä, joiden sisällä voidaan vapaaehtoisuuteen perustuen osallistua prosessin kehittämiseen liittyviin tehtäviin, suoraa kuormitusta ei nähdä merkittävänä.

Strategisella riskienhallinnalla on mahdollista vaikuttaa laajoihin kokonaisuuksiin, joiden vaikutukset heijastuvat useisiin toimijoihin suoraan tai välillisesti. Vaikka aihealueen kautta korostuu turvallisuuden varmistaminen, riskienhallinnalla pyritään ennen kaikkea mahdollistamaan strategiset toiminnot sekä tukemaan strategisten tavoitteiden saavuttamista sekä mahdollistamaan organisaation jokapäiväinen toiminta. Sen lisäksi, että riskien vaikutuksia voidaan vähentää ja neutraloida, strategisessa riskienhallinnassa tuleekin pyrkiä myös huomioimaan mahdollisuudet eli haittojen kääntäminen joksikin positiiviseksi lopputulemaksi. Onnistuneen ennakkovaroituksen saaminen riskienhallinnasta tarkoittaa yleensä merkittävää kustannussäästöä verrattuna siihen, että riski pääsee muodostumaan akuutiksi tilanteeksi ilman ennakkovalmistautumista. Lisäksi hallintatoimiin voi kuulua esimerkiksi turvallisuuteen liittyvien tai muiden toimintojen uudistaminen, joka tehostaa sekä rikastaa palveluita tai mahdollistaa uusien teknologioiden tai toimintatapojen käyttöönoton ja tehostaa tiedon hyödyntämistä. Näiden etujen mittaaminen, etenkin euromääräisesti, voi olla mahdotonta, mutta niiden tukemiseksi tehtävien digiturvallisuuden tehtävien arvon määrittäminen vaikuttavuuden mittarina on osa malliin sisältyviä ohjauksen tarpeita.

## 3.5 Riskienhallintamallin kehitys

Kattavan riskienhallintamallin rakentaminen toimivaksi järjestelmäksi, joka vastaa muuttuvia tarpeita, on pitkällinen prosessi itsessään. Tämä prosessi alkoi vuonna 2020 pilotoidulla kyselyllä, jota on toistettu ja edelleen kehitetty. Kysely ja sillä kerättävät näkemykset riskeistä ovat kuitenkin vain yksi palanen ja näkökulma. Riskienhallinnan kokonaisuudessa on useita osa-alueita, joita tulee kehittää. CMMI-mallin[17]

[17] Capability Maturity Model Integration

viisiportaista edistymisen mittaria mukaillen, tämänhetkinen tilanne voidaan nähdä täyttävän korkeintaan tason kaksi tilanteen.

Kehityskohteita kartoitettiin myös esiin pilotointien perusteella tehdyissä huomiossa. Testauksen kautta havaittuja tavoiteltavia kehityskohteita voisivat olla:

- tiedonkäsittelyn järjestelmäpohjaisuus ja yhteentoimivuus eri määrittelyiden kanssa
- laaja osallistuminen ja vastausmäärien kasvattaminen laajemman kuvan saamiseksi
- osallistujien suhteellisen hyödyn kasvattaminen nähtyyn vaivaan nähden,
- useamman lähteen ja ulkopuolisten arviointien käyttö täydentämään tietoa
- monipuolisemman analyysimetodologian käyttö
- yleisnäkymän kehittämisen jälkeen kohdistetut syvemmät tarkastelut
- yleisten ja digitaalisen turvallisuuden tavoitteiden parempi huomioiminen
- ennakointityön ja toimintaympäristöjen muutospolkujen tunnistaminen ja huomioiminen pidemmältä ajalta
- toiminnan pitkäaikaisuuden kautta saatavan muutostiedon hyödyntäminen
- riittävä resursointi loppuun asti kehitettyjen tietotuotteiden toteuttamiseen eri kohderyhmille

Strategisen tiedonhallinnan prosessin neljän päävaiheen kautta katsottuna, kehityskohteita voisivat olla:

1 Riskienhallinnan ohjaamista ja tukemista palvelevan tehtävänannon (”tietopyyntö”) kehitys, eli miten muotoillaan oikeat kysymykset aiheen ympäriltä, jotta voidaan tuottaa tarvittavat vastaukset.
2 Tiedonkeräyksen laajentaminen ja syventäminen, kattavuuden varmistaminen eri osioissa, vertailutiedon kehittäminen ja rikastaminen sekä ulkoiset tietolähteet.
3 Tiedon käsittelyn kehitys, mihin kuuluu tehostaminen, yhtenevien käsittelytapojen kehitys, luokittelut sekä oppivien järjestelmien hyödyntäminen esimerkiksi tunnistamisessa sekä muutosten ennakoinnissa.
4 Analysoinnin ja raportoinnin kehitykseen liittyviä kysymyksiä menetelmistä ja työkaluista, tiedon visualisoinnista sekä laajemmasta tilannekuvasta ja sen ymmärryksestä.

Sekä testauksen kautta tehdyissä huomioissa että rakennetta analysoimalla nähdään useita samansuuntaisia kehityskohteita. Näistä useat ovat jo yksinään pieniä projekteja ja sisältävät käytännön tasolla useita muutoksia, joista tosin kaikki eivät tulisi olemaan ulospäin näkyviä. Erilaisten vaihtoehtojen määrästä johtuen näiden toteuttamista on priorisoitava.

### 3.5.1 Ensimmäinen kehitysvaihe

Ensimmäisen kehitysvaiheen tehtävät keskittyvät tiedon keräyksen osa-alueelle, vaikka voidaan katsoa, että jo toisessa pilotoinnissa 2021 kehitettiin tietopyyntöön liittyviä tarkennuksia osana kyselyn suuntaamista. Tiedon keräyksen tehostamiseksi, turvaamiseksi sekä yhdenmukaistamiseksi otetaan käyttöön tähän suunnattu tietojärjestelmä, jossa tuotetaan digitaalisen turvallisuuden kokonaiskuvaan liittyviä tietotuotteita, hyväksikäyttäen organisaatioista saatuja taustatietoja. Tähän järjestelmään siirtyminen tarkoittaa tietotuotteen sisällön kannalta taustoittavan digitaalisen

turvallisuuden tiedon hyväksikäytön mahdollisuutta luotaessa kuvaa riskienhallinnan tilanteesta. Sitä voidaan suhteuttaa riskeihin, mutta myös suhteuttaa eri toimijoiden ja luotujen vertaisryhmien kanssa. Tällöin pystytään tarjoamaan ajantasaista ja päivitettävää tietoa automaattisella raportoinnilla. Aluksi raportointi tulee olemaan perusmuotoista, mutta sitä voidaan myös kehittää datan määrän kertyessä. Toistettavuus ja kertyvän datan vertailumahdollisuus aikasarjoina mahdollistaa havainnot vuosien aikana tapahtuvista muutoksista, mikä avaa indikoivia näkyviä tulevaisuuden trendeistä.

Näillä toimilla saadaan luotua pohja organisaatioilta tehtävälle riskinarviointiprosessin tiedonkeruulle (erotuksena muista lähteistä tehtävälle). Tämän myötä muodostuvat prosessin keskeiset tuotokset osallistuville organisaatioille, eli vertaileva raportti riskien sekä riskienhallinnan tilannekuvasta, suhteessa muihin julkisen hallinnon toimijoihin. Ohjaukselle tässä muodostuu kehittyvä datalähde, jonka arvo kasvaa ajan kuluessa. Aluksi toiminnallisuutta on toki hiottava pilotoinneilla, ja toimintaan sisältyy käyttäjien kokema muutos siirryttäessä käyttämään uudenlaista palvelua, mikä aiheuttanee työtä. Riskinä on, että käyttäjämäärät jäävät alussa vähäisiksi, mikä hidastaa järjestelmään kertyvää dataa sekä haittaa kattavien näkymien saamista.

### 3.5.2 Toisen kehitysvaiheen hahmotelma

Toisessa vaiheessa tulisi keskittyä parantamaan aiempia kyvykkyyksiä, jotta näistä saatava hyöty saadaan ”kasvamaan korkoa” aikaisessa vaiheessa. Muutosten mielekkääseen ja uskottavaan seuraamisessa tarvitaan toistoja noin 3-5 vuoden ajalta, mutta tämä laskenta voidaan aloittaa vasta riittävän osallistujajoukon liityttyä osaksi prosessia.

Tässä vaiheessa tulisi täydentää olemassa olevaa riskinäkemyskyselyä sekä lisätä muita metodeja ja näkökulmia käyttäviä kyselyitä, jotka voivat vastata toisenlaisiin riskeihin ja riskienhallintaan liittyviin tarpeisiin. Näitä voisivat olla tulevaisuuden digitaalisen turvallisuuden muutostekijöihin liittyvät hahmotelmat (uhkia ja riskejä laajemmat kehityskulut), riskienhallinnassa käytettävien työkalujen tilaa ja yhteentoimivuutta luotaava toistettava selvitys, eritasoisten riskien havainnointiin ja käsittelyyn liittyvä tiedonkeruu ja niin edelleen. Osa esimerkeistä tukee enemmän osallistuvien organisaatioiden omatoimista riskienhallintaa, osa laajempaa julkisen hallinnon riskienhallinnan kehittämistä ja ohjausta.

Lisäksi tulisi tarkastella ja esimerkiksi pilotoinnilla testata tiedonkeräyksen laajentamista muihin lähteisiin (ulkoiset tilatut arviot), analyysimenetelmien monipuolistamista (systeeminen tilannekuva, verkostoanalyysi) sekä validoinnin määrittelyä (prosessi, laatukriteerit). Tuotettujen tietotuotteiden, eli erilaisten raporttien, kehitystä tulisi jatkaa. Kokonaisprosessin toimivuus tulisi varmistaa ja muuttaa pysyväisluonteiseksi, mikä on käytännössä edellytys edellä esitetylle laadun kehittämiselle.

### 3.5.3 Jatkokehityksen mahdollisia vaiheita

Kolmannessa kehitysaallossa julkisen hallinnon digitaalisen turvallisuuden riskienhallinta tulisi sovittaa riittävässä määrin yhteen ennakointi- ja tulevaisuustyön kanssa. Tällöin digitaalisen turvallisuuden strateginen näkymä olisi yhteneväisempi muiden yleisen digitalisaation kehitysnäkymien kanssa. Tähän sovittamiseen liittyy myös

valtioneuvostotasoisen riskienhallinnan kehittäminen, joka kokoaa yhteen vertikaalisten hallinnonalojen riskienhallinnan tietoja – tämän prosessin luonnollisestikin ollessa poikkihallinnollinen otos tietystä aihepiiristä.

Kerätyn datan kertyessä ja monipuolistuessa tulisi tiedon käsittelyä ja analysointia automatisoida sen tehostamiseksi ja tarkentamiseksi. Tämä voi tarkoittaa yhteensopivien järjestelmien rajapintojen kehittämistä, mutta myös oppivien järjestelmien hyväksikäyttöä tiedon käsittelyssä erilaisten ilmiöiden ja luokitteluryhmien tunnistamiseksi, jolloin voidaan tehdä kohdennettuja riskienhallintatoimia. Tämä voisi myös toimia syötteenä toiseen suuntaan toiminnallisen tason riskienhallinnalle, organisaatioiden omassa riskienhallintakontekstissa.

Tulevaisuuden muutosten luodessa uudenlaisia riskejä, mutta myös muokatessa toimintaympäristön toimintaa ja teknologiaa, on ensiarvoisen tärkeää tunnistaa uudet riskilähteet ja vaikutusten kanavat. Mikäli näitä ei osata tunnistaa, niitä ei voida myöskään huomioida riskienhallinnassa. Riskienhallinnalle tässä esitettyä mallia ja prosessia tulee arvioida jatkuvasti ja säännöllisesti, kysyen vastaako se tarkoitustaan ja tuottaako se tarvittua tietoa tehokkaasti. Inkrementaalisten tarkasteluiden lisäksi tulisi säännöllisesti muutamien vuosien välein pitää erityisiä kehitystä, laatua ja tulevaisuuden muutoksia tarkastelevia tapahtumia digitaalisen turvallisuuden strategisen riskienhallinnan toteutuksen ympärillä.

## 3.6 Tausta-aineistoja sekä tukimateriaaleja riskien tunnistamiseen

Riskien tunnistamisen kontekstin määrittelemiseksi, eli sisäisten tarpeiden, tavoitteiden ja strategioiden koostamiseksi sekä ulkoisen toimintaympäristön ja siinä toimivien muutostekijöiden tunnistamiseksi, on koottava kattava tausta-aineisto. Näistä muodostuu kiintopiste (tai pisteet) joiden kautta tunnistetaan, mitkä uhat ovat keskeisiä riskejä, joihin pitää kiinnittää huomiota. Osittain sama materiaali sekä muut lähteet tarjoavat myös ajatuksia uusista uhista ja niiden rakenteista, mutta myös riskien kehittymisestä. Näitä tulee käyttää hyväksi riskien tunnistamista tukevana materiaalina, jotta varmistetaan tarkastelussa sekä kattavuus, mutta myös erilaiset näkökulmat, joilla aiheita ja ilmiöitä voidaan lähestyä.

Alla olevassa taulukossa on lueteltu eräitä keskeisiä dokumentteja ja muita lähteitä, mutta lista ei ole täydellinen. Koska aiheeseen liittyvää kertaluonteista tutkimusta ja raportointia tehdään Suomessa laaja-alaisesti, on täydentävä haku tehtävä aina riskienhallintaprosessin syklin alkaessa. Käytetyn materiaalin kattavuutta voidaan tarkastella materiaalien hallintaa kehitettäessä esimerkiksi digitaalisen turvallisuuden keskeisten toteutusalueiden luokittelun kautta.

| Organisaatio | Dokumentti |
|---|---|
| **Digi- ja väestötietovirasto** | Organisaatioiden digiturvallisuus-raportti<br>Digiturvallisuuden riskinäkemyskysely 2021<br>Digiturvabarometri<br>Digihumaus-raportti |
| **Enisa** | Threat Landscape - 2020 |
| **Huoltovarmuuskeskus** | Huoltovarmuuden skenaariot 2030<br>Kyberturvallisuuden nykytila eri toimialoilla 2020 |

| | |
|---|---|
| **Hybridiosaamiskeskus** | Cyber |
| **Information Security Forum** | Threat Horizon 2022<br>Threat Radar 2022 |
| **Kyberturvallisuuskeskus** | Kybersää<br>Kyberturvallisuuden skenaariot 2030 (2022)<br>Kybermittari |
| **OECD** | Digital Security |
| **Sisäministeriö** | Kansallinen riskiarvio 2018<br>Sisäisen turvallisuuden selonteko 2021 |
| **Valtiovarainministeriö** | Julkisen hallinnon uudistamisen strategia<br>Digitaalisen turvallisuuden kustannus-vaikuttavuusraportti 2020<br>Digitalisaation tilannekuva |
| **World Economic Forum** | Global Risk Report 2020<br>Global Risk Report 2021 |

*Taulukko 2: Lista lähteistä riskienhallinnan kontekstin ja toimintaympäristön muutosten määrittämiseen sekä riskien tunnistamiseen.*