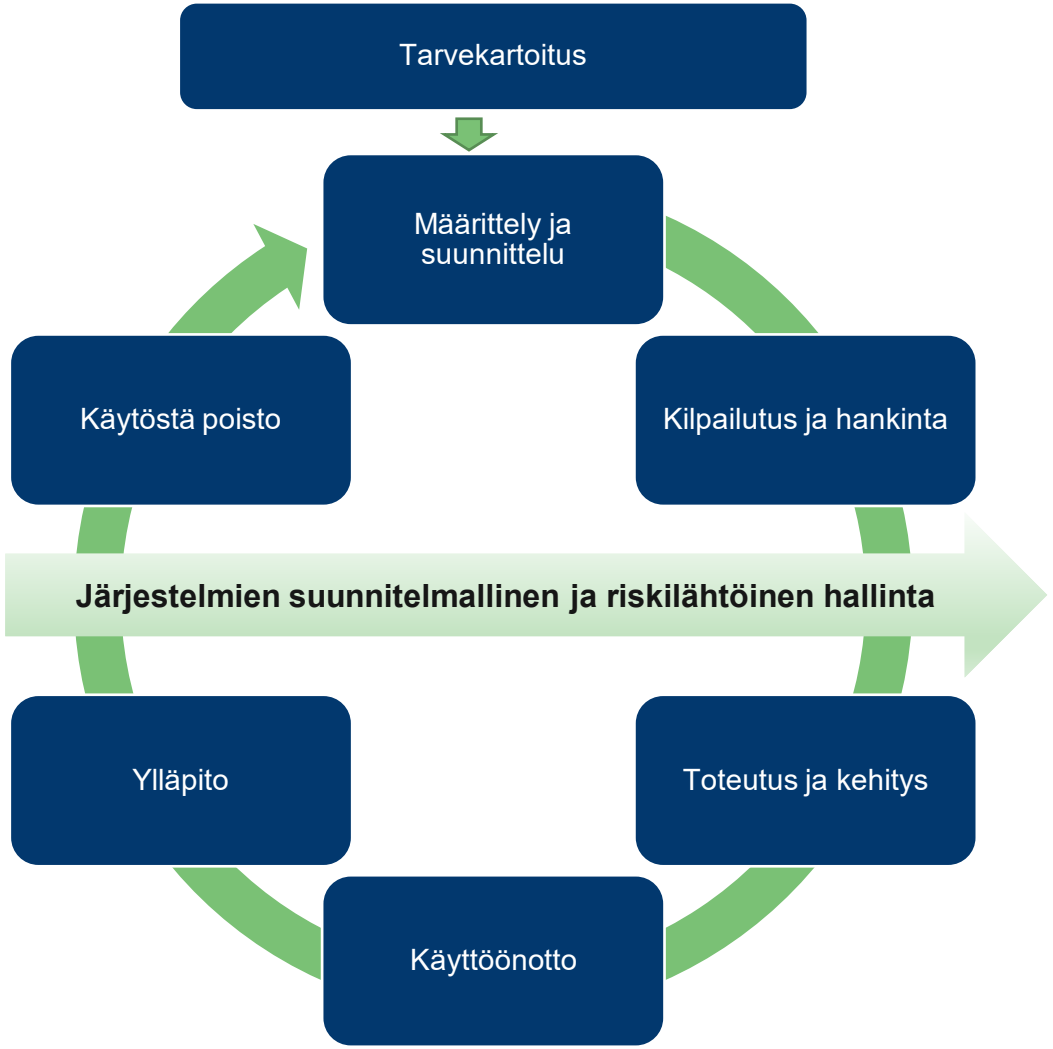
Tietojärjestelmän elinkaari - Tietoturva ja tietosuoja näkökulmat

Lataus23-tapahtuma
13.9.2023

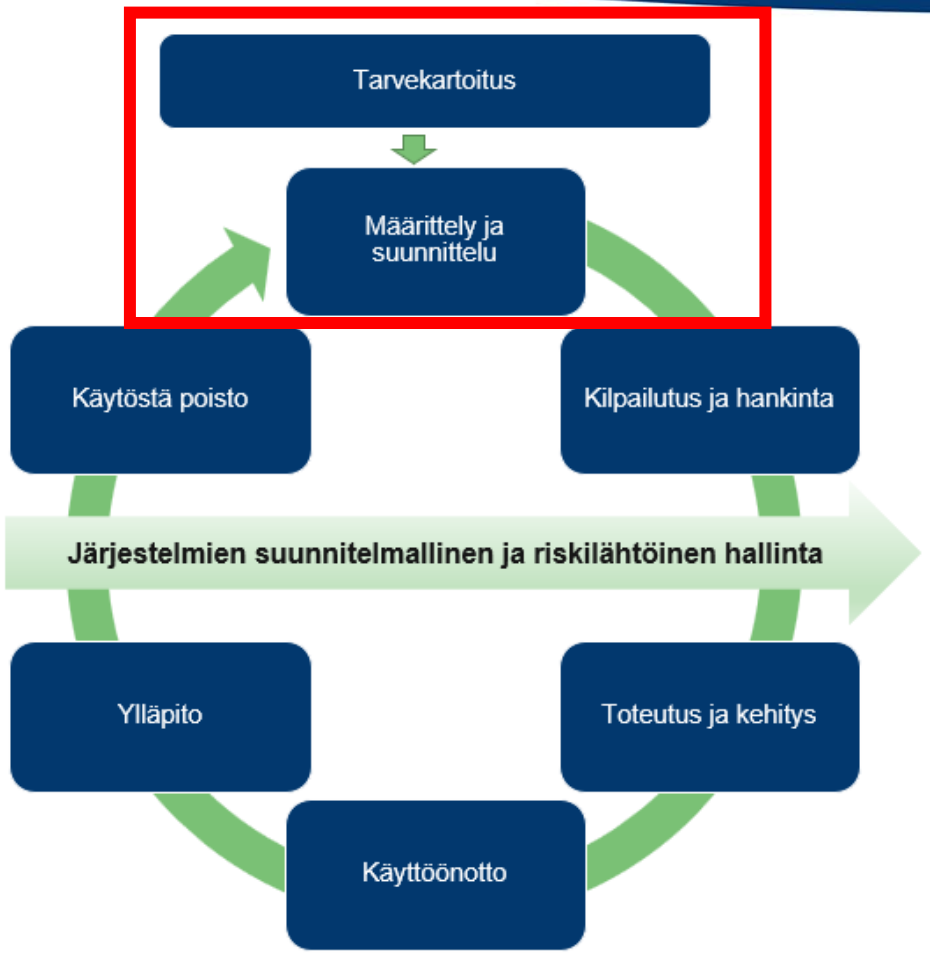
Tiina Rintamäki,
ratkaisuarkkitehti
Tietoturvakonsultointi

Sidosryhmäjulkinen

Tietojärjestelmän elinkaari



Tarvekartoitus, määrittely, suunnittelu

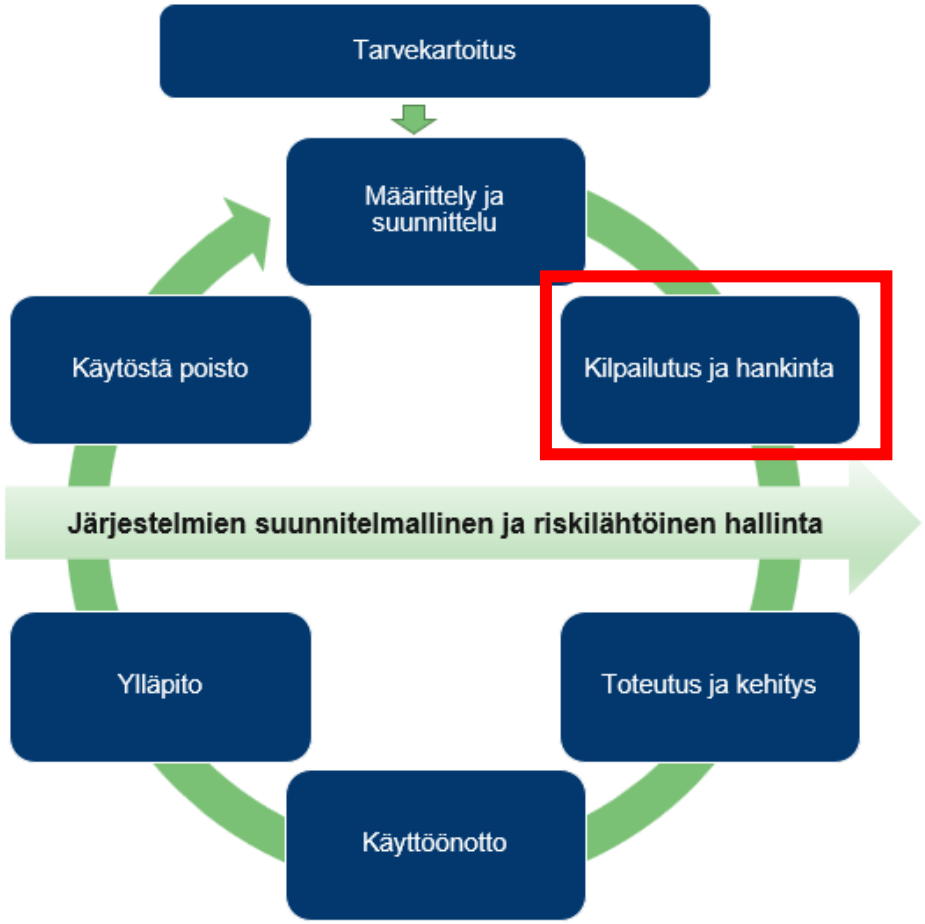


- Tunnistetaan käsiteltävät tietoaineistot, käyttötarkoitus ja vaatimukset → kriittisyys → riskiarvio → määritellään tietoturvallisuustaso
- Tunnistetaan liittymät, riippuvuudet, tietovirrat ja dokumentoidaan nämä
- Riskien arvioinnissa hyvä huomioida koko palvelu- ja toimitusketjun kaikki osapuolet ja heidän ympäristönsä

→Tietosuojavaikutusten arviointi

→Muutosvaikutusten arviointi

Kilpailutus ja hankinta

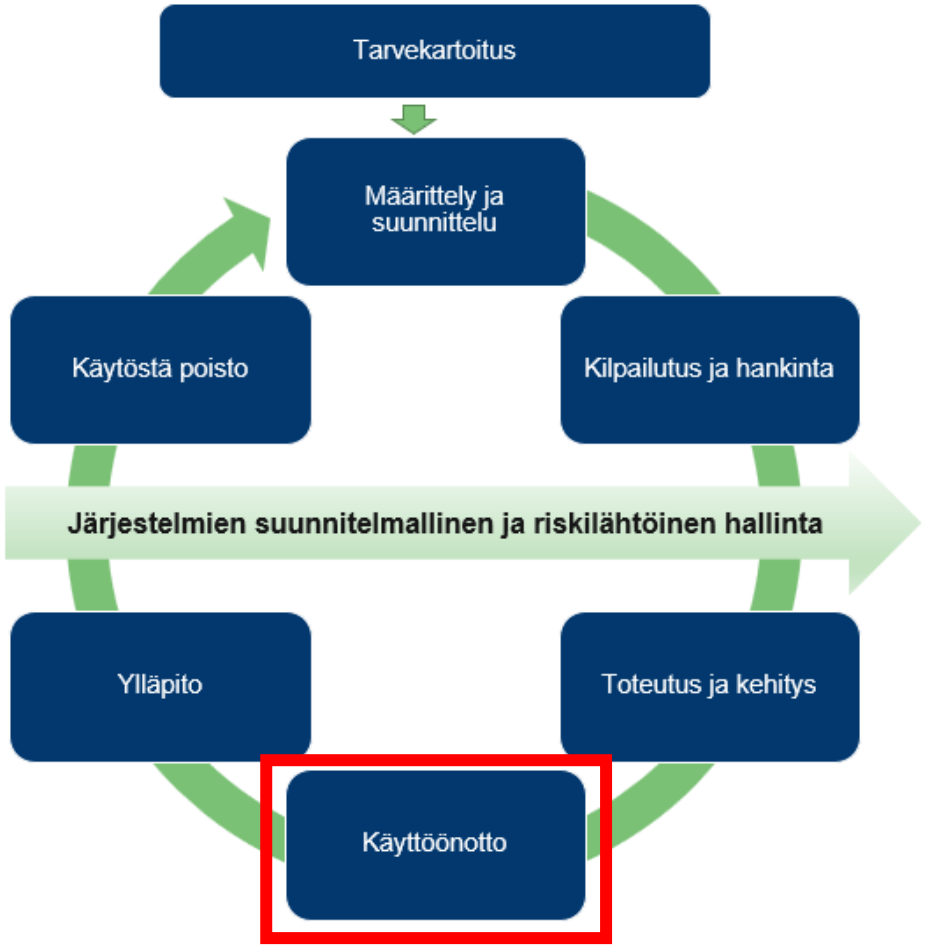


- Hankintavaatimuksiin, tarjouspyyntöihin ja sopimuksiin sisällytetään tietoturvaa ja tietosuojaa koskevat vaatimukset
- Tietoturva- ja tietosuojavaatimukset koskevat sekä tietojärjestelmää että sen toteuttavaa ja tarjoavaa toimittajaa
- Sopimukset ja RACIt eli vastuumatriisit toimijoiden välille

Toteutus ja kehitys

- Uudelleentarkastelu määrittelyvaiheessa laadittuun riskiarviointiin, uhkamallinnukset, riskiarviot -> toteutettavat tietoturvakontrollit
- Suunnitelmien mukainen toteutus vaiheittain → Sisäänrakennettu tietoturvallisuus
- Tietoturvakontrollien dokumentointi

Käyttöönotto



- Käyttöönottosuunnitelma: käyttöönottohyväksyntä; toiminnallisuuksien ja tietoturvakontrollien todentaminen
- **Käyttöönottoasennus tehdään määritetyn prosessin ja ohjeistuksen mukaisesti** → Arkkitehtuuriperiaatteet, suojaukset, kovennukset
- Tietoturvakuvauksen päivittäminen

Ylläpito

- Muutostenhallinta ja vaikutukset tietoturvakontrolleihin
- Säännölliset riskiarviot: katselmoinnit, tietoturvatestaukset, toimittajan auditoinnit, turvallisuustason seuranta, raportointi
- Dokumentaation ja kuvausten ylläpito
- **Noudatetaan organisaation muutos-, poikkeamien- ja riskienhallintamenettelyjä**
- **Huolehditaan toiminnan jatkuvuudesta: toipumissuunnitelmat ja harjoittelu**
- Ohjelmistohaavoittuvuuksien hallinnan prosessi
- Haittaohjelmasuojausta koskevat toimintamallit
- **Valvonta ja seuranta**
- Varmuuskopiointi, kopioiden suojaus ja lokitus
- **Ylläpitoyhteyksien ja –oikeuksien ylläpito:**

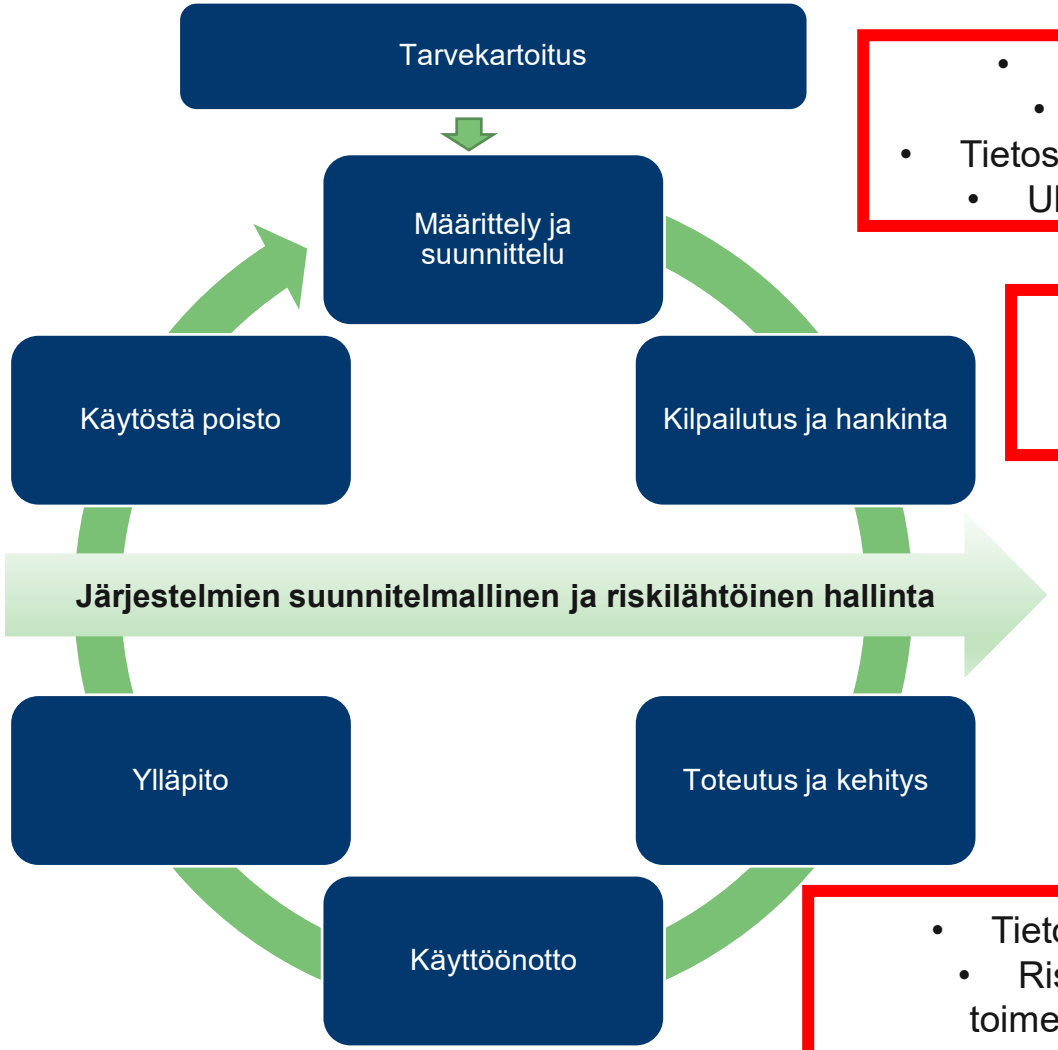
Vähimpien oikeuksien periaate

istekki

Käytöstä poisto

- Käytöstä poiston riskiarviointi
- **Käytöstä poiston suunnitelma**, missä huomioitu migraaatiot, tuhottavat laitteet, muistivälineiden sanitointi, tietojärjestelmien osien tuhoaminen
- **Huomioidaan tietoaineistojen elinkaari - arkistointi**
- Tuhoaminen luotettavalla tavalla

Istekin tietoturvakonsultoinnin palvelut



- Kriittisyysluokittelu
- Riskinarviointi
- Tietosuojavaikutusten arviointi
- Uhkamallinnustyöpaja

- Hankinnan konsultointi – tietoturva- ja tietosuojavaatimukset

- Muutosvaikutusten arviointi – tietoturvan ja tietosuojan arviointi
- Tietoturvatestaus

- Tietoturva-arvioinnit
- Riskinarviointi ja toimenpidesuositukset

istekki

Kysymyksiä?

Kiitos!