Valtiovarainministeriön
Digi- ja väestötietovirasto

Lausuntopyyntö: Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta DL 29.4

## Lausuntopyynnön kommentit/DVV/3687/2022

Kiitos kommentipyynnöstä.

## Onko malli selkeä ja uskottava?

Esitetty malli on pääosin selkeä. Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallintamalli tulee yhdistämään yhteistä tavoitetta ja luo hyvän tilannekuvan, erilaisten hyväksyttyjen toimintamallien COSO ERM, ISO 31000, ISO 27005, ISACA toiminnan tukemiseksi organisaatiotasolla.

Riskienhallinnan vuosikello on esitetty selkeästi. Vuosikellossa on tunnistettu hyvin keskeiset hallinnon vuosikellon aikataulut. Vuosikellon osalta tulee kuitenkin huomioida kasaantuvat raportointi ja valmisteluvelvoitteet. Toimenpide-ehdotusten käsittelyyn ja valmisteluun tulee varata riittävästi aikaa osana eri toimijoiden suunnitteluprosesseja. Tämä voi edellyttää vuosikellon tiivistämistä.

Vuosikellossa on painotettu valtionhallinnon budjetoinnin vuosikelloa. Kuntien ja hyvinvointialueiden päätöksenteon vuosikello voi poiketa valtionhallinnon vuosikellosta. Koska tavoitteena on tukea koko julkista hallintoa, tulee muiden kuin ministeriöiden ja virastojen vuosikellot huomioida.

Yleiskäyttöiset ja toistuvaan käyttöön eri käyttäjille tarkoitetut osiot olisi hyvä pyrkiä erottamaan taustoitus- ja historiaosioista. Raportti sisältää oletuksia esim. organisaatioiden työmäärästä jota tarvitaan esitettyjen mallien käyttämiseen tai toimintatapojen soveltamiseen. Koska kohdealueena ovat hyvin erityyppiset ja erikokoiset julkisen hallinnon organisaatiot, herää kysymys onko malli sovellettavissa eri laajuudessa tai eri tasoilla erilaisissa organisaatioissa - esimerkiksi pienillekin kunnille jää sote-palvelujen hyvinvointialueille siirtymisen jälkeenkin monia tehtäviä kuten ympäristöterveydenhuolto. Lisäksi joillakin toimialoilla kuten sosiaali- ja terveyspalveluissa osana julkisten palvelujen tuotantoa toimii merkittävästi yksityisiä toimijoita, ja tämä näkökulma olisi hyvä huomioida. Esimerkiksi kuinka esitetyt seikat tulisi huomioida sote-sektorin palvelujen tuottamiseen liittyvissä yhteistyösopimuksissa tai valtakunnallisessa viranomaisohjauksessa, jonka kohteena ovat eri rooleissa toimivat yksityiset yritykset, kuten ostopalveluja tuottava yksityiset sote-organisaatiot tai sote-tietojärjestelmäpalvelujen tuottajat. Materiaali vaikuttaa osin projektiraportoinnilta tai virastokohtaiselta suunnitelmalta (esim. luku 3.4, jossa jopa yksittäisen työntekijän palkka-arvio tai henkilötyömääräarviot joissa ei ole huomioitu erityyppisiä ja -kokoisia organisaatioita), osin yleiskäyttöisiä malleja ja jäsennyksiä sisältävältä uudelleenkäytettävältä materiaalilta.

On hyvä, että riskienhallintamallin kehityksessä on tehty vaiheittaista suunnittelua ja tunnistettu tarkemmin ensimmäisen ja toisen vaiheen tavoitteita ja toimenpiteitä.

## Tuottaako se oikeaa informaatiota?

Luonnoksessa on hyvin tunnistettu aikaisempina vuosina toteutettujen pilottien kehityskohteita. Pilotissa käytetyt väittämät vastaavat pitkälti digitaalisen turvallisuuden parissa työskentelevien arkikokemusta sekä kansainvälisiä selvityksiä. Tällä toimintatavalla riskianalyysi ei itsessään tuota uutta tietoa nousevista riskeistä. Riskianalyysi kuitenkin kertoo miten eri toimijoiden ja sektoreiden välillä riskit painottuvat suhteessa aikaan ja toimintaympäristön muutokseen.

Mikäli riskianalyysi toteutetaan pilottikyselyitä vastaavalla tasolla, kerättävän tiedon määrä voi olla jopa suppeampi.

Digitaalisen turvallisuuden strategisen riskianalyysi tulee olla sovitettuna yhteen ennakointi- ja tulevaisuustyön kanssa. Tämä on tunnistettu luonnoksessa hyvin, mutta vasta kolmannen kehitysvaiheen osana. Digitaalinen turvallisuus on edellytys toiminnan turvaamiseksi ja uusien mahdollisuuksien hyödyntämiselle. Toimintaympäristön havaitut ja toivotut muutokset tulee ohjata digitaalisen turvallisuuden riskianalyysiä ja sen painopisteitä.

Luonnoksessa on tunnistettu, että vastaajajoukko on valikoitunut. Riskianalyysin osalta voi olla tärkeä nähdä eroja sen suhteen, miten digitaalisen turvallisuuden asiantuntijat ja muu organisaatio kokee digitaalisen turvallisuuden tilanteen. Vastaajien rooli vaikuttaa siihen, mitkä digitaalisen turvallisuuden osa-alueet ja riskit korostuvat todennäköisyyden ja erityisesti merkityksen näkökulmasta.

Ehdotamme, että julkisen hallinnon digitaalisen turvallisuuden strategisessa riskienhallintamallissa jäännösriskien käsittelylle luodaan myös prosessimalli edistämään hyvää riskienhallintaa. Tavoitteena on, että organisaatiot ovat tietoisia minkälaista riskikuormaa kannetaan kulloisenkin tilanteen aikana. Jäännösriskien pitäminen kunkin organisaation omalla vastuulla on tietoinen valinta, mihin on sidottu omia taloudellisia ja toiminallisia resursseja. Organisaation omalla vastuulla olevat jäännösriskit ilmenevät usein vuositasoilla toistuvina riskeinä, joihin myös tulee varautua.  Riskien toteutuessa vahingon sietokyky tulee olla varmistettu ja mahdollisien vahinkojen seuraukset tulee organisaation kantaa itse.

## Kattaako malli riittävästi asiantuntija ja johtoryhmätasolle tarvittavia näkökulmia julkisen hallinnon digitaalisen turvallisuuden strategisen riskienhallinnan hahmottamiseksi?

Malli nostaa johdon tasolle hyödynnettävää paikallista vertailutietoa, josta tehty analyysi voi tukea tilannekuvan parempaa hahmotusta sekä päätöksentekoa. Mallin kuvauksesta ei voi päätellä, missä määrin se tuottaa sellaista tietoa, joka ohjaa digitaalisen turvallisuuden kehittämiseen kohdennettujen resurssien määrittelyä ja suuntaamista tehokkaammin.

Tältä osin malli vaikuttaa kohdistuvan erityisesti digitaalisen turvallisuuden asiantuntijoiden välisen vertaiskehittämisen tueksi.

Hallintotoimien sekä toimenpidesuositusten osalta tulee huomioida laajasti niiden vaikutukset. Hyvällä julkisen hallinnon tason riskienhallinnalla voidaan varmistaa, että julkiset organisaatiot voivat hyödyntää teknologian ja yhteistyön tuomia mahdollisuuksia vastuullisesti. Riskien minimointi itsessään ei riitä, mikäli tämä johtaa toiminnan kannalta osaoptimointiin ja toiminnan kustannusvaikuttavuuden heikentymiseen.

Luvussa 2.3.1 esitettyjen johtoryhmien työnjaon suhteen voisi edelleen tarkentaa sitä, mikä on DTS-joryn ja Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän sekä riskienhallinnan kehittämisen työryhmän (VAHTI) työnjako ja keskinäinen työnjako. Mikäli ryhmien ero on ensisijaisesti strateginen - operatiivinen -akselilla, tätä voisi olla tarpeen selkeyttää. Molemmissa näkyy yhteistyörakenteita sekä valmistelu- ja koordinaatiotehtäviä, joiden erot ja tarkemmat vastuut eivät täysin dokumentista avaudu. Kytkennät operatiiviseen kehittämiseen ja toimivaltaisten viranomaisten omaan toimintaan olisi hyvä pyrkiä edelleen konkretisoimaan. Riskienhallintaa tukevat kehittämishankkeet ja hallintatoimet eivät perustu pelkästään kokonaiskuvajärjestelmän tietoihin tai raportteihin vaan erityisesti toimijoiden omiin analyyseihin riskiympäristöstään, ja kaikki niistä eivät välttämättä välity koko julkishallintoa koskevaan yleiskuvaan.

Johtoryhmä- ja asiantuntijatasolla olisi tärkeää pystyä huomioimaan esitetyn mallin suhde kansainvälisiin ja suomalaisiin säädöksiin ja niiden kautta tapahtuvaan ohjaukseen. Esimerkiksi tuottaako malli syötettä tuleviin säädösvalmisteluihin, mitä säädösten mukaisia velvoitteita malli auttaa täyttämään ja mitkä ovat käytännössä ne säädökset, joihin malli linkittyy. Riskienhallintalähtöisyys on materiaalissa mainitun tiedonhallintalain lisäksi keskeinen mm. tietosuojaa ohjaavissa säädöksissä sekä sosiaali- ja terveydenhuollon julkisia palveluja osaltaan ohjaavassa kansallisessa erityislainsäädännössä (mm. asiakastietolaki 784/2021) sekä lääkinnällisten laitteiden säädöksissä.

Ehdotamme, että julkisen hallinnon digitaalisen turvallisuuden strategia riskienhallintamalliin huomioidaan skenaariotyö. Riittävällä ja laajalla riskienhallintatyöllä saadaan käsitys kulloisenkin ajankohdan kokonaiskuvasta, joka on avain myös mahdollisiin skenaarioihin. Riskienhallinnalla voidaan muodostaa omasta organisaatiosta kokonaistilannekuva eri toiminta-alueiden suhteista (esim. ICT-laitehankinnat ja yhteistyökumppanit) ja mahdollisista toteutumistodennäköisyyksistä. Tämä kokonaistilannekuva muodostaa skenaariotyölle pohjan uhkien, riskien ja tunnistettujen verkostojen avulla. Skenaariotyö on helpompaa riskienkokonaiskuvan avulla, varsinkin kun laajeneva toimintakenttä ja sidonnaisuudet ovat verkostomaailmassa jatkuvassa muutoksessa.

## Vastaako kehitettävä kokonaisuus organisaatioiden tai päätöksentekijöiden tarpeita?

Luonnoksen ja pilottikyselyiden perusteella malli tuottaa ensisijaisesti paikallista vertailutietoa. Yksittäisen organisaation kannalta tieto on hyödyllistä taustatietoa, joka vahvistaa niitä signaaleja, joita jo nykyisistä digitaalisen turvallisuuden ja kyberturvallisuuden raporteista saadaan. Luonnoksesta ei käy ilmi, mitä uuttaa tietoa tai yksittäisen organisaation päätöksenteon kannalta konkretisoivia toimenpidesuosituksia se tuottaa.

## Muut kommentit ja kehittämisehdotukset.

Dokumentin sisäistä jäsentelyä ja painotuksia voisi vielä tarkentaa, jotta riskienhallintamalliin liittyvät asiat tulisivat selkeämmin ja kattavammin esille verrattuna taustaoletusosioon. Luonnos sisältää nykyversiossa taustoitusta, yleiskatsauksen, prosessikuvaksen, kustannus- ja työmääräarvioita ja osin yksityiskohtaisia huomioita ja

havaintoja ml. eri pilottien kehitysehdotuksia. Samoin yleiseen luettavuuteen ja tekstin sujuvuuteen voisi kiinnittää huomiota dokumentin valmiiksi viimeistelyssä.

Viimeistellyssä versiossa tulisi voimakkaammin keskittyä mallin kuvaukseen ja erottaa selkeästi taustoitus omaksi kappaleekseen ja projektiraporttimainen sisältö esimerkiksi omaksi liitteekseen. Pilottikyselyissä käytettyjä sisältöä tulisi nostaa myös osaksi kuvausta, mikä auttaisi hahmottamaan konkreettisemmin.

On hyvä, että mallissa nojaudutaan yleisiin standardeihin ja yleisesti käytettyihin viitekehyksiin, kuten ISO 31000, ISO 27000-sarja sekä CMMI.

Digitaalinen turvallisuus on osa kokonaisturvallisuutta, jossa on yhteenliittymiä eri turvallisuusalueiden välillä. Riskienhallinnassa tämä on hyvä huomioida.

| | |
|---|---|
| Pääjohtaja | Markku Tervahauta |
| Hallinto- ja talousjohtaja | Mia Nykopp |

**SIGNATURES** **ALLEKIRJOITUKSET** **UNDERSKRIFTER** **SIGNATURER** **UNDERSKRIFTER**

This documents contains 4 pages before this page
Tämä asiakirja sisältää 4 sivua ennen tätä sivua
Detta dokument innehåller 4 sidor före denna sida
Dokumentet inneholder 4 sider før denne siden
Dette dokument indeholder 4 sider før denne side

Markku Petteri Tervahauta
4b11e2b3-aa4b-47db-9b01-9f8ecf10770e - 2022-05-02 15:56:35 UTC +03:00
BankID / MobileID - 917b2e27-53e4-46a0-bd29-641e18b1ee9d - FI

Mia Johanna Nykopp
7e065193-6ad5-4228-919f-17ea7584a906 - 2022-05-02 16:35:49 UTC +03:00
BankID / MobileID - 8e64b032-278f-414d-996a-809c201bfcf5 - FI

| | | | | |
|---|---|---|---|---|
| authority to sign | asemavaltuutus | ställningsfullmakt | autoritet til å signere | myndighed til at underskrive |
| representative | nimenkirjoitusoikeus | firmateckningsrätt | representant | repræsentant |
| custodial | huoltaja/edunvalvoja | förvaltare | foresatte/verge | frihedsberøvende |