

Ketterästi pilveen Digi- ja väestötietoviraston pilvimatka

Mira Holmroos-Kolari 3/2022



**DIGI- JA
VÄESTÖTIETO-
VIRASTO**



DVV:n pilvimatka lyhyesti



Pilvitransformaatiomme tavoitteet

- Cloud first –ajatuksella eli pilveen kaikki mitä voidaan DVV:n **linjaukset huomioiden**
- **Säästämme** ICT-infrastruktuurin sekä siihen liittyvän henkilötyön kuluissa ainakin 30 %, parhaimmillaan jopa 60%
- **Tehostamme** ohjelmistokehitystä ja operointia parantamalla alustan saatavuutta, skaalautuvuutta, siirrettävyyttä ja läpinäkyvyyttä
- Säästöjen ja tehostamisen myötä **saamme panostettua lisää** digitaalisten palveluiden asiakasarvoa tuottavien ominaisuuksien kehittämiseen
- **Lisäämme näkyvyyttä** konepellin alle vaarantamatta tietoturvaa ja tietosuojaa
- **Toimimme edelläkävijöinä** yhteiskunnassa



Pilvisiirrot eli ensimmäinen pilvimatkamme 2018-2021

Pilvessä:

- Suomi.fi Tunnistus EIDAS ja OIDC (2019)
- Yhteentoimivuusalusta (2019)
- DW (2019)
- Suomidigi (2019)
- Design System -komponentit (2019)
- TOIVO skannaus ja dokumenttivarasto (2020)
- Suomi.fi Mobiilibackend (2020)
- Suomi.fi Verkkopalvelu (2020)
- Suomi.fi Palvelutietovaranto (2020)
- Suomi.fi Valtuudet (2021)
- Suomi.fi Tunnistus (2021)
- Aurora-AI (alusta alkaen eli ei ole migraatio)

Etenimme migraatioissa helposta vaikeaan

- Ensin julkista tietoa sisältäviä pienempiä palveluita
- Sitten monimutkaisempia ja saatavuuskriittisiä Suomi.fi-palveluita

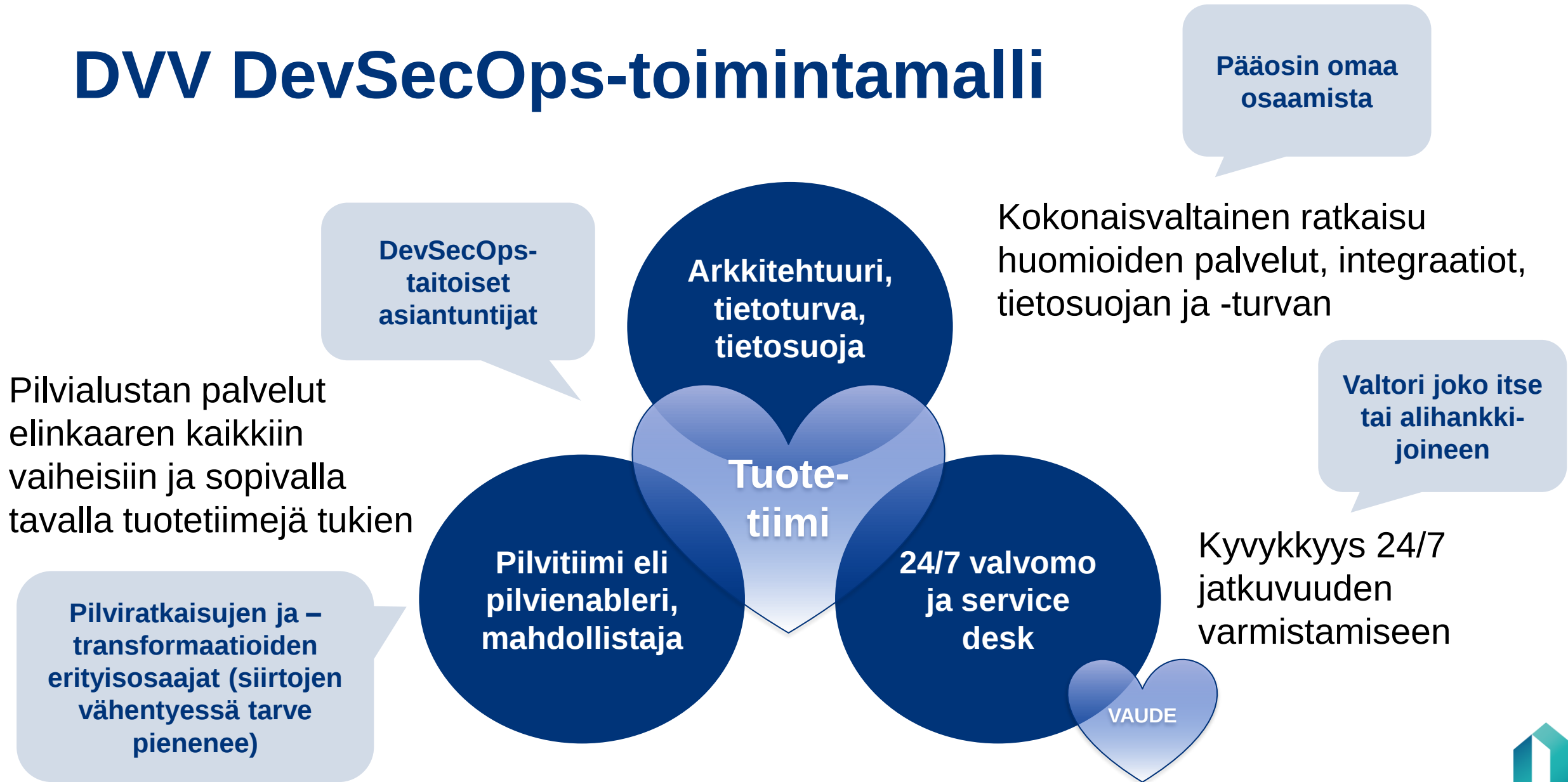
Kaikki uudet toteutetaan lähtökohtaisesti pilveen (linjaukset huomioiden)

Pilveen:

- VAAKA S3, tilintarkastus (avoin)
- Lisäksi Suomi.fi Viestit tekninen uudistus käynnissä H2/2020 alkaen, pilvipohjainen ratkaisu valmistuu 2022 loppuun mennessä



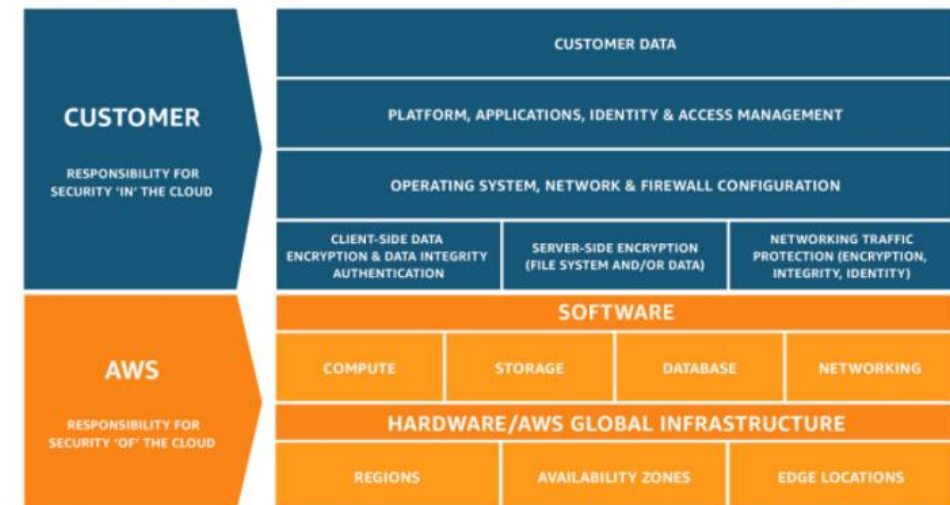
DVV DevSecOps-toimintamalli



Mikä pilvi, missä, miten?



- DVV:n pilvipalvelualusta on Amazon Web Services (AWS)
- DVV käyttää AWS:n Euroopassa sijaitsevia saatavuusalueita (Irlanti, Saksa, Ruotsi). Datat käsittelee tapahtuu siis EU-alueella
- Jaettu vastuu pilvessä: **AWS vastaa pilvialustasta** ja sen tietoturhasta, **DVV pilvialustalle kehittämistään sovelluksista** ja niiden tietoturhasta
- DVV:n arkkitehdit, tietoturva- ja tietosuoja-asiantuntijat tuottavat turvallisen sovelluskehityksen ohjeet, yhteiset toimintamallit (mm. riskienarviointi, uhkamallinnus, tietoturva-arkkitehtuuri..)
- DVV:n tuotetiimit vastaavat vastuupalvelunsa kehittämisestä, operoinnista ja ylläpidosta
- DVV:n pilvitiimi vastaa DVV:n pilvialustasta ja toteuttaa yhteisiä työkaluja tuotetiimien käyttöön
- Pilvitoteutukset ja pilvihallintamalli **auditoidaan 3.osapuolen toimesta** säännöllisesti
- DVV:n pilvi-infrastruktuuria hallitaan ohjelmistokoodina (Infrastructure as Code, IaC). Tämä tarkoittaa, että infran vikaantuessa voidaan nopeasti pystyttää siitä uusi versio.



Pilvitoiminnan johtaminen DVV:llä

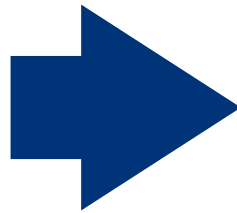
- **Palveluiden omistajat ja tuoteomistajat** johtavat palveluidensa kokonaisvaltaista kehittämistä
- **Tuotetiimin** työn johtamiseen kuuluu kehityksen lisäksi myös tuotannon ylläpito.
- **Pilvipalvelun omistaja** johtaa pilvipalvelun kehittämistä
- **Pilvipalvelun ohjaustiimi** toimii pilvipalvelun omistajan tukena palvelun johtamisessa sekä kehittämisen, että operatiivisten palveluiden osalta



Pilvimatkan suunta nyt

Painopisteenä erityisesti

- Toimintavarmuus ja toiminnan jatkuvuus, varautumisratkaisut
- Moniosaaminen ja jatkuva oppiminen
- Kustannustehokkuus ja optimointi



Pilvivalvomo ^{24/7}

Hallintamalli Valvontavälineet
Optimointi SOC Tietoturvallisuus
Varautuminen
Kustannustehokkuus



Keskeiset linjaukset



Linjausten taustaperiaatteita

- Pohjautuvat **Julkisen hallinnon pilvipalvelulinjauksiin** (Valtiovarainministeriön julkaisuja 35/2018) sekä **Yhteiskunnan turvallisuusstrategiaan**
- Ovat **johdon sekä asiantuntijoiden** kesken mietityt tiedon ja palveluiden sijainnin linjauksemme, joissa huomioidaan käsiteltävän **tietoaineiston luonne sekä toiminnan jatkuvuuden ja varautumisen vaatimukset**
- Haluamme hyödyntää pilvipalveluita mahdollisimman laajasti ja **etenemme ”cloud-first” –periaatteella**
- Merkittävä osa palveluista on siirrettävissä pilveen, **osan palveluista ja tietovarannoista on aina sijaittava Suomessa** esim. varautumisperusteilla



Periaate tietojen ja palveluiden sijainnista ”kolme kori”

- ”Punainen kori”; palvelut ja tietovarannot, jotka on tuotettava Suomessa
- ”Keltainen kori”; DVV:n kriittiset palvelut, jotka on joko tuotettava Suomessa, tai vaihtoehtoisesti oltava siirrettävissä kriittisiltä osin Suomessa tuotettaviksi
- ”Vihreä kori”; Jokaisen palvelun osalta (muutkin kuin yllämainitut), jota suunnitellaan siirrettäväksi Suomen ulkopuolelle tehdään riskienarviointi
 - Mitä varautumisen osalta on huomioitava
 - Tarvitaanko tietoturvallisuuden osalta lisäkontrolleja
 - Voiko palvelua tuottaa ja/tai hallinnoida Suomen ulkopuolelta huomioiden mm. edellä mainittujen toimenpiteiden kustannukset tai tietoturvallisuuteen liittyvät riskit
 - Arviota täydennetään teknisemmällä uhkamallinnuksella ja tietosuojaan vaikutustenarvioinnilla



DVV:n pilviteknologiavalinnat

- Valitaan ensimmäisessä vaiheessa **pilvipalvelualustaksi AWS** ja harkitaan myöhemmin useamman kuin yhden pilvipalvelutarjoajan hankkimista
 - Mahdollistetaan näin paras mahdollinen soveltuvuus DVV:n nykyisten palveluiden (ensisijaisesti Suomi.fi) sovellusarkkitehtuurin ja toteutusperiaatteiden näkökulmasta
 - Mahdollistetaan pilven aitojen hyötyjen ja valmiiden toiminnallisuuksien hyödyntäminen täysmittaisesti tulevaisuudessa ts. jos esim. Azure tarjoaa tiettyjen palveluiden näkökulmasta valmiimpaa → voidaan hyödyntää
- Hankitaan DVV:n käyttöön **alustariippumattomiin teknologioihin perustuva orkestrointiratkaisu** julkiseen pilveen **palveluna**
 - Soveltuvimmaksi sekä kustannuksiltaan mahdollisella tasolla on AWS:n EKS-palvelu (Amazon Elastic Container Service for Kubernetes, tuli markkinoille laajemmin kesällä 2018)



Tietoturva ja tietosuoja näkökulmia

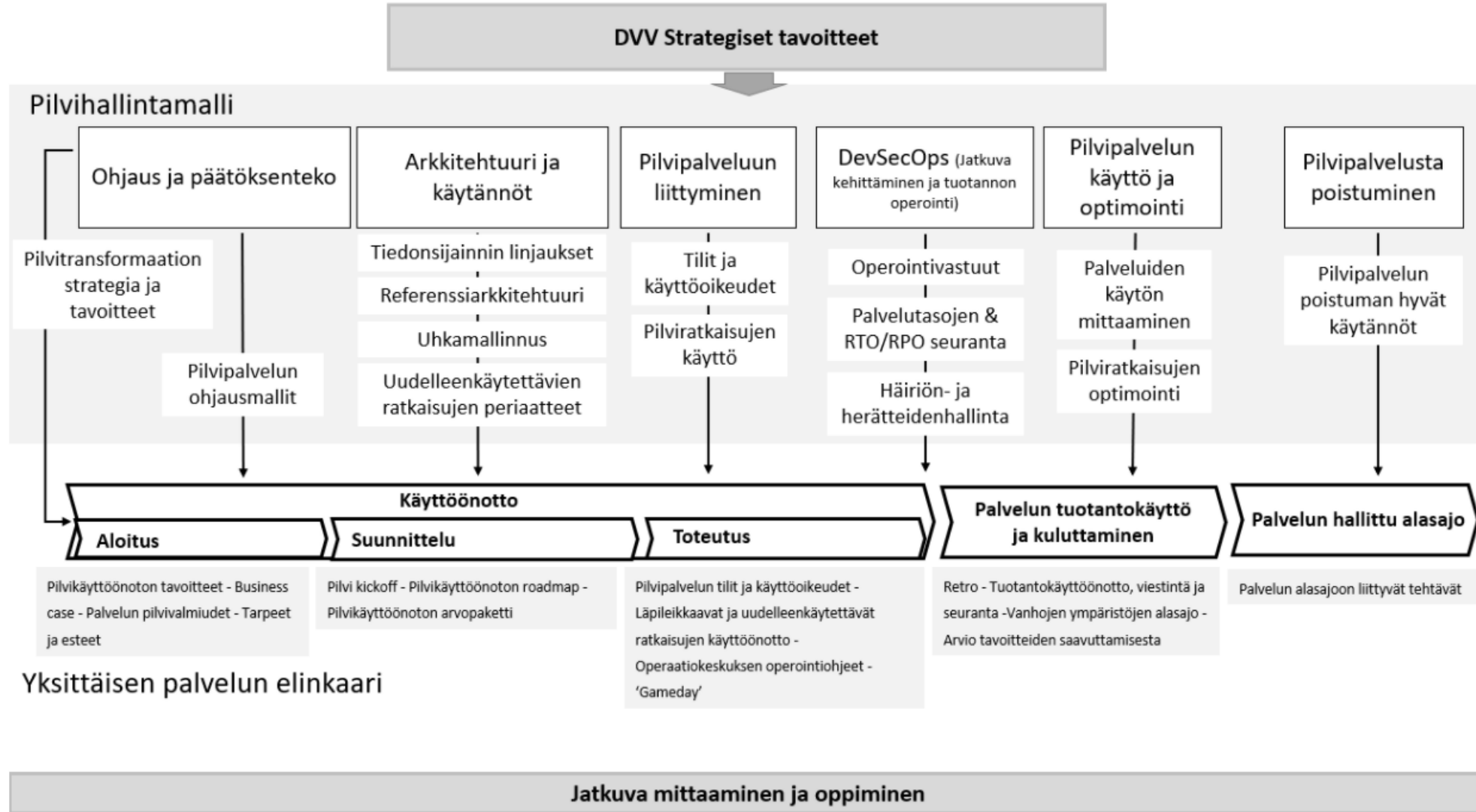


Pohjana tehdyt linjaukset ja periaatteet

- Julkisen hallinnon pilvipalvelulinjaukset, suositukset ja ohjeet
- DVV:n tiedon luokittelu, tiedon ja palveluiden sijainti
 - Mihin koriin kuuluu (vrt. aiemmat DVV linjaukset)
- Kehitettävälle/pilveen siirrettävälle palvelulle tehdään aina riskienarviointi
 - Mitä varautumisen osalta on huomioitava
 - Tarvitaanko tietoturvallisuuden osalta lisäkontrolleja
 - Voiko palvelua tuottaa ja/tai hallinnoida Suomen ulkopuolelta huomioiden mm. edellä mainittujen toimenpiteiden kustannukset tai tietoturvallisuuteen liittyvät riskit
 - Arviota täydennetään teknisemmällä uhkamallinnuksella ja tietosuojan vaikutustenarvioinnilla
- DVV:n turvallisen sovelluskehityksen käsikirja ml. AWS pilvitoteutusten periaatteet
- Auditoinnit ja jatkuva valvonta tehokkaiden työvälineiden avulla



DVV:n pilvihallintamalli



Lopuksi



Oppeja matkan varrelta

- Aloita yksinkertaisemmista ja pienemmistä palveluista, kerää opit teknologiasta ja toimintatavoista → sovelta ja muuta tarvittaessa suuntaa
- Hyödynnä erityisesti alkuvaiheessa riittävää asiantuntemusta ja vankkaa kokemusta pilvimigraatiosta ja -palveluista
- Valmistelkaa yhdessä johdon kanssa pilvilinjaukset
- Satsaa alusta alkaen tietoturvaan, ”Zero Trust” –periaatteella, moniulotteisesti!
- Hyödynnä 3. osapuolen tarkastuksia ja auditointeja matkan varrella
- Ole ennakkoluuloton ja rohkea, mutta huomioi toimintaympäristön tilanne - tämä on matka!





DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi