DIGI- JA VÄESTÖTIETO-VIRASTO

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta

Riskienhallintamallin rakenne

15.12.2022

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

15.12.2022

Sisällysluettelo

15.12.2022

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta - Riskienhallintamallin rakenne

Tässä asiakirjassa on kuvattu digitaalisen turvallisuuden strategisten riskien hallinnan toimintamallia ja kehitystä siltä osin, kuin sitä on suunniteltu toteutettavaksi julkisen hallinnon laajuisesti. Mallin kehittäminen alkoi 2020 ja se on ollut julkisessa kommentoinnissa keväällä 2022, minkä perusteella on tehty täydennyksiä. Tämä asiakirja on taustoittava yleiskatsaus digitaalisen turvallisuuden ja riskienhallinnan asiantuntijoille. Käytännön toteutusta varten tullaan luomaan kohdennetumpaa tukimateriaalia.

Esitetty toimintamalli 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. Esitetty kokonaisuus on kuvaus toimintamallista ja siihen sisältyvistä prosesseista. Se on pysyväisluonteinen, sillä digitaalinen turvallisuus tarvitsee pitkäjänteistä kehittämistä. Kokonaisuuteen liittyy kuitenkin myös kehitettäviä ja toimintaympäristöjen jatkuvan muutoksen huomioivia osia, joita ohjaavat tulevat tavoitteet ja riskienhallintatyön ohessa selkiytyvät tarpeet. Käytännön toteutusta on esitelty pääkohdiltaan prosessin ja sen kehityksen ymmärtämiseksi, muun muassa turvallisuusnäkökohtien osalta.

Yksittäisen organisaation tavoiteltavaa riskienhallintaprosessia kuvataan standardissa ISO31000. Siihen verrattuna tässä julkisen hallinnon laajuisessa riskienhallintamallissa on keskeisiä eroja, jotka johtuvat tietyt toimivaltuudet omaavien tahojen sekä muiden hajautetusta sijoittumisesta hallinnossa ja digitaalisessa toimintaympäristössä.

- Riskienhallintaprosessin perusteella yhteiseksi hyväksi tehtävien hallintatoimien tarkempi kehitys voi tapahtua erillisesti, toimivaltaisten viranomaisten toimesta, mikä voi tarkoittaa yhtä tai useampaa tahoa. Silti organisaatio on vastuussa näiden toimien toteuttamisessa omassa toiminnassaan. Poikkihallinnollisuus on haaste, jonka ratkaisuna toteutetaan hyvään hallintotapaan perustuvaa yhteistoimintaa, jäykemmän säädöspohjaisen rakenteen sijaan.
- Esitetyssä riskienhallintaprosessissa on huomioitu julkiselle hallinnolle luontainen tarve selkeän päätöksenteon rakenteelle, joka voi kontekstista riippuen sisältää yhden tai useamman tahon. Sen kuvaaminen luo näennäisesti poikkeaman standardiin. Hyvän hallintotavan huomioiminen ei kuitenkaan riko standardia vaan tukee tietojohtamista ja riskiperusteisuutta päätöksenteossa.
- Vaikka riskienhallinnan prosessi on kuvattu kokonaisuudessaan, mallissa painottuu sen alkupuolella muodostettavan tiedon käsittely. Toteutettavat käytännön toimet – kuten tiedon keräys ja analysointi – keskittyvät tämän tukemiseen, jotta prosessin jälkipuoliskolla riskienhallintatoimia voidaan tukea ja ohjata tehokkaasti.

Asiakirja on johdanto-osuuden jälkeen jaettu kahteen osaan. Ensimmäisessä esitellään mallia prosessin ja sen osien avulla. Jälkimmäisessä osassa tarkastellaan malliin liittyviä taustaoletuksia ja rajoitteita sekä hahmotelmaa sen kehittämiseksi tulevina vuosina. Mallin keskeisten osien suunnittelusta ja edistämisestä julkisessa hallinnossa voisi pitkällä aikavälillä vastata Digi- ja väestötietovirastoon mahdollisesti sijoitettava digitaalisen turvallisuuden riskienhallintapäällikkö.

1 Johdanto

Organisaatiot toteuttavat riskienhallintaa kukin omista lähtökohdistaan ja omaan toimintaansa keskittyen, kuten pitääkin. Erikseen tietyistä riskiprosessiin liittyvistä toimenpiteistä vastaavat toimivaltaiset viranomaiset. Riskienhallinnan tulee heijastaa organisaation (tai muun tarkasteltavan kohteen tai kokonaisuuden) toimintaa ja näkemystä itsestään sekä suhdetta ympäröivään toimintaympäristöön. Nykyaikainen riskienhallinta ja modernien, etenkin digiriskien, hahmottaminen vaativat laaja-alaisempaa tarkastelua myös yli omien rajojen, esimerkiksi asiakkaille ja sidosryhmille muodostuviin riskeihin. Niin tiukasti kytkeytyneet ketjut kuin löyhemmät ekosysteemitkin voivat vaikuttaa organisaation kykyyn toimia. Vastaavasti myös julkisessa hallinnon organisaatioiden tulisi tunnistaa miten niiden toimet vaikuttavat muiden, myös yksilöiden, digitaalisen turvallisuuden kehittymiseen.

Valtioneuvostotasoinen riskienhallinta on valmistelussa[1]. Valtioneuvoston tasolla ei ole ollut velvoitetta kerätä säännöllisesti hallinnonalat kattavaa riskitietoa, josta tunnistettaisiin ilmiöitä ja laajempia riskejä tai vertailtaisiin näkymiä niihin. Tämä koskee sekä kaikkien riskien kokonaisuutta että erillisiä aihealueita, kuten digitaalista turvallisuutta. Muuttuvan toimintaympäristön monimutkaistuvista tai hallinnon rajat ylittävistä riskeistä ei ole ajantasaista ja kattavaa tilannekuvaa. Kokonaiskuvan puuttuessa julkishallinnon riskien hallintatoimenpiteiden tukemiseen on voitu kohdistaa vain vaillinaiseen tietoon perustuvaa ohjausta ja resursseja. Koska hallintatoimenpiteiden määrittelyä ja seurantaa organisaatiokohtaisesti, ei julkishallinnossa tehtyjen kehittämistoimenpiteiden vaikuttavuutta ole myöskään voitu arvioida kattavasti[2].

Strategiseen riskikuvaan tunnistetaan useista kansallisista ja kansainvälisistä tietolähteistä sellaisia riskejä, jotka toteutuessaan aiheuttaisivat 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 suunnitelluista hallintatoimenpiteistä saatavien hyötyjen (toimenpiteiden vaikuttavuus) on oltava seurattavia sekä hyväksyttävässä suhteessa toteuttamiskustannuksiin.

[1] Asiaa valmistelleen työryhmän raportti: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163184/VM_2021_28.pdf Kehitysehdotuksessa esitettyihin tavoitteisiin nähden (raportti s.11) tämän mallin avulla tuotettu tieto olisi käytettävissä myös siinä prosessissa, kun se käytännössä kykenee sitä vastaanottamaan. Sitä ennen ja sen lisäksi tieto on käytettävissä normaaleissa virkakanavissa toimivaltaisten viranomaisten kautta. On kuitenkin huomattava, että riskikontekstin taso ja näkökulma muuttuvat, jolloin tietoa arvioidaan eri lähtökohdista ja eri tarpeisiin (raportti s. 27).

[2] Valtiontalouden tarkastusviraston tuloksellisuustarkastuskertomus 20/2018

1.1 Mallin kehityspolku

Julkisen hallinnon riskienhallintaa varten on laadittu melko kattavaa ohjeistusta sekä riskienhallinnan järjestämisen tukemiseksi että keskeisten prosessin osien yhdenmukaistamiseksi. Ohjeistus koskee niin vertailtavuutta, tarkastusten tehokkuutta kuin hyviin käytäntöjäkin. Julkisen hallinnon riskienhallinnassa keskeinen ohjeistaja on valtiovarainministeriön controller-toiminto. Digitaalisen turvallisuuden kokonaisuutta on ohjeistanut julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, eli VAHTI (alkujaan valtionhallinnon tietoturvallisuuden johtoryhmä) sekä sen alainen riskienhallinnan kehittämisen työryhmä. VAHTI-ohjeiden vaikuttavuudesta kertoo jotain se, että vaikka ne eivät ole velvoittavia, niihin edelleen (osin virheellisesti) viitataan. Viimeisin VAHTI-tukimateriaali riskienhallinnasta avasi digitaalisen toimintaympäristön riskienhallinnan käsitteistöä ja viestintää[3], mitä tämäkin asiakirja noudattaa. Annetut ohjeet, niihin liittyvä ohjaus tai muut saatavilla olevat tietolähteet eivät kuitenkaan ole tuottaneet selvää kuvaa niiden soveltamisesta tai esiin nousevista riskeistä – etenkään tietotarpeiden kehittyessä vuosikymmenien aikana.

Riskienhallintamallin lähtökohtana on valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta 8.4.2020 (VM 2020:23)[4]. Päätöksessä on listattu kuusi kehittämisen periaatetta, joista riskienhallintamallin lähtökohtana toimii periaate: ”*johdamme digitaalisen yhteiskunnan turvallisuutta yhdessä tilannetietoon ja riskiarvioon perustuen*”.

Digitaalisen turvallisuuden toimeenpanosuunnitelman 2020—2023 (Haukka)[5] mukaisesti on asetettu poikkihallinnollinen digitaalisen turvallisuuden strateginen johtoryhmä (DTS-JORY). Sen tehtävänä on muun muassa arvioida julkisen hallinnon digitaalisen turvallisuuden strategisen tason tilannetta, luoda ja koordinoida yhteistoimintamallia sekä arvioida, ohjata, koordinoida ja valvoa keskeisiä kehitettäviä digitaalisen turvallisuuden palveluja.[6] Tämän mallin työstäminen ja pilotointi aloitettiin yhdessä asetetun johtoryhmän kanssa. Ryhmän merkittävyys korostuu riskienhallintaprosessin jälkimmäisellä puoliskolla, yhtenä keskeisenä yhteistoiminnan foorumina, jonka avulla toimivaltaiset viranomaiset voivat koordinoida hallintatoimia ja niiden yhteensovittamista. Pidemmällä aikavälillähallinnolliset rakenteet voivat muuttua, , joten yhteisten riskienhallintatoimien koordinaatiota voidaan toteuttaa muullakin tarkoituksenmukaista yhteistyörakennetta hyödyntävällä tavalla, eikä malli ole siten tämän ryhmän määräaikaisuuteen sidottu.

Haukka-hankkeeseen kirjattu tehtäväkokonaisuus riskienhallinnasta käynnistettiin 2020 ja sitä on ohjattu julkisen hallinnon digitaalisen turvallisuuden kehittämishankkeen (JUDO) ohjausryhmässä. Alkuperäisen prosessimallin kehitystä, pilotointia ja

[3] https://dvv.fi/documents/16079645/110183105/VAHTI-riskienhallintasanasto.pdf

[4] Julkisen hallinnon digitaalinen turvallisuus

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

[6] Digitaalisen turvallisuuden strategisen johtoryhmän asettaminen, 19.12.2019 (VN/13510/2019) 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. Lisää tästä kohdassa 2.3.1

sen laajennettua jatkoa ohjasi tietohallintoneuvos Tuija Kuusisto. Hanketehtävän kehitys siirrettiin vuonna 2021 Digi- ja väestötietovirastolle (DVV), projektipäällikkönä on toiminut erityisasiantuntija Juho Reivo.

Riskien ja riskienhallinnan tarkastelulle on nähty pitkäkestoinen tarve, minkä vuoksi esitettyä malli ja siihen liittyvät tehtävät tulisi saada pysyviksi osiksi digitaalisen turvallisuuden johtamista.

1.2 Huomiot ja muutokset kommentoinnista

Tämä asiakirja oli julkisesti kommentoitavana huhtikuussa 2022, jolloin 34 eri julkishallinnon tahoa antoi palautetta ja kommentteja.[7] Yleisellä tasolla huomiot vaihtelivat laidasta laitaan, mutta selvästi pääosa piti digitaalisen turvallisuuden riskienhallinnan kehittämistä ja mallia toivottavina sekä organisaatioiden että yhteisen hyvän kannalta. Vaikka malli ei suoranaisesti tarjoa ratkaisuja mihinkään yksittäiseen uhkaan tai riskiin, tieto ja siitä jalostetut tietotuotteet mahdollistavat itseohjautuvuuden organisaatioiden omissa hallintatoimissa. Lisäksi niitä voidaan hyödyntää osana ohjaustoimia sekä kehittää tehokkaammin toimivaltaisten viranomaisten toimia yhteiseen käyttöön. Asiakirjaan tuottivat tarkennustarpeita myös samaan aikaan kehitteillä olevat digitaalisen toimintaympäristön ja digitaalisen turvallisuuden ohjaukseen liittyvät hallinnolliset muutokset.

Esitetyissä kommenteissa ei tullut esiin ohjauskehikoksi miellettävän mallin rakenteeseen liittyviä muutostarpeita. Niiden perusteella malliin kuuluvan prosessin osia kuitenkin tuodaan paremmin esiin, painottaen sen alkupuolta. Selkeimmin näkyvä osa on riskienarviointiprosessi (tunnistamiseen liittyvä tiedon kerääminen sekä tämän analysointi ja arviointi), jonka käytännön toteutuksen perusteella mallin toimintakin ymmärretään paremmin. Mallin toiminta ei edellytä tilapäisiä työryhmiä, vaikka niitä voidaan käyttää, eikä siinä oteta kantaa siihen, millä rakenteilla julkishallinnossa toteutetaan hallintatoimia. Tieto – sen kerääminen, käsittely ja jakaminen – saa hieman enemmän huomiota kuin riskienkäsittelyn päätöksenteon mallintaminen, jossa luotetaan olemassa oleviin rakenteisiin ja toimintatapoihin. Täten rakenne säilyy standardinmukaisena ja erilaisten rajapintojen hahmottaminen organisaatioiden omaan riskienhallintaan on helpompaa.

Useissa kommenteissa huomio liittyi käytännön toteutuksen tasolla tapahtuviin tai kehitettäviin asioihin. Näitä on avattu mahdollisuuksien mukaan enemmän. Oli nähtävissä, että moni kommentoija ei tunne kattavasti laajempaa digitaalista turvallisuutta, riskienhallinnan prosessia tai he eivät olleet tutustuneet pilotteihin. Jatkossa tätä tukemaan pyritään tuottamaan lisää koulutus- ja tukimateriaalia. Osa piti esitettyä mallia hyvinkin selkeänä, kun taas osa kaipasi materiaaleihin selkeytystä, painottaen nimenomaan viestinnällisiä näkökohtia ja käyttöä. Niitä varten pyritään tuottamaan enemmän ”käyttöohje” tyyppistä yksinkertaistettua materiaalia, erona tähän projektia ja mallia syvemmin avaavaan raporttiin.

Yleisemmällä tasolla mallin merkitys on, että siinä kuvataan toimintaa, jota jo osin pyritään tekemään, mutta ilman selvää muotoa. Kehitettävä kokonaisuus on suunniteltu toteutettavaksi laajentamalla organisaatioiden olemassa olevia

[7] Lausuttavissa Lausuntopalvelu.fi-sivustolla 7.-29.4.2022, minkä jälkeen toimitettiin vielä kaksi lausuntoa.

riskienhallintaprosesseja, eikä sen katsota luovan uutta, muusta toiminnasta irrallista prosessia. Mallin kuvaaminen mahdollistaa sen kehittämisen systemaattisesti ja kattavasti, mikä puolestaan mahdollistaa julkisen hallinnon digiturvallisuuden laadukkaamman tukemisen. Julkishallinnon yhteisen riskienhallinnan tavoitteena on kyky tunnistaa ja yhteisesti kohdata suurempia haasteita, jotka koskettavat useimpia, mutta joiden käsittely yksittäisen organisaation toimesta voi olla mahdotonta.

2 Strateginen riskienhallintamalli

Riskienhallintamalli koostuu kattavasta, systemaattisesta, toistettavasta ja kehittyvästä prosessista sekä siihen liittyvistä tehtävistä. Suunnitellun mallin toteuttaminen – yhdessä muiden riskienhallintaan liittyvien toimien kanssa – muodostaa riskienhallintajärjestelmän, eli systemaattisen tavan hallita riskejä. Mallin suuntaus ja rajat muodostavat siitä digiturvallisuuden strategisen riskienhallintamallin. Näitä määrittelyitä on avattu tarkemmin tämän asiakirjan osassa 3.2.

Riskienhallintamallin on tarkoitus erityisesti mahdollistaa poikkihallinnollisten ja laajojen jaettujen riskien tunnistaminen hajautettuun rakenteeseen perustuvassa julkishallinnossa, sekä niiden arviointi ja käsittelyyn ohjaus sekä hallintatoimien tehostaminen. Jotta aidosti hyödylliset toimenpiteet olisivat mahdollisia, huomioon on otettava useita toteutukseen vaikuttavia yksityiskohtia. Mallissa painotus on digitaalisen turvallisuuden riskien kokoamisella ja arvioimisella sekä strategisen tason riskianalyysien laatimisella tarvittavassa muodossa, toteutuksen maturiteetin rajoissa. Niiden avulla tuotetaan syötettä ja vaihtoehtoja erilaisten hallintatoimien muodostamiseen, päätöksentekoon ja toteutukseen. Näin mahdollistetaan laadukkaampi riskitietoinen ja tietoon pohjautuva päätöksenteko.

2.1 Nykytilan kuvaus

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

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

Kysely toteuttaa osaltaan riskienarviointiprosessia, joka on osa riskienhallintaprosessia. Arviointiprosessin 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 saatuja tuloksia voidaan jo hyödyntää, niin tehtyjen pilottien pohjalta voitiin tunnistaa useita kehityskohteita, joilla prosessia ja sen laatua voidaan kehittää. Esimerkkejä kehityskohteista:

- Riskien tunnistaminen on tehty rajatun asiantuntijaryhmän toimesta, mikä ei takaa kattavuutta. Tämä toisaalta auttaa kohdistamaan ja rajaamaan kyselyn laajuutta.

[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 määritelty kattavasti muun muassa toimintaympäristöä ja kriteereitä.
- Vastauksissa arviot perustuivat eri organisaatioissa toimivien virkamiesten asiantuntijanäkemyksiin. Tarkempien arvioiden tekemiseksi ja tilastollisen merkittävyyden takaamiseksi vastausten määrän tulisi olla suurempi.
- Analyysi hakee vielä muotoaan, sillä se perustuu suppeaan määrään lähteitä, eikä sisällä esim. historiatietoihin perustuvia muutostrendejä.
- Tuotettu tieto perustuu rajalliseen analysointimetodologiaan, mikä tosin on riippuvainen kerättävän tiedon määrästä ja laadusta.

Riskienhallintamallin ollessa vielä kehitysasteella, tarkkaa tai kattavaa strategisiin tavoitteisiin sidottua riskinäkemystä ei myöskään pystytty tarjoamaan, vaikka huomiota osattiinkin kiinnittää tunnettuihin haastaviksi tiedettyihin osa-alueisiin. Laajan ja päivittyvän tietomäärän käsittely perinteisenä kyselynä ei ole käytännöllistä, joten jatkoa varten riskienhallinnan kyselyt toteutetaan sähköisenä palveluna. Keskeisimmät pitkän aikavälin kehityskohteet ovat laajemman prosessin rakentaminen sekä siihen liittyvien tukijärjestelmien kehittäminen. Kehitystoimia on kuvattu tarkemmin tämän asiakirjan myöhemmissä osioissa.

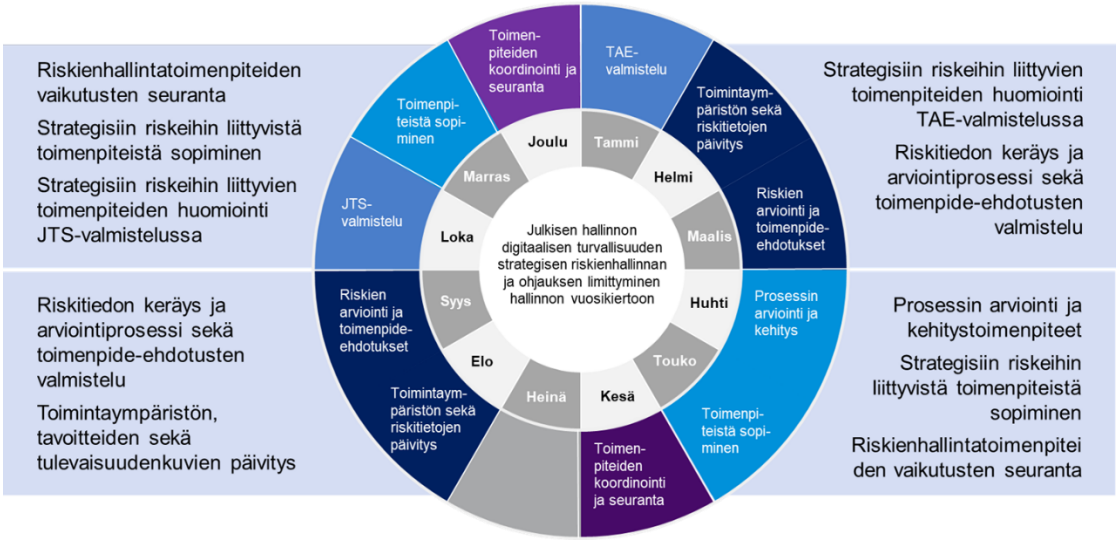
2.2 Riskienhallinnan vuosisuunnittelu

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 prosessinkehittämiseksi. Riskienhallinnan syklejä, ja joissain tapauksissa yksittäisiä vaiheita, voidaan toteuttaa tasaiseen rytmiin tai tarpeeseen perustuen (ns. dynaamisesti). Säännöllisesti toistuessaan riskienhallinta on usein sidottu toimintaa ohjaaviin rakenteisiin, kuten suunnittelun ja raportoinnin prosesseihin, dynaamisesti tarve riskienhallinnalle voi olla esimerkiksi havaittu uhka tai seuratun raja-arvon ylitys. Yleisesti ottaen riskienhallinnassa pitää kyetä molempiin, mutta riippuu organisaation toimintatavoista, missä suhteessa näitä kahta käytetään ja 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 esitetty pääkohdittain alla olevassa vuosikellossa. Riskienarviointiprosessin tavoiteltu sykli toteutuisi kahdesti vuodessa, jolloin tuettaisiin vuosisuunnittelua sekä kehitystarpeita niin organisaatioiden omassa toiminnassa kuin julkisen hallinnon yhteisissä tarpeissa. Mallin toteuttamisessa tulee pyrkiä oikea-aikaisuuteen, jotta talousvaikutteisten toimien suunnittelu ja päätöksenteko ehditään tehdä kaikilla tasoilla. Muuten hallintatoimiin asti pääsy voi laajoissa kokonaisuuksissa siirtyä seuraaviin vuosiin, mitä tulisi pyrkiä minimoimaan. Yhtä lailla, tulevaisuutta ennakoivissa strategisen tason toimissa talousvaikutteisia toimenpiteitä ei voi tehdä ohi JTS-prosessin.



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 kesän lomakausi. Riskienhallintamallin kokonaisuuden kehittämiseen liittyvät suuremmat suunnitellut muutokset on hyvä aikatauluttaa tapahtuvaksi pääosin keväisin, jotta niitä voidaan tarvittaessa tarkastella hyvissä ajoin ennen syksyn taloussuunnittelua mahdollisten budjettivaikutteisten toimien valmistelemiseksi.

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 eri viranomaiset arvioivat riskejä ja toimenpide-ehdotuksia sekä koordinoivat niiden kohdentumista ja yhteistoimintaa, tehden päätöksiä riskien seuraamisesta, tarkentamisesta tai hallintatoimenpiteiden suosittelemisesta. Koordinaatio voi tapahtua yhteistyöryhmissä, kuten digitaalisen turvallisuuden strategisessa johtoryhmässä (DTS-JORY), tai se voidaan tarjota suoraan toimivaltaisille viranomaisille. Toimenpiteet voidaan tehdä koko julkisen hallinnon laajuisesti tai niiden toteutus voi olla organisaatiokohtaista. Yhteisesti tehtävissä toimissa, kuten hankkeissa, hallintatoimenpiteille määritellään vastuutaho ja ohjausryhmä normaalien toimintatapojen

mukaisesti. 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). Prosessi kuvaa tiedon siirtymistä ja eri osioiden toteutusvastuita toimijoiden välillä. Se näkyy eri toimijoille vain osin, riippuen heidän roolistaan, joten sitä voidaan kutsua hajautetuksi prosessiksi. Prosessiin liittyviä määrittelyitä on avattu tarkemmin tämän asiakirjan osassa 3.2.

2.3.1 Prosessin toimijat ja roolit

Prosessin eri vaiheissa on erilaisia keskeisiä rooleja. Yksittäisessä organisaatiossa nämä roolit olisivat selkeästi osa tehtävänkuvia ja vastuutettu linjaorganisaatioon, organisaation lävistävien toimintojen asiantuntijoille ja johdon tuelle, kuten sisäiselle tarkastukselle. Huomattavaa on, että prosessiin osallistuvien organisaatioiden edustajat voivat toimia hyvinkin erilaisilla nimikkeillä, mutta heidän odotetaan tiedon keräyksessä tuovan esiin organisaationsa kokonaisnäkemyksen. Se tarkoittaa niin erilaisten palveluiden tuottamisen tarkastelua, asiantuntemusta digiturvallisuuden eri toteutusalueilta kuin johtotason näkemystä näiden merkityksestä. Prosessiin osallistuminen voi tapahtua vaiheittain, jolloin sopivimman asiantuntemuksen omaava edistää prosessia, mutta sen mahdollistamiseksi on varmistettava tietojen siirtyminen ja sitä tukevat järjestelyt. Tähän tulee kiinnittää huomiota, sillä yksittäisestä organisaatiosta poiketen, julkishallinnossa ei ole sellaista riskienhallintapäällikköä, jolla olisi mahdollisuus olla fasilitoimassa kaikissa vaiheissa kokojulkishallinnossa tai joka omaisi niin laajaa määräysvaltaa tai budjetointia.

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

Rooli	Kuvaus
Riskienhallintapäällikkö	Digi- ja viestintävirastoon (DVV) sijoitettu julkisen hallinnon digitaalisen turvallisuuden tehtävä, jonka vastuualueeseen kuuluu riskienhallintamallin mukaisen järjestelmän kehitys, prosessin ylläpito, laadun parantaminen sekä koostavien tilannekuvien muodostaminen ja raportointi. Tähän sisältyy digitaalisen turvallisuuden valittujen riskien koonti, luettelointi sekä tietojen ylläpito ja seuranta. Tehtävässä tuotetaan riskeistä sekä riskienhallinnasta arvioita ja analyysejä sekä muuta julkisen hallinnon digiturvallisuuden riskienhallintaa kehittävää materiaalia itsenäisesti sekä asiantuntijaryhmien 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. Asiantuntijoiden osallistumisen tarkoitus ei ole vain tukea riskienhallintapäällikköä, vaan tarkastelu eri näkökulmista on keskeinen prosessin laatuun vaikuttava tekijä. Riippuen riskienhallintapäällikön määrittelemän tarpeen mukaisesti asiantuntijat voivat olla julkisesta hallinnosta tai sen ulkopuolelta.
Kokonaiskuvapalvelun tuoteomistaja	Digi- ja väestötietoviraston tuottaman digitaalisen turvallisuuden tilannekuvatietojärjestelmän kehittämisestä, yhteensovittamisesta sekä tiedon hyödyntämisestä vastaava henkilö, jonka vastuulla on palveluiden kehittämisessä huomioida tämän riskienhallintaprosessin tarpeet yhteistyössä riskienhallintapäällikön kanssa.
Julkisen hallinnon organisaatiot ja näiden keskeiset asiantuntijat	Organisaatioiden riskienhallinnan ja/tai digiturvallisuuden asiantuntijat tuottavat, siirtävät ja (uudelleen)arvioivat tietoa uhista, riskeistä ja riskienhallinnastaan kokonaiskuvan muodostamista varten, edustaen organisaationsa ylemmän tason näkemystä digiriskeistä. Samalla he saavat tietoa oman organisaationsa riskinäkymästä suhteessa muihin vastaaviin toimijoihin ja koko julkishallintoon. Niiden perusteella organisaatiot voivat kehittää omaa riskinäkemystään, riskienhallintatoimiaan ja antaa syötteitä ylemmälle johtotasolle organisaation toiminnan ohjaamiseen. Organisaatiot voivat asiantuntijoidensa välityksellä myös osallistua toteutettaviin yleisiin hallintatoimiin ja niiden soveltamiseen omassa organisaatiossaan.
Toimivaltaiset viranomaiset	Toimivaltaiset viranomaiset ovat asiakkaina tuotetulle tiedolle, minkä perusteella ne voivat vastuualueellaan ohjata toimia ja omaa toimintaansa. Prosessissa ne toimivat oman toiminta-alueensa mukaisesti vastuullisena toimijana, joka tuottaa tarpeelliseksi ja tarkoituksenmukaisiksi katsottuja toimia riskien hallitsemiseksi, mukaan lukien uhka- ja riskitiedon jakaminen. Laajoissa julkisen hallinon strategisissa riskeissä tämä voi tarkoittaa myös yhteishankkeita useiden osapuolten kesken. Toimivaltaisuuden määrittelyssä on huomattava, että sen kapean määrittelyn sijaan painotetaan sopimuksellisuutta. Toimivaltaisuutta määritellään laissa pääosin nimenomaisena ja rajallisena (alueellisena, asteellisena tai asiaan kohdistuvana), mutta organisaatioilla on myös laajat mahdollisuudet ja velvollisuudet sopimalla vaikuttaa riskeihin, osallistua eri yhteistyöelimien kautta ja jakaa omassa toiminnassa kehittynyttä tietoa. Riskejä ja riskienhallintaa koskevaa toimintaa voidaan siis käsitellä monin tavoin yhteisinä asioina, ilman että vastuut siirtyvät tai hämärtyvät.

Hallintatoimia toteuttavat asiantuntijat	Erillisten kehityshankkeiden kautta riskienhallintatoimia suunnittelevat ja toteuttavat asiantuntijat toimivaltaisissa viranomaisissa sekä näiden yhteistyökumppanit. Kyseessä voi olla myös usean toimijan toteuttama kokonaisuus. Toimivaltaisten organisaatioiden tulisi varmistaa, että toimeenpanevien tahojen tuotoksista palautuu tieto myös riskienhallintaprosessiin (esim. julkisen hallinnon verkostoihin, kuten VAHTI), jotta toimien vaikuttavuutta ja kohdistumista julkisessa hallinnossa voidaan arvioida tehokkaasti.

Taulukko 1a: Digitaalisen turvallisuuden riskienhallinnan prosessin keskeiset toimijaroolit

Lisäksi on toimijoita, joilla voi olla merkittävä rooli riskienhallintamallin prosessin toteutumisen edistämiseksi ja kehittämiseksi. Tämä ei ole tyhjentävä lista, eikä sisällä esimerkiksi digiturvallisuuden sisällä tehtävää eri toteutusalueiden turvallisuutta ja yhteistoimintaa edistävää työtä (esimerkiksi turvallisuuskomitean rooli kyberturvallisuuden edistämisessä tai tietosuojavaltuutetun toiminta tietosuojaan liittyen) tai tahoja, joiden toiminta palveluntarjoajina mahdollistaa laajan vaikuttavuuden. Listattuina eivät myöskään ole ne monet viranomaistahot, joiden kanssa tiedonvaihto on mahdollista.

Toimija	Kuvaus
Digitoimisto	Digitalisaation ja datatalouden vastuualueen pysyvä yhteistyöryhmä, jonka tehtävänä on vahvistaa ministeriöiden välistä yhteistyötä, koordinaatiota ja tiedonkulkua digitalisaatiossa ja datataloudessa. Digitoimisto ei suoranaisesti ole liitoksissa riskienhallintaprosessiin, mutta sen tehtäväalueen koordinaatiotoimet voivat olla merkittävä vaikuttaja erilaisten laajojen strategisten riskien hallinnassa sekä niihin liittyvien mahdollisuuksien jalostamisessa. Digitoimiston koordinoimat strategiset tavoitteet (”digikompassi”) vaikuttavat merkittävästi digiturvallisuudenkin riskien tunnistamiseen ja arviointeihin.
Digitaalisen turvallisuuden strateginen johtoryhmä	Toimivaltaisia viranomaisia edustaa digitaalisen turvallisuuden strategisen johtoryhmä (DTS-JORY)[10], jonka tehtäväksi on asetettu käsitellä riskitilannekuvaa sekä siihen mahdollisesti sisältyviä toimenpide-ehdotuksia julkishallinnon poikkileikkaavan koordinaation toteuttamiseksi. Se tukee perustamaan tarvittavat digitaalisen turvallisuuden kehityshankkeet toimivaltaisten viranomaisten toimesta. Tässä DTS-JORY rinnastuu toimivaltaisiin viranomaisiin, sillä se on niiden muodostama. Se myös osallistuu riskienhallintamallin kehittämiseen palautteen ja asiantuntijuuden muodossa. Riskienhallintamallin näkökulmasta DTS-JORY:n rooli on tehostaa riskienhallintaa, erityisesti hallintatoimien toteuttamisen osalta.

[10] https://vm.fi/hanke?tunnus=VM025:00/2020

VAHTI-johtoryhmä (julkisen hallinnon digitaalisen turvallisuuden johtoryhmä) sekä VAHTI-työryhmät	Vuoden 2020 alusta Digi- ja väestötietoviraston vastuulle siirretty toiminto, joka toimii julkisen hallinnon keskeisten operatiivisten organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä. VAHTI-johtoryhmä käsittelee muun muassa sille tuotettua riskiraportointia ja digitaalisen turvallisuuden tilannetta sekä näiden perusteella mahdollisesti kehitettäviä toimenpiteitä, mukaan lukien näitä tukevien toimintamallien ja järjestelmien kehityksen ohjaukseen osallistuminen palautteellaan. Johtoryhmä kokoontuu viisi kertaa vuodessa. VAHTI-johtoryhmän alaisuuteen on asetettu tällä hetkellä viisi VAHTI-työryhmää, joista yhden työryhmän tehtävänä on digiturvallisuuden riskienhallinnan kehittäminen.

Taulukko 1b: Digitaalisen turvallisuuden riskienhallinnan prosessia tukevat toimijat

2.3.2 Prosessin osat ja vaiheet

Riskienhallinnan prosessiin on laadittu kolme keskeistä näkymää, sillä kokonaisprosessissa tuotetaan vastaus kolmeen tarpeeseen.

1. 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.
2. Toinen näkymä sisältää ohjaavan toiminnan tukemiseksi muodostettavaa tietoa ja tarjoaa toimivaltaisten viranomaisten ja hallinnonalojen johdolle näkymän riskienhallintaprosessiin julkisen hallinnon laajuisena kokonaisuutena.
3. Kolmas näkymä palvelee strategisen tiedonhallinnan prosessia[11] eli tarjoaa pääasiassa riskipäällikölle näkymän kokonaisuuteen (joskaan prosessin loppuosan käytännön toteutumisesta ei ole mahdollista saada täyttä kuvaa hajautetussa rakenteessa). Sen pysyväisluonteisena tehtävänä on vastata ”tietopyyntöön” koskien digitaaliseen turvallisuuteen vaikuttavia riskitekijöitä, mitä riskipäällikkö toteuttaa. Tämän sisällä voidaan tehdä kohdistamista julkisen hallinnon ohjauksen painopisteiden ja tavoitteiden mukaisesti, mutta myös huomioiden toimintaympäristön ja sen ilmiöiden kehitys. Lopputuloksena on tarkoitus tuottaa tietoa erilaisiin tietotuotteisiin, sovitettuna eri käyttötarkoituksiin ja erilaisiin näkökulmiin.

Hyvän hallintotavan mukainen päätöksenteko edellyttää sen tuomista esiin klassisessa neliosaisessa jatkuvan kehityksenprosessissa[12]. Tämä ei niinkään muuta prosessia, vaan alleviivaa sitä, että siirrytään suunnittelemisesta toteutukseen hyväksyttävällä tavalla, noudattaen sovittuja päätöksentekoprosesseja. Tässä vaiheessa

[11] Strategisen tiedonhallinnan prosessi, niin sanottu tiedusteluympyrä (tieto ”kehittyy” ja tarkentuu prosessissa, eli uuden tai päivitettävän raportoinnin pohjana on aiempi), rakentuu eri vaiheista ja yleensä siihen kuvataan muun muassa tietopyyntö, sen tarkempi määrittely, tiedon keräys, tiedon käsittely, tiedon analysointi, raportoinnin muodostus sekä raportin viestintä. Yksinkertaistaen, se toimii viitekehyksenä johdon taholta asiantuntijoille annettaville laajemmille selvitystehtäville. Tätä on sovellettu myös esitettyyn strategisen riskienhallintamallin tiedon tuottamisen rakenteeseen. Erona muunlaiseen tutkimukseen, tuotos on luonteeltaan ”parasta saatavilla olevaa tietoa”, jota määräajassa ja muiden rajoitteiden sisällä voidaan koota.

[12] PDCA (plan, do, check, adjust / act) ja sen variaatiot, eli ”suunnittele, tee, tarkista, korjaa / tee pysyväksi”. Merkittävää on jatkuvaa kehittymistä tukeva toistettava prosessi, kuten riskienhallinnan prosessi ISO31000 sisältää.

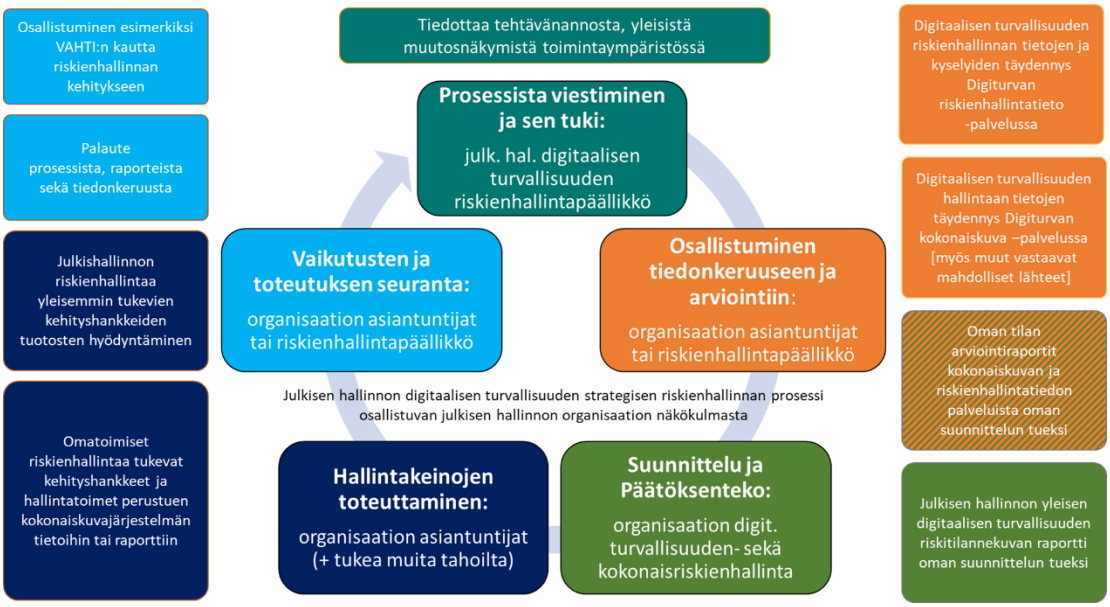
tapahtuu riskitietoinen päätöksenteko, jossa huomioidaan esimerkiksi suhteutus muihin tavoitteisiin sekä dokumentoidaan ja hyväksytään jäännösriskit.

On huomattava, että kaikki prosessin osat sisältävät useampia toimenpiteitä ja osaprosesseja. Yleinen rakenne säilyy ennallaan, vaikka osien sisältöjä täydennettäisiin tulevaisuudessa. Prosessin osiot voivat myös käytännössä toteutua limittäin, erityisesti laajoja hallintatoimia kehitettäessä, sillä niiden saattaminen loppuun voi kestää useita prosessin syklejä.

Julkisen hallinnon riskienhallinnan kokonaisprosessia voidaan pitää hajautettuna, sillä sitä toteuttavat yhden organisaation sijaan eri toimijat eri vaiheissa. Julkisen hallinnon riskit ovat usein yhteisiä, useimpiin toimijoihin kohdistuvia uhkia, joiden merkitykset jaetaan toimijoiden kesken. Niiden tarkastelu "virtuaalisina kokonaisuuksina" voi tarjota analogian tämän hahmottamiseen. Tämänkaltainenkin rakenne tuottaa riskienhallintaa standardoitua prosessirakennetta soveltaen. Hajautuksen etuina voidaan nähdä laaja-alaisuus (osaaminen, resurssit) ja häiriönsietoisuus, mutta vastaavasti se on vähemmän tehokas kuin yksittäisen toimijan prosessi.

Oheisista prosessia avaavista rakennekuvista voidaan tunnistaa eri toimijoiden väliset yhtenevyydet.

Kuva 2: Yleiskuva riskienhallinnan kokonaisprosessin mallin päävaiheista. Viides vaihe, joka on lisätty perinteiseen neliosaiseen kehittämisprosessiin, on julkishallinnossa korostuva päätöksenteko. Se sisältyy myös normaaliin nelivaiheiseen (hyvin yksinkertaistettuun) prosessiin, mutta sitä on korostettava; se toimii merkittävänä kiintopisteenä hallintoprosesseissa, se jakaa prosessin kahtia ja prosessin yksi merkittävä funktio on tuottaa tietoa päätöksentekoon, jossa riskitieto yhdistetään muihin tietoihin ja näkemyksiin. Päätöksentekoon sisältyy myös vastuiden dokumentointi, mukaan lukien jäännösriskien hyväksyntä tarvittavan korkealla päätäntätasolla. Yleiskuva tarkentuu ja laajentuu kolmeen hieman eroavaan näkymään toisiinsa liitoksissa olevista prosesseista. Riskienhallintaan kuuluu lisäksi tukevia toimintoja, kuten viestintä, joka liittyy eri tavoin jokaiseen prosessin vaiheeseen.



Kuva 3: Julkisen hallinnon digitaalisen turvallisuuden strategisen riskienhallinnan prosessi osallistuvan organisaation näkökulmasta. Painotus on julkisen hallinnon strategisen riskienhallinnan merkityksessä organisaation oman riskienhallinnan tukemiseksi. Käytännön toteutuksen tasolla etenkin ensivaiheessa vertailutieto on suuntaa antavaa ja anonymisoitua, perustuen erilaisiin ryhmittelyihin (esimerkiksi organisaation koon ja toimialan mukaisesti). Organisaatioilla on mahdollisuus soveltaa prosessia omaa päätöksentekoa tukevan suunnittelun, toteutuksen ja seurannan tukena..

Kuva 4: Julkisen hallinnon digitaalisen turvallisuuden strategisen riskienhallinnan prosessi ohjauksen näkökulmasta. Painotus on riskienhallintatoimien sekä muun ylemmän tason päätöksenteon tarvitseman tiedon tuottamisessa. Ohjauksselliset tarpeet myös suorasti tai epäsuorasti liittävät prosessin osaksi laajempiakin ohjauksen rakenteita, jolloin se toimii syötteenä myös laajempaan päätöksentekoon digiturvallisuuden riskienhallinnan ulkopuolelle. On muistettava, että moniin turvallisuuden näkökulmasta tunnistettaviin riskeihin voidaan vaikuttaa muussa toiminnassa, esimerkiksi ehkäisemällä jo suunnitteluvaiheessa riskien syntymistä ja kehittymistä.

Kuva 5: Julkisen hallinnon digitaalisen turvallisuuden strategisen riskienhallinnan prosessi tiedonhallinnan toteutuksen näkökulmasta. Painotus on prosessin alkupuolella, tiedon tuottamisen prosessissa, jossa voidaan tehdä tiedonvaihtoa toisten toimijoiden ja tietolähteiden kanssa. Tiedon tuottamisen prosessissa tuotetaan ennakointitietoa sekä vaihtoehtoja ja ehdotuksia päätöksenteon syötteiksi. Se, miten näitä hyödynnetään, on riippuvainen riskienhallinnan prosessin ulkopuolisista asioista päätöksenteossa (muut strategiset tavoitteet, resurssit jne.).

Prosessin ensimmäisessä vaiheessa kootaan lähtötiedot digitaalisen turvallisuuden strategisen tason riskiarvioprosessia varten. Siinä 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) ylläpitämässä digiturvan kokonaiskuvapalvelussa, jossa on osiot organisaation hallinnolliselle digiturvalle sekä digiturvan riskitiedolle. Digiturvan riskienhallintatieto -palvelu toimii riskienhallinnan työkaluna, varmistaen kerätyn tiedon turvallisuuden, yhdenmukaisuuden sekä pitkäjänteisen käytön. Palvelu on käytännön toteutus osasta prosessia, jolla tuotetaan osallistuville organisaatioille vertailutietoa riskeistä ja riskienhallinnasta julkisessa hallinnossa toiminnan itsenäiseksi kehittämiseksi.

Digiturvan riskitiedon palvelua täydentävinä lähteinä analyysien kokoamisessa voidaan hyödyntää muita kansallisia ja kansainvälisiä tietolähteitä (raportit, tutkimukset, tietokannat, tietotuotteet yms.). Merkittävin on samalla alustalla toimiva digitaalisen turvallisuuden kokonaiskuvaa kokoava palvelu, jossa on oma riskienhallinnan hallintajärjestelyitä tarkasteleva osionsa. Mahdollistamalla kerättyjen tietojen ristiin hyödyntäminen tarvittavilta osin, säästetään käyttäjiltä vaivaa molemmissa kyselyissä ja annetaan tietoja tarkasteltaessa arvioinnille parempi konteksti.

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 päätösehdotuksiksi jatkokäsittelyyn hallintakeinoille hahmotelmat.

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 käytössä olevia muita tietoja, kuten toiminnallisia ja taloudellisia seikkoja, jotka voivat ohjata vaihtoehtoja. Julkishallinnon organisaatioiden tulee huomioida laajemmat riskinäkymät osana organisaation kokonaisriskienhallintaa.

Riskienhallinnan hallintakeinojen toteuttaminen sisältää eri toimenpiteiden tarkentamisen tarvittavilta osin toimivaltaisten viranomaisten toimesta. Niitä voivat olla hankkeistaminen, mahdollisten yhteistyötahojen kanssa sovittavat työnjaot, rahoituksen, toimintakehyksen tai projektien tavoitteiden ja aikataulun selventäminen. Lisäksi sovitaan toimenpiteiden etenemisen seurannasta ja vaikutusten arvioinnista sekä varmistetaan jälkiseuranta. Hallintatoimenpiteiden toteutuksen etenemisestä tulisi informoida tarkoituksenmukaisessa määrin ja tavalla niiden kohteita sekä koordinaatiossa mukana olevia tahoja, mukaan lukien julkisen hallinnon digitaalisen turvallisuuden riskienhallintapäällikkö, joka ylläpitää riskinäkymää.

Organisaatioiden omiin riskinarvioprosesseihin tuottamat tiedot toimivat pohjatietona strategisen tason riskianalyysille. Niiden jakaminen tuottaa vertailutietoa riskien ja riskienhallinnan tilanteesta julkisessa hallinnossa, jolla voidaan kehittää organisaatioiden yhteistä näkymää digitaalisen turvallisuuden tilasta. Organisaatiot hyötyvät laajemmista julkishallintoon toteutettavista 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 edelleen laadullisesti sekä 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 ovat olennaisia, 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 prosessiin. Nämä taustaoletukset suoraan, tai näiden päälle rakentuvat tarkennusmahdollisuudet, antavat strategisen tason toimijoille mahdollisuuksia ymmärrettävästi ja määritellysti kohdentaa riskienhallintaa tarpeiden mukaan.

3.1 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. Mallin osioista on nyt luonnosteltu kehitysvaiheita, joita voidaan tarpeiden, teknologian ja toimintaympäristön kehittyessä muuttaa.

Riskienhallintamallin tehtävä on toimia tukena ennakoitaessa tulevia digiturvallisuuden haasteita, muun muassa tuottamalla yhteisesti jaettua tietoa. Siihen kuuluvien prosessien tehtävänä on varmistaa pyrkimys luotettavaan laatuun ja jatkuvuuteen. Tarkoitus on luoda digitaalisen turvallisuuden strategisen tason riskeistä ja riskienhallinnasta tilannekuvaa, jonka avulla pystytään vaikuttamaan muun muassa 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 mahdollisia muita organisaation toimintaan liittyviä erityisiä digiturvan toteutuksen osa-alueita, toteuttaa kukin organisaatio itsenäisesti, mutta niillä toimii myös nimettyjä 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 strateginen johtoryhmä (DTS-JORY)[13], 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 muodostavat digitaalisen turvallisuuden keskeiset toimivaltaiset viranomaiset. DTS-JORYn tehtävänä on tarkastella kuvaa digiturvallisuuden hallinnan, tietoturvan, tietosuojan, kyberturvallisuuden sekä jatkuvuuden ja varautumisen riskitilanteesta, joiden perusteella voidaan sopia jatkotoimista. On oleellista, että johtoryhmä myös seuraisi jatkotoimien toteutusta mahdollisimman pitkälle sekä antaisi palautetta päätöksentekoa tukevasta tiedosta prosessin laadunhallinnan parantamiseksi.

[13] https://vm.fi/hanke?tunnus=VM025:00/2020

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, VAHTI (alun perin ”Valtionhallinnon tietoturvallisuuden johtoryhmä”), jonka nykyinen toimikausi on 01.03.2020 - 31.12.2024, on julkisen hallinnon digitaalisen turvallisuuden kehittämisen yhteistyö-, valmistelu- ja koordinaatioelin. Sen toiminta kehittää digiturvallisuuden riskienhallintaa ja se voi kommentoida riskienhallintamallin rakenteita ja toteutusta osana toiminnan tavoitteeksi kirjattua 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 ja riskienhallinnan kehittämisen työryhmän kautta strategiseen riskienhallintakokonaisuuteen osallistuvat organisaatiot voivat vaikuttaa sen kehittämiseen.

Julkishallinnon organisaatioiden on tarkoitus saada tukea omaan riskienhallintatyöhönsä prosessissa tuotetun riskejä, riskienhallintaa ja riskienhallintajärjestelmiä koskevan tilannekuvatiedon sekä laajempien hallintatoimien kautta. Vertailutiedon tulisi myös mahdollistaa itsearviointi sekä itseohjautuvuus digiturvan järjestämisessä. Asiaa yleisemmin tarkasteltuna, julkishallinnon laajuisen suuremman kokonaisuuden riskienhallintaprosessi toteutuu virtuaalisesti ja loogisesti eri toimijoiden toteuttaessa sen eri osia, kun organisaatiot toteuttavat omaa sisäistä riskienhallintaansa tai osallistuvat yhteisen riskitiedon tuottamiseen. Organisaatioiden käytännön tasolla tässä esitetyssä riskienhallintamallissa tuotetun tuen voi kuitenkin olettaa olevan pääosin soveltamista vaativaa (organisaatioiden yksilöllisyys) tai välillistä (mm. hallintorakenteet ja epäsymmetria riskeihin nähden). Niiden seurauksena positiivisten vaikutuksien odotetaan siirtyvän organisaatioiden asiakkaiden ja sidosryhmien digiturvallisuuden tasoon ja kokemukseen.

3.2 Perusoletukset ja rajaukset

Riskienhallintamallin suunnittelussa ja toteutuksessa on sovellettu kansainvälisiä riskienhallinnan standardeja[14]. Mallissa kuvatun prosessin tuottamien riskien merkitysten ymmärtämiseksi on pyritty tunnistamaan rakenteen sisältämät keskeiset kontekstit, rajaukset ja valinnat. Nämä pyritään tuomaan esiin. Niiden lisäksi, kun prosessia toistetaan, on tarkasteltava mitä oletuksia ja määrityksiä tehdään toimintaympäristöön ja sen muutoksiin liittyen. Sen lisäksi, että toimintoympäristön merkitys on huomioitava riskien suhteen, tulee myös tarvittaessa arvioida, onko riskienhallintamallin perusoletuksia ja rajauksia päivitettävä ja mallia muutettava, jotta se vastaa todellisuutta ja sille asetettuja tarpeita.

Käsitteistössä pyritään noudattamaan digitaalisen turvallisuuden riskienhallinnalle kehitettyä sanastokokonaisuutta (2022)[15], joka täydentää ISO31000- ja ISO73-

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

[15] Syvällinen riskienhallinnan prosessin ja viestinnän läpikäynti termeineen tältä alueelta on julkaisu VAHTI Hyvä Käytännöt -tukimateriaaleissa https://dvv.fi/digiturvajulkaisut ja sanaston julkaisu tapahtuu Yhteentoimivuusalustan Sanastot-työkalussa https://sanastot.suomi.fi/ myös ruotsiksi ja englanniksi

sanastoja[16] sekä soveltuvin osin kokonaisturvallisuuden[17] ja kyberturvallisuuden[18] sanastoja. Digitaalisen turvallisuuden kokonaisuuden hallinnan laajempi esittely on riskienhallintasanaston liitteessä 1. Tässä asiakirjassa ilmaistut määrittelyt ja käytetyt esimerkit ovat sovelluksia riskienhallintasanastossa yhteisesti sovituista määrityksistä.

3.2.1 Sisäinen näkymä ja tarkastelulle merkityksellinen näkökulma

Tarkastelu on pääasiassa rajattu Suomen julkishallinnon organisaatioihin. Tämän katsotaan sisältävän laajasti valtion virastot, liikelaitokset, ministeriöt ja muut toimijat sekä kunnat ja erilaiset kuntayhtymät. Julkishallinto tässä yhteydessä ymmärretään samassa laajuudessa kuin tiedonhallintalaissa on määritelty tiedonhallintayksiköt.

Julkishallinto-rajauksen ulkopuolelle jäävät 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 riskienhallintatieto voi olla sovellettavissa myös julkishallinnon ulkopuolella ja antaa kansalaisille osaltaan kuvaa julkishallinnon kyvystä huolehtia digiturvallisuudesta, mikä voi olla merkittävää demokratian ja luottamuksen kannalta. Riskeille kehitettävissä hallintatoimissa tulee pyrkiä huomioimaan julkishallinnon alihankintaketjuissa sekä sen ulkopuolella toimivat tahot.

Digiturvallisuus on valittu erityiseksi tarkastelun aiheeksi, jota käytetään poikkileikkaamaan julkisen hallinnon alueita. Se on otettava sisäisenä määrittelynä, vaikka itse termi on asetettu kaiken kattavaksi. 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. Digiturvallisuuteen luettaviin asioihin voidaan ottaa kapeampia tai kattavampia näkökulmia, mikä heijastuu merkityksellisinä pidettäviin riskeihin, joita sisällytetään tarkasteluun ja seurantaan.

Käsitys julkisen hallinnon digiturvallisuuden tilasta ja tavoitteista perustuu sekä prosessissa tuotettuun tietoon että muissa lähteissä tuotettaviin asiakirjoihin. 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.

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

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

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

3.2.2 Toimintaympäristöt, joiden sisällä tarkastelu tehdään

Tässä mallissa riskienhallinnalle määritettävä toimintaympäristö koostuu useista risteävistä alueista, joista 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. Nämä digin rajat ylittävät vaikutukset voivat olla negatiivisia (esimerkiksi kaapeleiden katkeaminen, osaajien puute, hyökkäykset) tai asioita, joiden estyminen olisi negatiivinen (esimerkiksi energia, komponentit, palvelut). On myös huomattava, että digitaalinen toimintaympäristö on jatkuvasti kehityksessä ja uudelleenmäärityksessä, , koska se on vuorovaikutuksessa monien muiden toiminta-alueiden kanssa. Tämä muokkaa ja luo uusia uhkia ja mahdollisuuksia, joista voi muodostua riskejä.

Fyysisen ympäristön tarkastelussa olemme sidottuja 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 kansainväliset toimijat, kuten EU.

Abstraktimmassa tarkastelussa, kehityskulkuja laajassa sosio-teknisessä todellisuudessa kuvataan käsitteellä VUCA (volatility, uncertainty, complexity, ambiguity)[19]. 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 siis ole todennäköisiä strategisella tasolla.

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

3.2.3 Strategisen määrittely tässä mallissa

Strategialle ei ole olemassa yhtä selkeää määritelmää, eikä tämä malli määrittele absoluuttista ja pysyvää ”strategisen” merkitystä, mikä olisi ongelmallinen muuttuvassa toimintaympäristössä ja vanhentuessaan nopeasti tekisi siihen liittyvästä riskien seurannasta merkityksetöntä. Riskienhallinta on aina kontekstisidonnaista, eikä siksikään ole mielekästä pyrkiä määrittelemään yhtä merkitystä. Mallin tarkoituksena on

[19] VUCA:n jälkeen on keskusteluun tullut myös akronyymi BANI (Brittle, Anxious, Non-linear, Incomprehensible) ja pääosin USA:ssa RUST (Rapid, Unpredictable, Paradoxical, Tangled). Nämä ovat ajatustyökaluja hahmottamaan laajempia toimintaympäristöjä. BANI:n voidaan katsoa olevan jatkoa tai täydennys VUCA-ajattelulle, jolloin huomioidaan enemmän ihmisen konteksti. Digiturvallisuus on yksi näkökulma, jonka kautta voidaan pyrkiä hallitsemaan ja minimoimaan näitä aspekteja, tuottaen luottamusta järjestelmien, viranomaisten ja koko yhteiskunnan kykyyn käsitellä näitä haasteita.

tunnistaa keskeisimmät riskit, joilla on yhteiskunnallista vaikutusta. Näin tuotetaan vaihtoehtoja päätöksentekoon ja hallintatoimien kohdistamiseen digiturvan alueella. Laajempi ja hallinnonalakohtainen strateginen riskienhallinta toteutetaan nykyisellään osana toiminnanohjausjärjestelyitä. Tulevaisuudessa valtioneuvosto-tasoinen[20] riskienhallinta tarkastelee näitä julkishallintoa laajemmissa ja valtionjohdon omasta kontekstista.

Strategisten riskien tarkastelu, vaikka käsitetään ylätasolla laajaksi, ei voida olettaa olevan täysin kaiken kattavaa rajallisten resurssien ja kapasiteetin johdosta, vaan tarkastelun on oltava tietyin rajauksin kohdennettua. Tarkastelijalla on aina oma kontekstinsa, josta tarkastelua tehdään. Osallistuvan organisaation näkökulmasta on erityisesti huomioitava, että sen oma konteksti sisältää aina erilaisia ja nimen omaisesti sille ominaisia riskejä, joita ei voida eikä ole tarpeen, sisällyttää yleiseen julkisen hallinnon läpäisevään tarkasteluun sellaisenaan. Julkisen hallinnon kokonaisuuden tasolla strategisen kontekstin määrittely on vielä haasteellisempaa, sillä sen tulisi edustaa usean toimijan yhteistä diskurssia. Toisten tarpeet voivat olla hyvinkin konkreettisia, mutta samalla niihin liittyy usein hyvin abstrakteja pyrkimyksiä, kuten luottamuksen parantaminen, turvallisuuden tunne tai resilienssi. Kohdistus ei myöskään rajaa tarkasteltavia asioita vain kriittisinä tai keskeisinä pidettyihin asioihin tai kriisiaikoihin vaan nimenomaisesti laajentaa tarkastelua arkisempiinkin aspekteihin, joihin myös liittyy digiturvallisuus. Strategisen käsittelyn on siksi oltava eri rajausten sisälläkin kattavaa.

Strateginen on myös suhteellinen käsite toiminnassa ja sitä on verrattava tavoitteisiin. Tämäkin on kuitenkin ymmärrettävä riittävän laajasti, sillä kaikissa tapauksissa suora yhteys digiriskeihin ei ole selkeä organisaation keskeisitä toiminnoista ja palveluista tai niihin liittyvistä pyrkimyksistä. Riippuen organisaation koosta ja hallinnan rakenteista, sen strategiset tavoitteet voivat olla yksistään osa kirjattua kokonaisstrategiaa, tai niistä voi olla johdettuna muita strategisia suunnitelmia, kuten mahdollisia digitaalisen turvallisuuden tai jopa sen osien strategioita (joita ei edellytetä). Strategisten linjausten ja tavoitteiden kirjaamisen taso ja tarkkuus vaihtelevat monestakin syystä, eivätkä kaikki strategiset tiedot ole julkisia.

Mallin käytännön toteutukseen liittyen, strateginen riski ei ole selkeästi määriteltävissä, eikä tarkkarajainen määrittely tue mallissa toteutettavaa riskienhallintaa. Sen määritelmä on enemmän sekä toiminnallinen että dynaaminen, jotta se soveltuu hyvin moninaisten ilmiöiden ja toimijoiden käyttöön. Strategisella viitataan mallissa suhteelliseen rakenteeseen, jossa se on ylemmällä tasolla, kun keskivaiheilla ovat organisaatioiden sisäiset toimenpiteet ja toisessa päässä toiminnallisemmat asiat. Strateginen ei siis sinänsä ota kantaa arvoon, kokoon tai tärkeyteen, vaikka nämä määreet seuraavat usein mukana, kun tarkastellaan vaikutuksia organisaatiota laajempiin kokonaisuuksiin, kuten vaikutuksia julkisen hallinnon toimintakykyyn, toimijoiden järjestelmiin, asiakaskuntaan tai laajemmin yhteiskunnan voimavaroihin. Tällaisessa tarkastelussa yksittäiselle organisaatiolle toiminnallisen tasoinen ongelma voidaan tunnistaa strategiseksi julkisessa hallinnossa, mikäli se toistuu useassa paikassa. Toisaalta, jokin organisaation strateginen riski voi olla ainutlaatuinen mutta toteutuessaan se voi vaikuttaa moneen muuhun verkostojen välityksellä. Tästä johtuen

[20] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163184/VM_2021_28.pdf

määritelmän on oltava väljä, jotta merkitykselliset ilmiöt voidaan tunnistaa. Käytännön tason strategisen riskin hahmottamisessa on viime kädessä luotettava prosessiin osallistuvien asiantuntijoiden näkemykseen sekä pyrittävä rakentamaan prosessi sellaiseksi, että ymmärrys ja tiedon laatu kehittyvät tukemaan kulloisenakin aikana tarvittua strategisten riskien ennakointia.

3.2.4 Aikaikkuna

Riskienhallinnan strategisessa tarkastelussa on määriteltävä aikaikkuna, jossa tarkastelua tehdään. Perinteisen ajattelutavan mukaan, strateginen näkymä on noin 2-5 vuotta eteenpäin, mutta tämä aika määrittyy usean tekijän mukaan. Nopeidenkin päätösten vaikutukset voivat olla kauaskantoisia ja niiden erottaminen muista tapahtumista voi kestää tuon aikaikkunan tai pidemmällekin. Asioiden kehittyminen merkittäviksi voi viedä aikaa, mutta digiaikakaudella ne voivat skaalautua yllättävän nopeasti. Aikaikkuna asettuu, määrittelystä riippuen, niin sanotulle keskipitkälle tähtäimelle.

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

Aikaikkunan minimin määrää 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 tulisi tulla niin ajoissa, että tarvittavat toimet ehditään tehdä. 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 tietylle aikajaksolle. Prosessin kaikkien osien läpimenon syklin kestosta tuleva viive määrittelee lyhimmän mahdollisen ajan, jolla malli voituottaa riskienhallintaan tukea. Se on riippuvainen erilaisista taustajärjestelmistä, mutta myös tarvitusta arvioinnin ja analysoinnin laajuudesta ja syvyydestä. Prosessi on lisäksi sidottu hallinnolliseen vuosikelloon, mikä tahdistaa sen toimintaa muiden prosessien kanssa, pyrkien tuottamaan tietoa oikea-aikaisesti.

3.2.5 Tiedon laatu ja käytännön toteutuksen vaikutukset

Tiedon laatu vaihtelee organisaatioiden osaamisen ja sitoutumisen mukaan, mutta tämän odotetaan paranevan ajan kuluessa. Jo pilottien perusteella on tunnistettu viitteitä siitä, että riskienhallintaan liittyy myös osaamisen kehittämisen tarpeita, joista yksi osa on kokemuksen myötä kertyvä ymmärrys. Mikäli tiedonkeruu samankaltaisten yksiköiden sisällä pysyy vuosittain pääosin yhteismitallisena, muutosten seurannan vertailukelpoisuuden tulisi pysyä hyvänä. Tämä tukee erilaisten tapahtumien muokkaaman toimintaympäristön muutosten merkityksen seurantaa, jota riskienhallinta osin on.

Vastaajamäärän suuruus parantaa tilastollista laatua, joten osallistujien aktiivisuus on tämän vuoksi tärkeää. Vastausten kerääminen pyritään sovittamaan painotetusti vuotuisiin JTS- ja TAE-sykleihin[21], jolloin tuotettu tieto tukee organisaatioiden toiminnan suunnittelua. Käytännön järjestelmätasolla voidaan mahdollistaa tiedon kerääminen, päivittäminen ja omien vertailutietojen tarkastelu ympäri vuoden. Aktiivisuuden ja osallistumismahdollisuuden ei siis tarvitse olla sidottu tiettyyn hetkeen, mutta suuret poikkeamat siinä voivat osaltaan heikentää tietojen yhteismitallisuutta.

Vastaajilla on osallistuvien organisaatioiden tueksi tämänhetkisessä teknisessä toteutuksessa mahdollisuus lisätä vastauksien oheen omia muistiinpanoja, jotka näkyvät vain organisaation omille käyttäjille. Tämän, sekä aiempien kyselyiden tarkastelumahdollisuuden, pitäisi helpottaa tasalaatuisemman näkemyksen kehittymistä. Muita prosessin muiden osien laadunvarmistukseen liittyviä toimenpiteitä ovat mm. useiden riskitietolähteiden käyttö (aineiston riittävä laajuus), muiden asiantuntijoiden käyttö eri vaiheissa (analyysin ja arvioiden kattavuus) sekä käyttäjäpalautteen kerääminen eri muodoissa (prosessin sekä tuotosten arviointi ja kehitystarpeet). Näidenkin osalta tarkka toteutus, joka on tasapainossa tehokkuuden ja resurssien kanssa, kehittyy yhdessä käytännön toteutuksen kanssa.

Vastaajien taustatietojen avulla voidaan huomioida vertailuissa esimerkiksi eri kokoisten toimijoiden painotukset. Tämä mahdollistaa erityyppisten toimijoiden muodostamien ryhmien ja näihin kohdistuvien riskien paremman tunnistamisen. Esimerkiksi vuoden 2021 pilotin raportoinnissa tarkasteltiin erikokoisia kuntavastaajia ja näiden eroja samoja riskejä kohdattaessa.

Digiriskit tulisi pyrkiä arvioimaan toiminnalle ja ydintoimintojen toteuttamiselle. Siinä tulisi mahdollisuuksien mukaan huomioida riskit asiakkaille, alihankkijoille ja muille sidosryhmille, jos ne voivat säteillä näihin verkostojen kautta. Haasteellista on tunnistaa digitoimintojen rooli kaikissa vaiheissa tai digiturvan toteuttamiseen vaikuttavat asiat. Yhteisen näkemyksen muodostaminen on tunnistettu haaste ja sitä tullaan kehittämään tulevien vuosien aikana. Kyse on jatkuvasti kehittyvästä jaetun ymmärryksen muodostamisesta (diskurssista), johon vaikuttavat erityisesti johtavien tahojen esittämät näkemykset ja viestintä. Jo riskienhallintaan osallistumisen voidaan olettaa kehittävän asiantuntemusta, mikä parantaa laatua vuosien myötä.

[21] Katso: riskienhallinnan vuosisuunnittelu ja vuosikello, tämän asiakirjan osa 2.2

3.2.6 Tiedon turvallisuus

Turvallisuuteen liittyvien asioiden käsittelyssä tiedon turvallisuus on ensiarvoisen tärkeää. Tähänkin tulee soveltaa riskienhallintaa ja siksi on avattava mallilla käsiteltävän tiedon luonnetta suhteessa vaatimuksiin. Erityisesti jaettavan tiedon osalta on huomioitava käytettävä konteksti, eli digitaalinen turvallisuus strategisella tasolla julkisessa hallinnossa. Vaikka tähän voidaan sisällyttää myös laajempia ja sensitiivisempiä turvallisuusnäkymiä, ero niihin tulee käytännön toteutuksessa ja prosessille halutuista tietotarpeista. Eri digiturvallisuuden näkökulmilla on luonnollisesti päällekkäisyyttä, sillä digiturvassakaan ei ole vain yhtä turvallisuuden tai turvallisuustiedon kokonaisuutta – esimerkkinä vaikka tietoturvallisuus ja tietosuoja, joissa voidaan tarkastella samaa asiaa eri lähtökohdista. Laajasta digitaalisen turvallisuuden tarkastelusta voi olla johdettavissa huomioita sekä rajatumpiin digitoimintaympäristön turvallisuuden tarkasteluihin, että laajempiin kokonaisuuksiin.

Prosessimalli sinänsä ei ota kantaa siihen, miten syvällisesti joitain turvallisuuden alueita tarkastellaan, vaan tarpeiden lisäksi tätä ohjaa laki ja käytäntö. Käytännön tiedonkeruuta ohjaavat tietotarpeet ovat toisenlaisia kuin miten ne käsitetään esimerkiksi "kansallisen turvallisuuden" tai "kyberturvallisuuden" konteksteissa, mikä osaltaan muuttaa tiedon sisältöä. Kertyvä tieto on joka tapauksessa arvioitava ja pystyttävä suojaamaan vaaditulla tavalla (erityisesti Tiedonhallintalain 18 §:n 1 momentti ja Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 3 §)[22]. Tämän lisäksi riskienhallintanäkökulmasta on huomioitava niin kohtuuttoman riskin luominen keräämällä tarpeeseen nähden tarpeettoman sensitiivistä ja yksityiskohtaista tietoa, kuin myös muodostuvan riskin hallintaan tarvittavien toimenpiteiden kustannukset ja käsittelyn vaativuus. On myös muistettava, että tiedon keruuseen voi liittyä useita tapoja ja järjestelmiä, mukaan lukien viranomaisten tiedonvaihto eri tasoilla sekä avoimet lähteet.

Näitä rajoja vasten voidaan arvioida yhteen kootun tiedon muodostuvan korkeintaan "luottamukselliseksi" pidemmälläkään aikavälillä, ilman että se haittaisi prosessin tarkoitusta. Tällä hetkellä prosessimallia tukevien järjestelmien ja järjestelyiden mukaisesti tiedon luonteeksi saa muodostua korkeintaan käytöltään rajoitetun tasoiseksi (turvallisuusluokka neljä, TL IV)[23], mikä on soveliasta huomioiden viranomaisten välisen tiedonvaihdon. Käytännössä kerättävän tiedon luokitteluna on kuitenkin ”salassa pidettävä”, perustuen muun muassa pilotoinneissa saatuihin kokemuksiin. Erikseen on huomautettava, että yksittäinen tieto voi olla osallistuvan organisaation julkiseksi luokittelemaa, mutta koostettujen raporttien ja muiden tietotuotteiden luokittelu voi olla korkeampi tai matalampi sisällön mukaan, jolloin jatkokäsitellylle tiedolle on sovellettava asianmukaisia vaatimuksia.

Riskitiedon tallentamiseen liittyvät turvallisuus- ja luottamuskysymykset selvenevät käyttäjille prosessin käytännön toteutuksen myötä, mikä on oma kokonaisuutensa. Prosessia tukevaa tiedon keräämistä on tehty jo vuosina 2020 ja 2021 VM:n sekä Digi- ja väestötietoviraston toimesta, mistä saadut opit on sulautettu uuteen kokonaisuuteen. Koska runkona käytetyssä kyselyssä on strateginen kohdennus ja siinä

[22] Lisätietoja: Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta

[23] Lisätietoja: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

tiedustellaan arvioita suhteellisesta merkityksestä, järjestelmään kerääntyy vain tilastollisesti käytettävää tietoa. Kysymyksissä ei esimerkiksi tiedustella tietoja tietojärjestelmien yksityiskohdista. Tämä ei olisi tarkoituksenmukaistakaan tavoitellun merkityksen näkökulmasta, sillä osa-alueiden toteutukset erilaisissa organisaatioissa vaihtelevat suuresti. Tiedon kokoamisessa on siis huomioitu vähäriskisyys suunnittelussa (security by design -ajattelu) sekä haettu tasapainoa tarvitun tiedon muodossa ja määrän minimoimisessa suhteessa käyttötarpeisiin. Yleistäen voitaisiin todeta, että mahdollisten hyökkääjien lisäksi myös julkishallinnon tulee kyetä kokoamaan riittävät tiedot omasta tilanteestaan digiturvallisuuden toimenpiteiden kohdistamiseksi.

Prosessimallista erillistä käytännön tiedon keräystä ja hallintaa varten käytettävien järjestelmien vaatimukset ja toteutukset ovat kehittyneet pilottivaiheiden aikana. Suomi.fi palveluhallinnassa muun muassa käytetään vahvaa tunnistautumista ja organisaatioilla on oman pääkäyttäjänsä kautta kontrolli siihen, keillä on valtuudet käsitellä tietoja. Lisäksi kyselyissä on mahdollisuus tiedon luokittelutason määrittelyyn. Tiedot on tallennettu DVV:n suojattuun ympäristöön. Palvelu toteuttaa lisäksi kaksikielisyyden ja saavutettavuuden vaatimukset.

3.2.7 Suhde organisaatioiden omaan riskienhallintaan

Koska strateginen näkymä riskeihin on kontekstisidonnaista, on hyvä muistuttaa, että jokaisen organisaation omat digiturvan riskit on otettava osaksi organisaation kokonaisriskienhallintaa. Kolmen puolustuslinjan mallin mukaisesti, digiturvariskien tarkastelu on osa linjaorganisaatioissa tapahtuvaa riskien tarkastelua, osa organisaation läpäiseviä asiantuntijapalveluita (kuten tietohallinto tai turvallisuuspalvelut) sekä sisäisen tarkastuksen mahdollinen tarkastelun kohde.

Kokonaisriskienhallinnassa, kuten digiriskeissäkin, voidaan tehdä erilaisia luokitteluita riskien tyyppien ja ominaisuuksien mukaan, ja nämä auttavat hahmottamaan mistä tarkastelualue muodostuu. Painotukset digiturvan sisällä, sekä keskeisten toteutusalueiden että muiden näkökulmien suhteen, tulee perustua organisaation omaan toimintaan ja tarpeisiin. Kokonaisriskienhallinnassa tarkasteltavat riskit keskeisille tehtäville ja tavoitteille, joihin liittyy digitaalinen ulottuvuus, tulisi olla johdettavissa digiturvallisuuden riskeihin. Yhteys ei välttämättä ole suora vaan välillinen vaikutussuhde tai liitos. Digiriskit eivät siis siten ole erillisiä vaan osa riskienhallinnan kokonaisuutta.

Kokonaisriskienhallinnan näkökulmasta - tehdään sitä organisaation kontekstissa tai yhteiskunnan eri osien tai valtionhallinnon osa-alueilla - erilaisten siiloutuneet rakennelmat lävistävien aiheenmukaisten riskitarkasteluiden myötä (kuten digiturvallisuus, mutta myös esimerkiksi logistiikka, viestintä tms.) voi nousta esiin lähempää tarkastelua vaativia asioita uusista näkökulmista. Tämä on osa hyvää hallintoa ja hyödyttää yhteistyön myötä useita toimijoita - myös osallistuvien organisaatioiden ulkopuolella. Standardin mukaisen rakenteen ja vapaaehtoisen osallistumisen sekä valtion varojen käyttöön liittyvän ohjauksen vuoksi tässä asiakirjassa esitetty malli tukee VM:n controller-toiminnon ohjaamaa riskienhallintaa.

3.2.8 Suhde muihin riski- ja turvallisuusarvioihin

Digitaalisen turvallisuuden strateginen riskinarvio on poikkihallinnollinen ja digitaalisen toimintaympäristön kontekstiin[24] sidottu katselmus erilaisten ilmiöiden tilanteesta. Tämän rajatun erityisalueen tarkastelun mahdollistamiseksi kerätty tieto on käytettävissä yhtenä lähteenä tietyin varauksin myös muissa aiheeseen liittyvissä tarkasteluissa tai osa-analyysina laajemmissa tarkasteluissa. Jo pilottivaiheessa tuotettua tietoa on käytetty valtionhallinnossa osana turvallisuutta sekä digitalisaatiota tarkastelevia arvioita[25]. Se siten esimerkiksi asettuu kansallisen riskinarvion alapuolelle, mutta voi tarkastella sitä laajemmin turvallisuutta sivuavia ilmiöitä alueellaan.

On kuitenkin huomattava, että eri arvioiden kontekstit ja tarkastelun tasot voivat vaihdella[26], jolloin tieto on tarvittaessa uudelleen analysoitava ja arvioitava riittävällä tarkkuudella uutta käyttötarkoitusta varten. Tämä on osa kaikkiin tietotuotteisiin liittyviä tehtäviä.[27] Tuotaessa tietoa organisaatioiden omaan riskinarviointiprosessiin, onkin suositeltava käytettäväksi myös tärkeiksi koettujen digiturvallisuuden osa-alueiden muuta raportointia ja tietolähteitä. Laajempaa kuvaa muodostettaessa lisätietona voidaan käyttää esimerkiksi Kyberturvallisuuskeskuksen tuottamia teknisemmän tason arvioita ja tiedotteita, sillä on hyvä tietää minkälaisia käytännön ilmiöitä suuremmat aihealueet pitävät sisällään.

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.[28]

[24] Määritelmän mukaisesti digiturva liittyy asioihin, jotka tapahtuvat digitaalisessa toimintaympäristössä, mutta myös asioihin, jotka vaikuttavan sen ulkopuolelta siihen sekä sieltä sen ulkopuolelle suuntautuviin vaikutuksiin. Joissain tapauksissa digiriskeiksi luettavissa olevia asioita ei käsitellä kuitenkaan tämän näkökulman kautta, vaan jokin toinen määrittely voi olla merkitsevämpi tai erityisistä syistä valittu. Esimerkiksi tiettyjä kyberturvallisuuteen luettavissa olevia uhkia käsitellään (ulko)politiikan kontekstissa.

[25] Digitalisaation tilannekuvakokonaisuutta mallinnettiin systeemisen lähestymistavan kautta uudella tavalla. Materiaali: https://vm.fi/digitalisaation-mittarit-ja-tilannekuva

[26] Esimerkeiksi alueelliset tai kansalliset riskinarviot kohdistuvat hieman eri tavalla ja ovat suunnattuja hieman eri tarpeeseen, mutta käsittelevät myös osin samoja aiheita.

[27] Esimerkkejä tässä mallissa käsiteltävästä riskitiedosta voi katsoa vuoden 2021 pilotointiin liittyvästä avoimesta raportoinnista.

[28] Esimerkkejä tausta-aineistoista: Digihumaus-raportti (DVV), Threat Landscape (Enisa), Huoltovarmuuden skenaariot 2030 (HVK), Threat Horizon 2022 (Information Security Forum), Kansallinen riskiarvio (SM), Global Risk Report (WEF), Digikompassi (Digitoimisto), Digitalisaation tilannekuva (VM), Yhteiskunnan turvallisuusstrategia (Turvallisuuskomitea), Kyberturvallisuusstrategia (Turvallisuuskomitea)

3.2.9 Suhde standardeihin

Riskienhallintajärjestelmien prosessien luominen standardia noudattaviksi julkishallinnossa ja suurissa monimutkaisissa organisaatioissa on haasteellista. Tämä pätee erityisesti laajempien hallinnon- ja toimialat yhdistävissä järjestelyissä (esimerkiksi aihealueen ympärille, kuten digiturvallisuus tai jokin toimiala), joita luodaan tukemaan eri riskienhallintakokonaisuuksia. ISO31000:ssa kuvattuun mallirakenteeseen ei ole valmiiksi sisällytetty laajan organisaation tai sitä 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 kokoamiseksi luokitteluiksi ja tilastoiksi.

Keskeistä on huomioida, että kukin organisaatio tai sen osa toteuttaa riskienhallintaa sekä tunnistaa ja arvioi riskejä ensisijaisesti omasta näkökulmastaan, vaikka pyrkisikin huomioimaan muita. Näkökulmat eivät useinkaan ole sellaisenaan kaikilta osin 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 ja vastaanottavassa päässä, mutta arviointi 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 edellyttää standardin noudattamista. Koska ISO27000-sarjassa käytetty riskienhallintaprosessi perustuu ISO31000:een, löytyy tarvittaessa rajapinta ja mahdollisuus kytkeä prosessi 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 riskienhallintaan[29] ohjeita sekä riskienhallintapolitiikkamallin. Malli sisältää politiikalle suositellut vähimmäisvaatimukset sekä eräitä muita mallia ohjaavia ominaisuuksia.[30] Suositukset pohjautuvat ISO 31000 -riskienhallintastandardiin.

3.3 Kustannuksista ja vaikuttavuudesta

Julkisen hallinnon strategisen riskienhallinnan vaikutukset ja vaikuttavuus ovat laajoja kokonaisuuksia. Niiden 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

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

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

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 vakituisessa tehtävässä johtavana asiantuntijana (tai vastaavana, riippuen tehtäväkokonaisuudesta), jonka päätehtävänä nämä toimet olisivat. Tämän henkilötyövuoden palkkaus sivukuluineen sekä kehittämiseen ja viestintään tarvittava alustava budjetti olisivat yhteensä noin 170000€ vuodessa, mutta luvun voidaan odottaa kasvavan kehitystoimien myötä. DVV:n kuluiksi on myös huomioitava digitaalisen turvallisuuden asiantuntijoiden sekä konsulttien hyödyntäminen. Erityisiä riskejä arvioitaessa ja niiden hallintatoimia suunniteltaessa on asiantuntijoina käytettävä myös muiden julkisen hallinnon toimijoiden asiantuntemusta, mitä ei tässä lasketa. Tämän päälle tulevat järjestelmien ylläpitokulut, jotka nivoutuvat muihin DVV:n kuluihin, mukaan lukien esimerkiksi digitaalisen turvallisuuden kokonaiskuvapalvelu, jonka tietoja hyödynnetään myös tämän mallin mukaisessa riskienhallinnassa.

Riski- ja riskienhallintatiedon tuottamiseen osallistuvien organisaatioiden arvioidaan käyttävän tähän noin 1-3 htp vuodessa. Tuottamiseen voi osallistua usea asiantuntija ja panostus on riippuvainen organisaatioiden muusta riskienhallinnan järjestämisestä. Tiedonsyöttöön käytettävän ajan voidaan olettaa laskevan selvästi ensimmäisten prosessisyklien jälkeen, sillä alussa käyttöönottokynnys voi olla suurempi. Saatujen raporttien käyttö omassa riskienhallinnassa vie käsittelytavasta riippuen saman verran aikaa, minkä päälle luonnollisesti tulevat erikseen välilliset vaikutukset mahdollisista hallintatoimista. Kokonaiskuvapalvelun kautta riskienhallinnan tiedonjakoon osallistumattomat organisaatiot tulisivat hyötymään yleisestä digitaalisen turvallisuuden riskienhallinnan raportoinnista sekä mahdollisista yleisistä digitaalisen turvallisuuden riskienhallintatoimista. Toimien kohdistus voi kuitenkin kärsiä kattavuuden puutteesta, mikäli osallistujia on vähän.

Riskienhallintaprosessissa tuotettu tieto aiheuttaa tehtäviä niille toimivaltaisille viranomaisille, joille riskienhallintatoimia ohjautuu. Koordinaatiotoimia varten on olemassa keskeisten viranomaisten muodostama digitaalisen turvallisuuden strateginen johtoryhmä, jonka toimintaan liittyvä ajankäyttö sisältyy suunniteltuihin kokouksiin. Toteuttavien viranomaisten kohdalla vaikutukset ovat tapauskohtaisia ja osa toimenpiteistä on normaalien prosessien puitteissa tehtäviä, mutta laajemmissa hankkeissa on tehtävä 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 aihealueessa korostuu turvallisuuden varmistaminen, riskienhallinnalla pyritään ennen kaikkea mahdollistamaan strategiset toiminnot ja tukemaan strategisten tavoitteiden saavuttamista sekä mahdollistamaan organisaation jokapäiväinen toiminta. Sen lisäksi, että riskien vaikutuksia voidaan vähentää ja neutraloida, strategisessa riskienhallinnassa tulee pyrkiä huomioimaan myös 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 sisältyä esimerkiksi turvallisuuteen liittyvien tai muiden toimintojen uudistaminen, joka tehostaa ja rikastaa palveluita tai mahdollistaa uusien teknologioiden tai toimintatapojen käyttöönoton ja tehostaa tiedon hyödyntämistä. Näiden etujen saavuttamisen mittaaminen, etenkin euromääräisesti, voi olla mahdotonta, mutta niiden tukemiseksi tehtävien digiturvallisuuden tehtävien arvon määrittäminen vaikuttavuuden mittarina on osa malliin sisältyviä ohjauksen ja kehittämisen tarpeita.

3.4 Riskienhallintamallin kehitys

Kattavan riskienhallintamallin rakentaminen toimivaksi järjestelmäksi, joka vastaa muotoutuvia tarpeita, on pitkällinen prosessi. Mallin kehitys alkoi vuonna 2020 toteutetulla kyselyllä, jota on kehitetty ja toistettu. Kysely ja sillä kerättävät näkemykset riskeistä ovat kuitenkin vain yksi palanen ja näkökulma. Riskienhallinnan kokonaisuudessa on useita osa-alueita, joita tulee kehittää. CMMI-mallin[31] viisiportaista edistymisen mittaria mukaillen, tämänhetkisen tilanteen voidaan arvioida täyttävän korkeintaan tason kaksi määritelmän.

Esitetty kokonaisuus on kuvaus toimintamallista ja siihen sisältyvistä prosesseista. Malli on pysyväisluonteinen, sillä digitaalinen turvallisuus tarvitsee pitkäjänteistä kehittämistä ja tukea. Siihen liittyy kuitenkin, erityisesti käytännön tasolla, kehitettäviä ja toimintaympäristöjen jatkuvan muutoksen huomioivia osia, joita ohjaavat tulevat tavoitteet sekä riskienhallintatyön ohessa selkiytyvät tarpeet. Esitetyssä mallissa on pyritty huomioimaan molemmat haasteet.

Pilotointien ja nykytilan tarkastelussa sekä käytön testauksen perusteella havaittuja kehityskohteita voisivat olla:

- Tiedonkäsittelyn järjestelmäpohjaisuus ja yhteentoimivuus eri määrittelyiden kanssa voisi tehostaa riskienhallintaa, kun tietyt osat siitä voitaisiin automatisoida ja tuotettu data ja informaatio olisivat ainakin joiltain osin yhteismitallisempia ja rakenteisia. Esimerkiksi arviointiin ja luokitteluun käytettävien asteikkojen soveltamista voitaisiin kehittää. Riskitiedon vertailtavuus ja hyödyntäminen toiminnanohjauksessa nopeutuisivat organisaatioissa. Osa organisaatioista on tässä jo pidemmällä, mutta osa toimii edelleen lähes manuaalisesti. Tason parantuminen olisi suotavaa julkisen hallinnon kokonaisuuden riskienhallinnan laadukkuuden näkökulmasta.
- Osallistuja- ja vastausmäärien kasvattaminen on tärkeää kyselyistä saatavan datan tarkkuuden parantamiseksi sekä laadun varmistamiseksi. Riittävä data tuo paitsi luotettavuutta, mutta myös riittävästi tietoa etenkin pienemmistä vertailuryhmistä. Tämä on tärkeää toimenpiteiden oikein kohdentamiseksi.
- Osallistujien datasta ja prosessin osallistumisesta saamia hyötyjä voidaan kasvattaa ajan kuluessa, kun dataa kertyy. Tällöin siitä voidaan tuottaa enemmän ja luotaavampia tietotuotteita sekä yhdistää siihen muita lähteitä. Pidempi historia myös lopulta tasoittaa eri aikapisteiden välisiä mahdollisia vinoumia. Datan

[31] Capability Maturity Model Integration

kerryttämisen tuottama arvo kasvaakin nopeammin kuin vain lineaarisena kasvuna vuosikymmenen loppua kohti.

- Kerätyn tiedon sisällön ja keräyksen kattavuuden varmistamiseksi tulee pyrkiä käyttämään useampaa lähdettä sekä ulkopuolisia arviointeja täydentämään tietoa ja analyysiä.
- Laadun varmistamiseksi analyysimetodologiassa tulisi pyrkiä monipuolisuuteen toteutettavuuden rajoissa. Toisaalta tiedon esittämisessä tietotuotteissa tulisi pyrkiä lukijaa oikealla tavalla palvelevaan tehokkuuteen ja selkeyteen. Vaikkakin ne ovatkin erillisiä kohtia prosessissa, niillä on epäsuora yhteys toisiinsa, oikean merkityksen esittäminen oikealla tavalla on tärkeää asian sisäistämiseksi ja informaatiotulvan välttämiseksi.
- Yleisempien tietotuotteiden kehittyessä ja tarkempien tietotarpeiden selkiytyessä syntynee tarve kehittää tarkempia ja erikoistuneempia tarkasteluita. Vaikka prosessin rakenteen on tarkoitus olla pysyvä, sen hyödyllisyys edellyttää jatkuvaa kehitystä uusien riskien ja kehitystarpeiden huomioimiseksi.
- Prosessiin ei alkuvaiheessa ole sisällytetty osallistuville organisaatioille erityistä mekanismia uhkatiedon jakamiselle ja tuottamiselle. Oletuksena on, että organisaatioiden normaaliin digiturvallisuustoimintaan sisältyy omaan toimintaan ja toimintaympäristöön liittyvä havainnointi ja tilanteen seuranta. Kokonaisuuden parempaa hahmottamista varten voitaisiin pyrkiä tuottamaan koottuja näkymiä uhista, joita organisaatiot sitten voisivat käyttää arvioidessaan omia riskejään, osana riskienarviointiprosessiaan.
- Vaikka uhkia voidaan tunnistaa yleisen käsityksen tai asiantuntijanäkemyksen perusteella, riskejä tulisi arvioida asetettuihin tavoitteisiin nähden. Digitaalisen turvallisuuden tulee tukea erilaisissa strategioissa, päätöksissä ja suunnitelmissa asetettuja tavoitteita, jotka voivat olla yleisempiä tai digitaaliseen toimintaympäristöön kohdistuvia. Arvioinnin järjestelmällisempää toteuttamista käytännössä, mahdollisesti osin ristiriitaistenkin tavoitteiden osalta, tulisi työstää sekä prosessissa että mahdollisuuksien mukaan myös sen ulkopuolella strategisessa tavoitteidenasetannassa.
- Riskienhallinnassa tulisi tarkastella ennakointityössä tuotettavien näkymien ja muutospolkujen hyödyntämistä pitkän tähtäimen toivottujen kehityssuuntien tukemiseksi.

Strategisen tiedonhallinnan prosessin kehityskohteita voisivat olla:

- Riskienhallinnan ohjaamista ja tukemista palvelevan tehtävänannon (”tietopyyntö”) kehitys, eli miten muotoillaan oikeat kysymykset, jotta voidaan tuottaa tarvitut vastaukset.
- Tiedonkeräyksen laajentaminen ja syventäminen, kattavuuden varmistaminen eri osioissa, vertailutiedon kehittäminen ja rikastaminen sekä ulkoiset tietolähteet.
- Tiedon käsittelyn kehitys; tehostaminen, yhtenevien käsittelytapojen kehitys, luokittelut sekä oppivien järjestelmien hyödyntäminen esimerkiksi tunnistamisessa sekä muutosten ennakoinnissa.
- Analysoinnin ja raportoinnin kehitykseen liittyviä seikkoja 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. Vaihtoehtojen määrästä johtuen, näiden toteuttamista on priorisoitava.

3.4.1 Ensimmäinen kehitysvaihe

Ensimmäisen kehitysvaiheen tehtävät keskittyivät tiedon keräykseen, vaikka jo toisessa pilotoinnissa 2021 kehitettiin tietopyyntöön liittyviä tarkennuksia kyselyn suuntaamiseksi. Tiedon keräyksen tehostamiseksi, turvaamiseksi ja yhdenmukaistamiseksi on otettu käyttöön tietojärjestelmä, jossa tuotetaan digitaalisen turvallisuuden kokonaiskuvaan liittyviä tietotuotteita, hyväksikäyttäen samoja organisaatioiden taustatietoja. Järjestelmän käyttöön siirtyminen tarkoittaa tietotuotteen sisällön kannalta taustoittavan digitaalisen turvallisuuden tiedon hyväksikäytön mahdollisuutta. Sen avulla luodaan kuvaa riskienhallinnan tilanteesta, jota voidaan suhteuttaa riskeihin, mutta myös suhteuttaa eri toimijoiden ja luotujen vertaisryhmien kanssa. Lisäksi pystytään tarjoamaan ajantasaista ja päivittyvää tietoa automaattisella raportoinnilla. Aluksi raportointi tulee olemaan perusmuotoista, mutta datan määrän kertyessä sitä voidaan kehittää. Toistettavuus ja kertyvän datan vertailumahdollisuus aikasarjoina mahdollistaa erilaisten kyselyiden toteuttamisen. Niistä saadaan vuosien aikana tietoa muutoksista, mikä avaa indikoivia näkyviä tulevaisuuden trendeistä.

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

3.4.2 Toisen kehitysvaiheen hahmotelma

Toisessa vaiheessa tulisi keskittyä parantamaan aiempia kyvykkyyksiä, jotta niistä saatava hyöty saadaan ”kasvamaan korkoa” aikaisessa vaiheessa. Muutosten mielekkääseen ja uskottavaan seuraamiseen tarvitaan toistoja noin 3-5 vuoden ajalta. Tämä laskenta voidaan tosin aloittaa vasta riittävän osallistujajoukon liityttyä prosessiin.

Olemassa olevaa riskinäkemyskyselyä tulisi täydentää sekä lisätä muita metodeja ja näkökulmia käyttäviä kyselyitä, jotka voivat vastata toisenlaisiin riskeihin ja riskienhallintaan liittyviin tarpeisiin. Näitä metodeja 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). Lisäksi tuotettujen tietotuotteiden, kuten raporttien, kehitystä tulisi jatkaa. Kokonaisprosessin toimivuus tulisi varmistaa ja muuttaa pysyväisluonteiseksi, mikä on käytännössä edellytys edellä esitetylle laadun kehittymiselle.

3.4.3 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 muun yleisen digitalisaation kehitysnäkymien kanssa. Sovittamiseen liittyy myös valtioneuvostotasoisen riskienhallinnan kehittäminen, joka kokoaa yhteen vertikaalisten siiloutuneiden hallinnonalojen riskienhallinnan tietoja. Tässä kuvattu prosessi luonnollisestikin on poikkihallinnollinen otos tietystä aihepiiristä.

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

Tulevaisuuden muutosten luodessa uudenlaisia riskejä, mutta myös muokatessa toimintaympäristöä 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, ja arvioida vastaako se tarkoitustaan ja tuottaako se tarvittua tietoa tehokkaasti. Inkrementaalisten tarkasteluiden lisäksi tulisi säännöllisesti pitää erityisiä strategisen riskienhallinnan kehitystä, laatua ja tulevaisuuden muutoksia tarkastelevia tapahtumia.