SaaS-palvelun hankinta- ja digiturvaopas

SaaSec-hanke 2023

Sisällys

SaaS-palvelun hankinta- ja digiturvaopas 3

Pääkäyttötilanteet 6

Kotimaisen tai alueellisen SaaS-ratkaisun hankkiminen 7

Globaalin SaaS-ratkaisun hankkiminen 10

Olemassa olevan palvelun siirtäminen On-premisestä SaaSiksi 13

Pilvipalveluiden elinkaari 16

Pilvipalveluvalmiuksien kehittäminen ja pilvipalveluiden johtaminen 16

1) Kohteen määrittely ja rajaus 17

2) Kohteen vaatimusten määrittely 18

3) Ratkaisuvaihtoehtojen arviointi 20

4) Hankinta ja sopimus 22

5) Palvelun toteutus ja muutosten hallinta 23

6) Palvelun päättäminen tai siirto 25

SaaS-palvelun digitaalinen turvallisuus aiheittain 27

Tarjouspyyntö 27

Vaatimusmäärittely 28

Arkkitehtuurin kuvaaminen 31

Tietoturvallisuuden arviointi 37

Tietosuojan vaikutustenarviointi (DPIA) 40

Tietojen siirron vaikutustenarviointi (TIA) 41

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) 42

RACI-vastuunjakotaulukko 44

SaaS-palveluntoimittajien vinkit 47

Linkkivinkit muihin aineistoihin 49

Hankintapohjien esittely ja käyttöohjeita 52

A: Esikonseptointipohja 52

B: Hybridihankintojen tarkistuslista ja tiivisvaatimukset 52

C: Tietoturvan, tietosuojan ja jatkuvuuden erityisvaatimusten kokoamispohja 53

D: Käyttötapausten kuvauspohja 53
E: Integraatioiden kuvauspohja 54
F: Hinnan kokoluokka-arviopohja 54
G: Pilviratkaisun riskiarviopohja 54
K: Vaatimuslomake – yleiset SaaS (tarjouspyynnön liite 4) 55
L: Mallivaatimukset – SaaS-hosting 55
M: SaaS-hintalomake (tarjouspyynnön liite 5) 56
N: Hankinnan kohde -kuvauspohja (tarjouspyynnön liite 1) 56
O: Arkkitehtuuritiivistelmä 57
P: Tarjousohjeet ja vertailuperusteet (tarjouspyynnön liite 6) 57
SaaSec-hanke lyhyesti 58
Käsitteitä ja sanastoa 59

SAAS-PALVELUN HANKINTA- JA DIGITURVAOPAS

Tämä SaaSec-hankkeen tuottama opas antaa kunnille tietoa ja työkaluja SaaS-palvelun hankintaprosessin tueksi. Tärkeänä näkökulmana on pyrkiä varmistamaan palvelun digitaalinen turvallisuus sen elinkaaren kaikissa vaiheissa. Opas on suunnattu erityisesti IT-asiantuntijoille, tietosuoja- ja tietoturvavastaaville, hankinta-asiantuntijoille sekä toimialojen substanssiasiantuntijoille, jotka ovat työssään tekemisissä pilvipalveluiden hankintojen ja turvallisuuden kanssa. SaaSec-hankkeen esittely löytyy tämän oppaan lopusta.

SaaSec-hankkeessa on tuotettu SaaS-hankintojen turvallista ja tuloksellista läpivientiä varten joukko esiselvitykseen, vaatimusmäärittelyyn, tarjouspyyntöön, vaikutustenarviointiin ja sopimukseen liittyviä pohjia SaaS-hankintaprosessin tueksi. Oppaan sisältämiä uusia sisältöjä ja pohjia on kehitetty hankkeessa järjestetyissä koulutuksissa ja työpajoissa pilvipalveluiden ja digitaalisen turvallisuuden asiantuntijoiden johdolla.

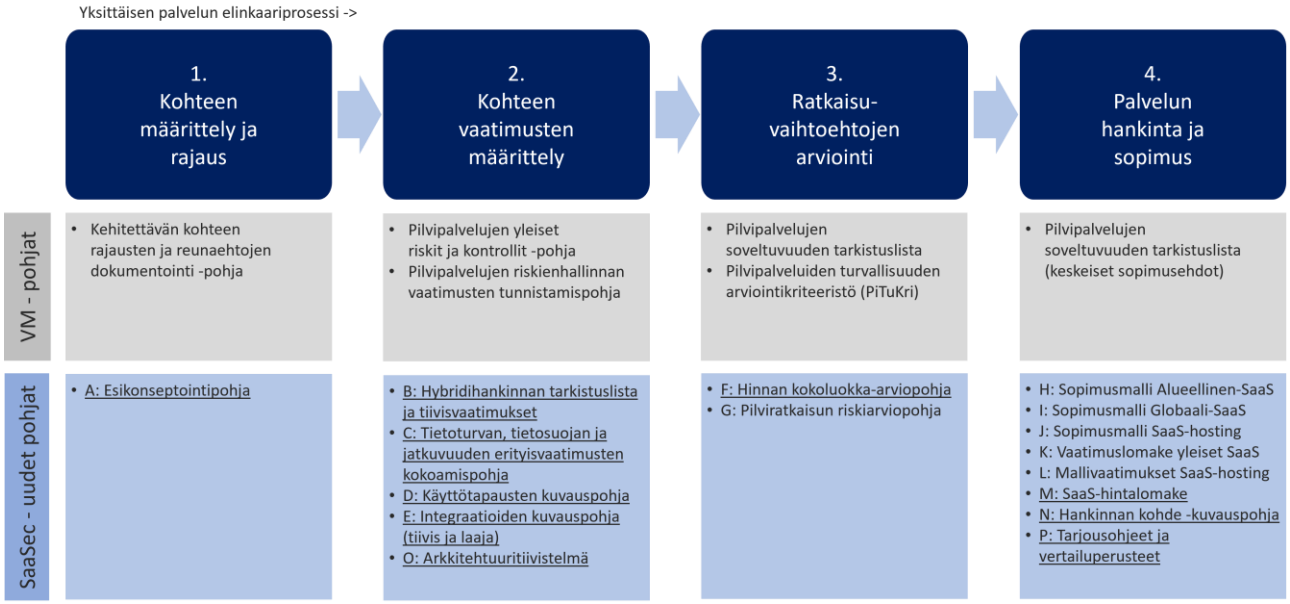
Pohjat ovat ladattavissa valtiovarainministeriön Tiimeri-työtilasta SaaSec-hankkeen kansiosta (vaatii kirjautumisen) ja Sipoon kunnan verkkosivuilta SaaS-palvelun hankinta- ja digiturvaoppaasta.

➔ Ladattavissa olevat, suositellut pohjat on merkitty oppaassa nuolella.

Voit vapaasti ladata pohjia omaan käyttöösi. **Materiaalin soveltuvuus tulee arvioida aina tapauskohtaisesti lainsäädäntö, sopimuksen ehdot ja olosuhteet kokonaisuutena huomioiden.**

Oppaan tekstisisältöjen koostamisessa on hyödynnetty useiden eri tahojen tuottamia, verkossa julkaistuja ohjeita ja tietosisältöjä sekä verkkokoulutuksia. Opas ohjaa myös linkkien avulla ulkopuolisiin verkkosivustoihin, esimerkiksi eri viranomaisten tuottamiin ohjeisiin ja arviointikriteeristöihin. Pilvipalveluiden elinkaarimallin lähteenä ja taustadokumenttina on valtiovarainministeriön julkaisu Pilvipalvelujen soveltamisohje.

SaaSec-hankkeen SaaS-hankintoja tukevat pohjat



Yllä olevaan taulukkoon on koottu SaaSec-hankkeen suosittelemat ja tuottamat pohjat SaaS-palvelun hankinnan tueksi.

- Valtiovarainministeriön pilvipalvelujen soveltamisohjeen pohjat (harmaalla alueella) ja
- SaaSec-hankkeessa tuotetut, pilvipalvelujen soveltamisohjetta täydentävät pohjat (vaaleansinisellä alueella). Alleviivattuja pohjia voidaan hyödyntää muissakin kuin SaaS-hankinnoissa.

Voit tutustua oppaaseen kahdella eri tavalla: SaaS-palvelun elinkaaren vaiheiden kautta edeten tai oppaassa kuvattujen kolmen pääkäyttötilanteen kautta. Voit myös hyödyntää suoraan aihesivuja, mikäli haluat nopeasti tietoa esimerkiksi tarjouspyynnön laatimisesta, kokonaisarkkitehtuurista tai tietosuojan ja tietoturvan arvioinnista.

Vastuuvapauslauseke

Tämän SaaSec-hankkeen tuottaman oppaan ja verkkosivujen avulla SaaSec-hanke ja hankekunnat helpottavat tiedonsaantia ja tarjoavat työkaluja SaaS-palveluiden hankintaprosessin ja digitaalisen turvallisuuden varmistamisen tueksi. Aineiston ajantasaisuutta ja virheettömyyttä ei voida kuitenkaan taata hankkeen päättymisen jälkeen.

SaaSec-hanke ja hankekunnat eivät vastaa oppaan ja verkkosivujen sisältämästä aineistosta. Oppaassa ja verkkosivuilla oleva aineisto on yleisluonteista, eikä sitä ole pyritty sovittamaan erityisesti minkään kunnan, hankinnan tai järjestelmän tarpeisiin. Aineiston soveltuvuus tulee arvioida aina tapauskohtaisesti lainsäädäntö, sopimuksen ehdot ja olosuhteet kokonaisuutena huomioiden. SaaSec-hankkeen tuottama opas ja verkkosivut sisältävät linkkejä ulkopuolisiin verkkosivustoihin, joihin SaaSec-hanke ja hankekunnat eivät voi vaikuttaa ja joiden sisällöstä SaaSec-hanke ja hankekunnat eivät vastaa.

SaaSec-hanke ja hankekunnat eivät vastaa millään tavoin mahdollisista menetyksistä, vahingoista, kustannuksista tai korvauksista, jos jokin taho käyttää näitä tietoja päätöstensä perusteena tai tekee tai jättää tekemättä jotakin julkaistun materiaalin perusteella. SaaSec-hankkeen tuottaman oppaan ja verkkosivujen sisältämien tietojen ja aineiston käyttö on kokonaan käyttäjän vastuulla.

Pääkäyttötilanteet

SaaSec-hankkeessa on kuvattu kolmen pääkäyttötilanteen hankintapolut SaaS-hankinnoille:

- Kotimaisen tai alueellisen SaaS-ratkaisun hankkiminen
- Globaalin SaaS-ratkaisun hankkiminen
- Olemassa olevan palvelun siirtäminen On-premisestä SaaSiksi

Eri hankintatilanteissa suositeltujen pohjien käytöstä voit lukea tarkemmin oppaan osiosta Hankintapohjien esittely ja käyttöohjeita.

Valinta, kumpaa mallia (kotimainen/alueellinen vai globaali) lähdetään hakemaan, on hyvä tehdä ennen vaatimusmäärittely- ja tarjouspyyntövaihetta. Mallien keskeisimmät erot ja ominaisuudet:

Kotimainen tai alueellinen SaaS	**Globaali SaaS**
• Tyypillisesti paikallinen tai pohjoismainen toimija, jolla ei ole vielä valtavaa määrää asiakkaita • Kohtalaiset tai pienet käyttövolyymit • Usein aika kevyesti tuotteistettu palvelu- ja toimitusmalli – koko SaaS-palvelu usein aika uusi ratkaisumalli ja vielä kehittyvä • Asiakkaalla voi olla mahdollista vaikuttaa sopimusehtoihin ja käyttää asiakkaan ehtoja + JIT 2015 -ehtoja • Ei välttämättä erillistä integraattoria vaan maksimissaan toimittaja-alihankkijasuhde ➢ Kotimaisen tai alueellisen SaaSin vaatimukset ja sopimusehdot (vain yksi vastuurooli, ei kahta roolia)	• Suuri kansainvälinen teknologiatoimittaja, jolla on tuhansia asiakkaita (esim. SAP, Google, Oracle, Microsoft, Salesforce, ServiceNow jne.) • Valtavat käyttövolyymit • Erittäin pitkälle tuotteistettu palvelu- ja toimitusmalli • Toimittajalla on globaalit sopimusehdot, joihin asiakas ei voi käytännössä vaikuttaa lainkaan • Varsinaisena käyttöönottajana usein erillinen integraattori ➢ Globaalin SaaSin vaatimukset ja sopimusehdot (näissä Ohjelmistopalvelutoimittajan ja Järjestelmätoimittajan roolit on eroteltu toisistaan)

Roolituksesta SaaS-toimituksissa

Kotimainen tai alueellinen SaaS	**Globaali SaaS**
Toimittaja: Vain yksi toimittaja, joka yleensä toimittaa omaa järjestelmäänsä. Toimii sekä järjestelmän sovittajana, SaaS-toimittajana että omistaa oikeudet järjestelmään.	**Järjestelmätoimittaja (järjestelmäintegraattori)**: Sovittaa valmisohjelmiston asiakkaan tarpeisiin. Tuottaa ns. sovellusylläpitopalvelun toimittamalleen järjestelmälle. **Ohjelmistopalvelutoimittaja (järjestelmävalmistaja)**: Tuottaa SaaS-palvelun. Omistaa oikeudet järjestelmään.

KOTIMAISEN TAI ALUEELLISEN SAAS-RATKAISUN HANKKIMINEN

Tarve

- Tarve hankkia kilpailuttamalla järjestelmä, joka toteutetaan SaaS-mallilla
- Kunnalla voi olla tähän jo olemassa oleva järjestelmä tai hankittava järjestelmä on kokonaan uusi

Huomioitavaa

- Kunnan on valittava ennen tarjouspyynnön julkaisua, eteneekö se alueellisen SaaSin vai globaalin SaaSin mallilla. Kaikki voivat vastata globaalin SaaSin malliin, mutta globaalien SaaSien toimittajat eivät voi vastata alueellisen SaaSin malliin. Kuitenkin globaalin SaaSin mallissa on kuntien kannalta heikommat ehdot ja sen sopimus näyttäytyy toimittajille vähän monimutkaisemmalta.
- Markkinavuoropuhelussa ja alustavan tarjouspyynnön kommenttikierroksissa on oltava tasapuolinen ja neutraali.

Eteneminen

1. Määritä tarkemmin hankinnan kohde ja sen keskeiset tiedot (esim. integraatiotarve, käyttövolyymit, migraatiotarve). Tässä voi hyödyntää **pohjaa A**.
2. Dokumentoi hankinnan kohde (**erityisesti pohja N**, sekä tämän **tukena pohjat C, D ja E**). Laajoissa hankinnoissa kannattaa hyödyntää kokonaisarkkitehtuuripohjaa.
3. Käynnistä markkinavuoropuhelu keskeisten tarjoajakandidaattien kanssa. Käy läpi:
   ⇒ SaaSin toimitusmalli: toimittaako toimittaja omaa järjestelmäänsä vai jonkun toisen valmistamaa järjestelmää ja onko SaaS-ratkaisu globaali vai alueellinen. Valitse kumpaa hankintamallia käytetään (tässä alueellinen).
   ⇒ Pyydä tarjoajakandidaatteja täyttämään oman pilvipalvelunsa soveltuvuudesta arvio (**esim. VM:n pilvipalvelujen soveltuvuuden tarkistuslista tai PiTuKri**).
   ⇒ Pyydä tarjoajakandidaatteja täyttämään heidän ratkaisunsa hinnan kokoluokka-arvio (**pohja F**).
4. Arvioi tarvittaessa vielä itse muut riskiarviot (esim. DPIA, TIA sekä pilvipalvelun riskiarvio (**pohja G**). Haastavissa tapauksissa valitse (kilpailullinen) neuvottelumenettely.
5. Laadi tarjouspyyntö
   ⇒ Hankinnan kohde (**pohja N**), sopimusmalli (**pohja H**), vaatimukset (**pohja K**), hintalomake (**pohja M**) jne.
6. Lähetä alustava tarjouspyyntö vielä keskeisille tarjoajakandidaateille kommentoitavaksi. Ota kommentit aidosti huomioon.
7. Vie tarjousprosessi läpi, tee hankintapäätös.
8. Täsmennä käyttöönottosuunnitelma ennen sopimuksen allekirjoittamista.
9. Ota SaaS-järjestelmä käyttöön, päivitä järjestelmädokumentaatio.

Hyödynnettävät pohjat

H: Sopimusmalli Alueellinen-SaaS

Tarjouspyynnöstä koottavat:

- ➔ K: Vaatimuslomake – yleiset SaaS (.xlsx)
- ➔ M: SaaS-hintalomake (.xlsx)
- ➔ N: Hankinnan kohde -kuvauspohja (.docx)

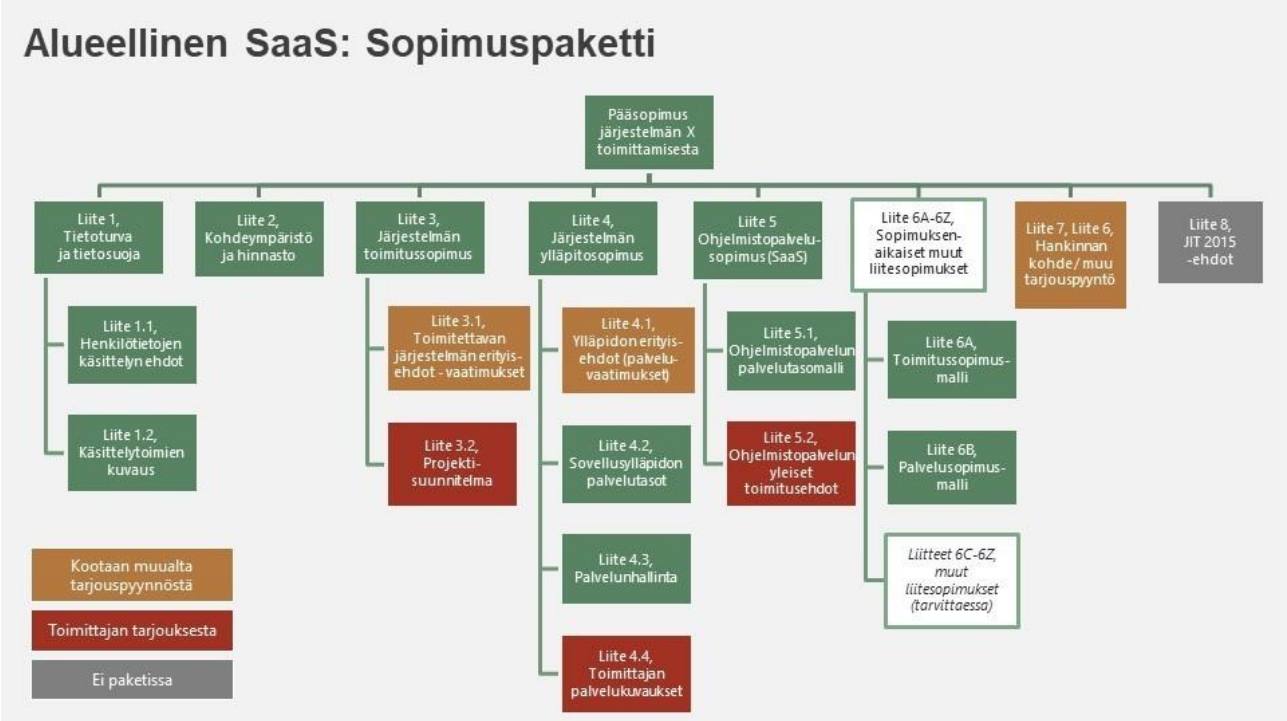
Bonuspohjat (käytä tarpeen mukaan):

- ➔ A: Esikonseptointipohja (.pptx)
- ➔ C: Tietoturvan, tietosuojan ja jatkuvuuden erityisvaatimusten kokoamispohja (.xlsx)
- ➔ D: Käyttötapausten kuvauspohja (.docx)
- ➔ E: Integraatioiden kuvauspohja (.xlsx)
- ➔ F: Hinnan kokoluokka-arviopohja (.xlsx)
  Pilvipalvelujen soveltuvuuden tarkistuslista (.xlsx)
  Ladattavissa täältä: Pilvipalvelujen soveltamisohje, valtiovarainministeriö
  Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKri
  Ladattavissa täältä: PiTuKri, Traficom
- ➔ G: Pilviratkaisun riskiarviopohja (.xlsx)

H: Sopimusmalli Alueellinen-SaaS

Alueellinen SaaS -sopimusmallissa järjestelmätoimittaja vastaa myös ohjelmistopalvelusopimuksesta. Sopimuksessa voidaan käyttää asiakkaan ehtoja ensisijaisesti. Ei siis erikseen järjestelmätoimittajaa ja ohjelmistotoimittajaa – vain toimittaja ja yksi pääsopimus.

Oheinen kaaviokuva esittää kotimaisen tai alueellisen SaaS-palvelun hankinnassa hyödynnettävien mallipohjien suhteen toisiinsa ja sopimuspaketin kokonaisuudessaan.



Pääsopimus liitteineen:

- ➔ Pääsopimus järjestelmän X toimittamisesta ja ylläpidosta (.docx)
- ➔ Liite 1, Tietoturva ja tietosuoja (.docx)
- ➔ Liite 1.1,Henkilötietojen käsittelyn ehdot (.docx)
- ➔ Liite 1.2, Käsittelytoimien kuvaus (.docx)
- ➔ Liite 2, Kohdeympäristö ja hinnasto (.docx)
- ➔ Liite 3, Järjestelmän toimitussopimus (.docx)
- ➔ Liite 4, Palvelusopimus, järjestelmän ylläpitosopimus (.docx)
- ➔ Liite 4.2, Sovellusylläpidon palvelutasot ja sanktiot (.docx)
- ➔ Liite 4.3, Palvelunhallinta (.docx)
- ➔ Liite 5, Ohjelmistopalvelusopimus SaaS (.docx)
- ➔ Liite 5.1, Ohjelmistopalvelun palvelutaso- ja sanktiomalli (.docx)
- ➔ Liite 6A, Toimitussopimusmalli (.docx)
- ➔ Liite 6B, Palvelusopimusmalli (.docx)

GLOBAALIN SAAS-RATKAISUN HANKKIMINEN

Tarve

- Tarve hankkia kilpailuttamalla järjestelmä, joka toteutetaan SaaS-mallilla
- Keskeiset ratkaisukandidaatit perustuvat globaaleihin SaaS-palveluihin
- Kunnalla voi olla tähän jo olemassa oleva järjestelmä tai hankittava järjestelmä on kokonaan uusi

Huomioitavaa

- Kunnan on valittava ennen tarjouspyynnön julkaisua, eteneekö se alueellisen SaaSin vai globaalin SaaSin mallilla. Kaikki voivat vastata globaalin SaaSin malliin, mutta globaalien SaaSien toimittajat eivät voi vastata alueellisen SaaSin malliin. Kuitenkin globaalin SaaSin mallissa on kuntien kannalta heikommat ehdot ja sen sopimus näyttäytyy toimittajille vähän monimutkaisemmalta.
- Markkinavuoropuhelussa ja alustavan tarjouspyynnön kommenttikierroksissa on oltava tasapuolinen ja neutraali.

Eteneminen

1. Määritä tarkemmin hankinnan kohde ja sen keskeiset tiedot (esim. integraatiotarve, käyttövolyymit, migraatiotarve). Tässä voi hyödyntää **pohjaa A**.
2. Dokumentoi hankinnan kohde (**erityisesti pohja N**, sekä tämän **tukena pohjat C, D ja E**). Laajoissa hankinnoissa kannattaa hyödyntää kokonaisarkkitehtuuripohjaa.
3. Käynnistä markkinavuoropuhelu keskeisten tarjoajakandidaattien kanssa. Käy läpi:
   ⇒ SaaSin toimitusmalli: toimittaako toimittaja omaa järjestelmäänsä vai jonkun toisen valmistamaa järjestelmää ja onko SaaS-ratkaisu globaali vai alueellinen. Valitse kumpaa hankintamallia käytetään (tässä globaali).
   ⇒ Pyydä tarjoajakandidaatteja täyttämään oman pilvipalvelunsa soveltuvuudesta arvio (**esim. VM:n pilvipalvelujen soveltuvuuden tarkistuslista tai PiTuKri**).
   ⇒ Pyydä tarjoajakandidaateilta globaalien SaaS-palvelujen vakioehdot. Peilaa näitä mallivaatimuksiin (**pohja K**) ja muokkaa vaatimuksia siten, että ne soveltuvat useimmille pääkandidaateille. Toimittaja ei voi muuttaa globaalin SaaSin ehtoja.
   ⇒ Käy tarjoajien kanssa läpi järjestelmäintegraattorin ja SaaS-palveluntuottajan roolit ja hankintalain ehdot (= muodostettava ryhmittymä tai alihankintamalli).
   ⇒ Pyydä tarjoajakandidaatteja täyttämään heidän ratkaisunsa hinnan kokoluokka-arvio (**pohja F**).
4. Arvioi tarvittaessa vielä itse muut riskiarviot (Esim. DPI, TIA sekä pilvipalvelun riskiarvio (**pohja G**). Haastavissa tapauksissa valitse (kilpailullinen) neuvottelumenettely.
5. Laadi tarjouspyyntö
   ⇒ Hankinnan kohde (**pohja N**), sopimusmalli (**pohja I**), vaatimukset (**pohja K**), hintalomake (**pohja M**) jne.
6. Lähetä alustava tarjouspyyntö vielä keskeisille tarjoajakandidaateille kommentoitavaksi. Ota kommentit aidosti huomioon.
7. Vie tarjousprosessi läpi, tee hankintapäätös.
8. Täsmennä käyttöönottosuunnitelma ennen sopimuksen allekirjoittamista. Tarkenna, kuka vastaa toimituksessa mistäkin (integraattori vs. SaaS-toimija).
9. Ota SaaS-järjestelmä käyttöön, päivitä järjestelmädokumentaatio.

Hyödynnettävät pohjat

I: Sopimusmalli Globaali-SaaS

Tarjouspyynnöstä koottavat:

- ➔ K: Vaatimuslomake – yleiset SaaS (.xlsx)
- ➔ M: SaaS-hintalomake (.xlsx)
- ➔ N: Hankinnan kohde -kuvauspohja (.docx)

Bonuspohjat (käytä tarpeen mukaan):

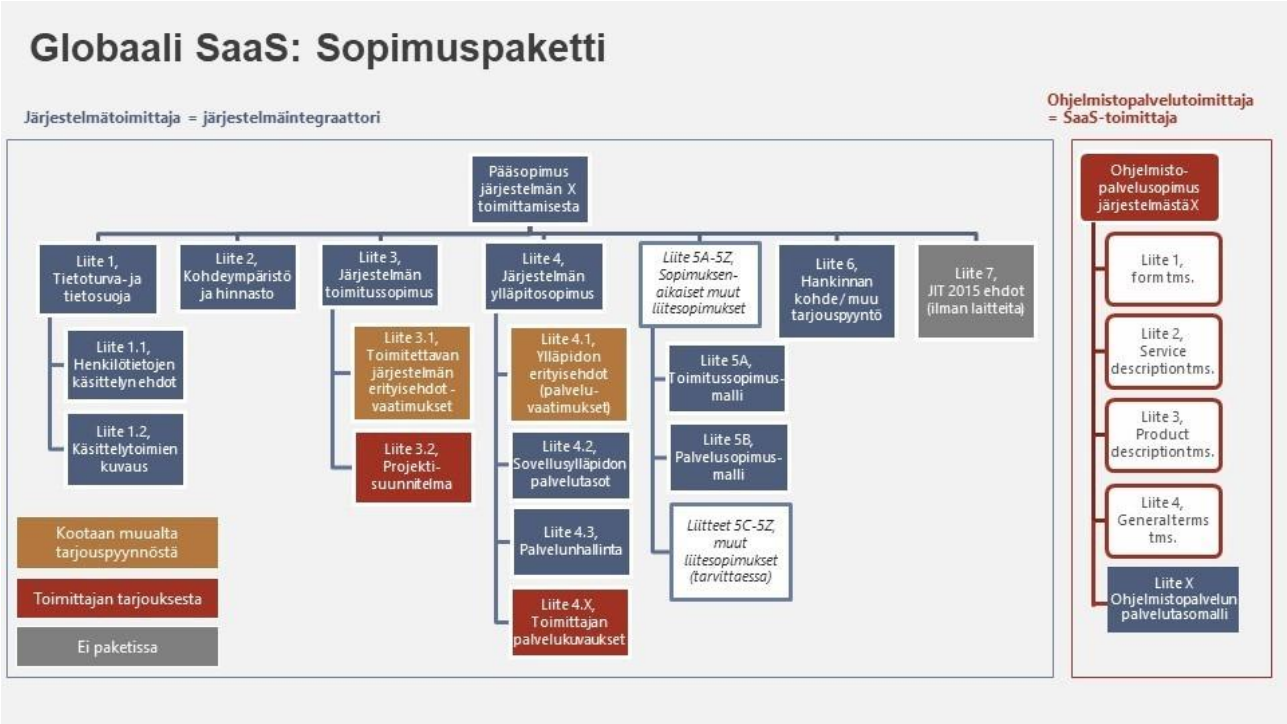
- ➔ A: Esikonseptointipohja (.pptx)
- ➔ C: Tietoturvan, tietosuojan ja jatkuvuuden erityisvaatimusten kokoamispohja (.xlsx)
- ➔ D: Käyttötapausten kuvauspohja (.docx)
- ➔ E: Integraatioiden kuvauspohja (.xlsx)
- ➔ F: Hinnan kokoluokka-arviopohja (.xlsx)
  Pilvipalvelujen soveltuvuuden tarkistuslista (.xlsx)
  Ladattavissa täältä: Pilvipalvelujen soveltamisohje, valtiovarainministeriö
  Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKri
  Ladattavissa täältä: PiTuKri, Traficom
- ➔ G: Pilviratkaisun riskiarviopohja (.xlsx)

I: Sopimusmalli Globaali-SaaS

Globaali SaaS -sopimusmallissa erillinen/rinnakkainen ohjelmistopalvelusopimuspohja on tarjouspyynnössä mukana lähinnä yhtenäistämässä pääehtoja tarjouspyynnössä. Käytännössä ohjelmistopalvelusopimus tehdään globaalien SaaS-toimittajien kanssa aina heidän omilla sopimusmalleillaan – he eivät anna tähän vaihtoehtoja. Globaalit SaaS-toimittajat eivät yleensä suostu ottamaan mitään tarjouksensa dokumentteja tai niiden osia omaan sopimukseensa – ei edes vaatimuksia.

Tämä johtaa siihen, että järjestelmän toimivuuden vastuu joudutaan siirtämään järjestelmätoimittajalle ja pääsopimuksen alaiseen liitteen 3 mukaiseen toimitussopimukseen.

Oheinen kaaviokuva esittää globaalin SaaS-palvelun hankinnassa hyödynnettävien mallipohjien suhteen toisiinsa ja sopimuspaketin kokonaisuudessaan.



Pääsopimus liitteineen:

- ➔ Pääsopimus järjestelmän X toimittamisesta ja ylläpidosta (.docx)
- ➔ Liite 1, Tietoturva ja tietosuoja (.docx)
- ➔ Liite 1.1,Henkilötietojen käsittelyn ehdot (.docx)
- ➔ Liite 1.2, Käsittelytoimien kuvaus (.docx)
- ➔ Liite 2, Kohdeympäristö ja hinnasto (.docx)
- ➔ Liite 3, Järjestelmän toimitussopimus (.docx)
- ➔ Liite 4, Palvelusopimus, järjestelmän ylläpitosopimus (.docx)
- ➔ Liite 4.2, Sovellusylläpidon palvelutasot ja sanktiot (.docx)
- ➔ Liite 4.3, Palvelunhallinta (.docx)
- ➔ Liite 5A, Toimitussopimusmalli (.docx)
- ➔ Liite 5B, Palvelusopimusmalli (.docx)
- ➔ Malli Ohjelmistopalvelun palvelutasoista ja sanktioinnista (.docx)
- ➔ Ohjelmistopalvelusopimus – pohja (.docx)

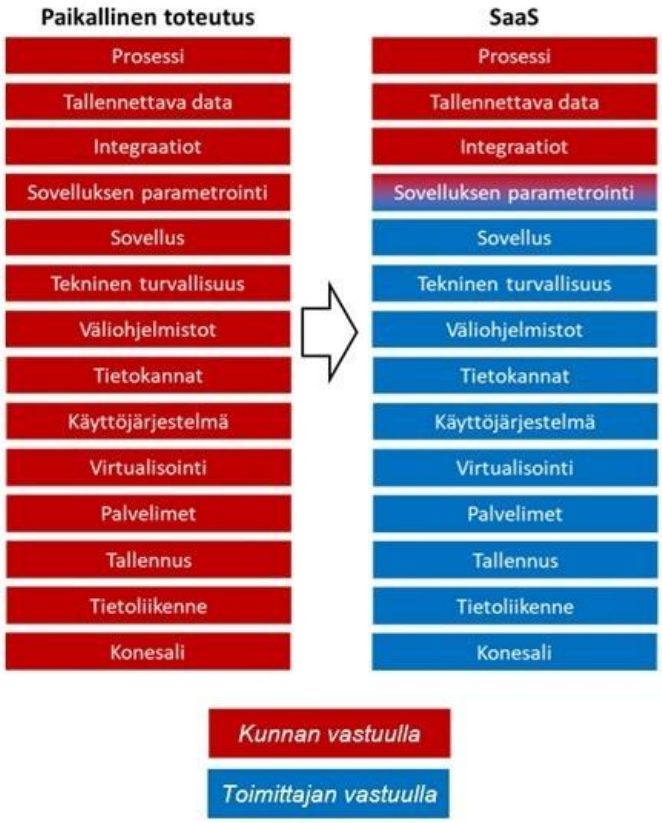
OLEMASSA OLEVAN PALVELUN SIIRTÄMINEN ON-PREMISESTÄ SAASIKSI

Mikä muuttuu siirryttäessä On-premise → SaaS?

- **Tekniset muutokset**
  - Alustamuutos
  - Kunnan sovituksen / parametroinnin siirto SaaS-alustalle
  - Datamigraatio
  - Integraatioiden uudistaminen

- **Vastuumuutokset**
  - Konesali-, käyttö- ja kapasiteettipalvelut toimittajalle
  - Alustan ja sovellusylläpidon tuen yhdistäminen, tukipyyntöjen hallinnan muutokset
  - Kapasiteetinhallinta- ja konfiguraationhallinnan vastuut toimittajalle
  - Versiojulkaisuvastuiden muutokset

Oheisessa kuvassa esitetään kunnan ja toimittajan vastuut paikallisessa toteutusmallissa ja SaaS-palvelumallissa.



On-premise -sopimusten päivittämisessä on kaksi vaihtoehtoa:

A. Laaditaan kokonaan uusi SaaS-pohjainen sopimus = muutetaan merkittävästi olemassa olevan sopimuksen rakennetta ja sisältöä
B. Lisätään ns. SaaS-hosting -sopimus olemassa olevaan sopimukseen

Molemmissa tapauksissa (erityisesti mallissa A) haasteena on se, että ne ovat yleensä hankintalain vastaisia. Erityisesti mallia A voidaan käyttää lähinnä In-house -yhtiöiltä hankittaviin sopimuksiin.

SaaS-hosting on väliaikaisratkaisu

SaaS-hosting toimii askeleena siirryttäessä perinteisestä järjestelmäratkaisusta SaaSiin. Järjestelmäsopimusten (käyttöoikeussopimusten) päivittäminen on sopimusteknisesti helpointa ns. SaaS-hosting -alasopimuksen lisäämisellä olemassa olevaan sopimukseen. SaaS-hosting on väliaikaisratkaisu, sillä usein SaaS-hostingilla ”SaaSitettu” perinteinen järjestelmä on toteutettu varsin kevyellä ja puutteellisella tuotteistuksella (palvelutasolupaukset, palvelunhallinnan prosessit sekä käytön ja sopimuksen joustamattomuus tarpeiden muuttuessa).

Jos jatkossa on tarve hankkia vielä On-premise -ratkaisuja, niihin kannattaa liittää mukaan jo valmiiksi mahdollisuus siirtyä SaaS-malliin – vähintään SaaS-hosting -malli lisäämällä.

Tarve

- On olemassa oleva järjestelmäsopimus, järjestelmä on toimitettu On-premise -mallilla
- On tarve siirtyä toimittajan SaaS-mallilla tuottamaan järjestelmään ⇒ pois On-premise -ratkaisusta

Huomioitavaa

- Tarkista hankintalain reunaehdot tähän sopimusmuutokseen – hankintalaki yleensä edellyttää, ettei sopimuskaudella saa tehdä sellaisia olennaisia sopimusmuutoksia, joiden ehtoja ei ole määritetty jo kilpailutusvaiheessa ja alkuperäisessä sopimuksessa.

Eteneminen

1. Tarkista sopimusmuutoksen hankintalainmukaisuus.
2. Arvioi tarkemmin hankittavan kokonaisuuden tietoturvallisuuden ja tietosuojan erityistarpeet ja vaatimukset (**pohja C**).
3. Käy toimittajan kanssa tarkemmin läpi heidän SaaS-ratkaisunsa ominaisuudet ja siihen liittyvät tekniset sekä riskienhallinnan ratkaisut. Tässä voit hyödyntää esimerkiksi **pilvipalvelujen soveltuvuuden tarkistuslistaa** (VM:n pohja) tai pilvipalvelujen riskiarviopohjaa (**pohja G**).
4. Kokoa vielä järjestelmän käyttöön liittyvät volyymit (esim. eri käyttäjäroolien määrät, järjestelmässä säilytettävän datan tai transaktioiden määrä).
5. Merkitse omat volyyminne hinnoittelulomakkeeseen (**pohja M**) ja toimita ko. pohja toimittajalle täytettäväksi. Käy hintakeskustelut hankintalain puitteissa.
6. Toimita toimittajalle ehdotus sopimukseen lisättävästä uudesta SaaS-hosting-palvelusopimuksesta (**pohja J**) sekä tämän liitteeksi tulevista vaatimuksista (**pohja L**).
7. Neuvottele sopimusehdot ja palvelun sisältö kuntoon.
8. Suunnittele SaaS-palvelun käyttöönotto ja migraatio On-premise-palvelusta (huom. integraatioiden uusiminen, datamigraatio, vastuiden muutokset).

9. Kokoa käyttöönottosuunnitelma projektisuunnitelman muotoon ja ota se osaksi uutta käyttöönottosopimusta (tähän voi hyödyntää **sopimusmallin H liitettä 6A**).
10. Irtisano On-premise -alustan sopimukset / palvelut käyttöönottoprojektin aikataulun mukaisesti.
11. Ota SaaS-järjestelmä käyttöön, päivitä järjestelmädokumentaatio.

Hyödynnettävät pohjat

Keskeiset pohjat:

- ➔ J: Sopimusmalli SaaS-hosting (.docx)
- ➔ L: Mallivaatimukset – SaaS-hosting (.xlsx)
- ➔ M: SaaS-hintalomake (.xlsx)
- ➔ H: Sopimusmalli, liite 6A, toimitussopimusmalli (.docx)

Bonuspohjat (käytä tarpeen mukaan):

- ➔ C: Tietoturvan, tietosuojan ja jatkuvuuden erityisvaatimusten kokoamispohja (.xlsx)
  Pilvipalvelujen soveltuvuuden tarkistuslista (.xlsx)
  Ladattavissa täältä: Pilvipalvelujen soveltamisohje, valtiovarainministeriö
- ➔ G: Pilviratkaisun riskiarviopohja (.xlsx)

Pilvipalveluiden elinkaari

PILVIPALVELUVALMIUKSIEN KEHITTÄMINEN JA PILVIPALVELUIDEN JOHTAMINEN

Kehittämisen ja johtamisen ylätason kokonaisuudessa on tarkoituksena varmistaa organisaation kyvykkyys ja rakenteet suunnitella, johtaa ja hallita pilvipalveluiden kehittämistä ja hyödyntämistä organisaatiossa.

Pilvipalveluiden johtamisessa korostuu niiden merkityksen tunnistaminen. Organisaatio voi laatia pilvistrategian, jossa määritellään, miten pilvipalveluita on tarkoitus hyödyntää organisaation toiminnassa. Pilvistrategia on hyvä kytkeä yhteen organisaation varsinaisen toiminnan strategian sekä tietohallinnon yleisen toimintamallin kanssa. Pilvistrategia on pitkän tähtäimen suunnitelma, joka pyrkii luomaan kokonaiskuvaa tulevasta suunnasta ja toimimaan ohjenuorana IT-ympäristöä kehitettäessä.

Pilvistrategian hyötyjä

- Auttaa kokonaiskuvan hahmottamisessa ja yhteisen suunnan muodostamisessa
- Auttaa arvioimaan toimittajien palveluvalikoimaa ja osaamista
- Auttaa valitsemaan kustannusnäkökulmasta parhaat ratkaisut
- Auttaa valitsemaan parhaat teknologiaratkaisut
- Varmistaa valittujen ratkaisujen yhteensopivuuden
- Mahdollistaa valittujen ratkaisujen sujuvan käyttöönoton
- Auttaa oman organisaation avainroolien tunnistamisessa ja resursoinnissa
- Auttaa oman organisaation osaamisen ja koulutustarpeiden tunnistamisessa
- Auttaa digiturvallisen pilven rakentamisessa

Keskeisimpien riskien ja niiden hallintakeinojen sekä organisaation oman toiminnan ja tarpeiden tunnistamiseksi on suositeltavaa kuvata toiminta- ja teknologiaympäristö, siihen liittyvät sopimusrakenteet ja erilaiset toimintaan ja ympäristöön liittyvät vaatimukset, kuten tietoturvallisuus ja tietosuoja. Kuvaamisessa voi hyödyntää esimerkiksi kokonaisarkkitehtuurimenetelmää ja tiedonhallintamallin tietoja.

Vinkit organisaation pilvikyvykkyyksien kehittämiseen

- Luo organisaatioosi pilvipalvelulinjaukset – tämä toimii ratkaisujen peruskivenä
- Ymmärrä (ja hyväksy) pilvipalvelujen tuoma palvelumallin muutos
- Laadi yhdessä hankintatoimen kanssa pilvipalveluihin sopivat hankintapohjat
- Jalosta tietoturva- ja tietosuojatoiminnot pilviyhteensopiviksi
- Kehitä pilviosaamistasi ja/tai hanki neutraali ja joustava kumppani SaaS-hankintoihin

Hyödynnettävät pohjat

Pilvistrategia

Pilvistrategia luo organisaatiolle sen strategiasta ja julkisen hallinnon pilviperiaatteista johdetut ylätason tavoitteet ja linjaukset pilvipalveluiden hyödyntämiseen.

> Pilvipalvelustrategia-pohja (.docx)
> Ladattavissa täältä: Pilvipalvelujen soveltamisohje, valtiovarainministeriö

Pilvipalveluiden tietoturvapolitiikka

Pilvipalveluiden tietoturvapolitiikalla luodaan tietoturvan keskeiset periaatteet.

> Pilvipalvelun tietoturvapolitiikka -pohja (.docx)
> Ladattavissa täältä: Pilvipalvelujen soveltamisohje, valtiovarainministeriö

Hyödyllistä tietoa ja lisää pohjia myös oppaan osioissa:

Arkkitehtuurin kuvaaminen
Tietosuojan vaikutustenarviointi DPIA

Yksittäisen SaaS-palvelun elinkaaren vaiheet

1) KOHTEEN MÄÄRITTELY JA RAJAUS

Tässä vaiheessa määritetään ja rajataan kehittämiskohde, johon haetaan ratkaisua. Keskeinen tavoite on saada kehittämiseen osallistuville toimijoille ja henkilöille täsmällinen ja yhtenevä kuva siitä, mitä kehitetään.

On tärkeää pohtia, mihin kaikkeen kehittäminen vaikuttaa. Kehitettävän kohteen määrittely- ja rajausvaiheen keskeisiä tehtäväkokonaisuuksia ovat:

- Suunnittelun kannalta keskeisen materiaalin kokoaminen ja aitojen toiminnan tarpeiden tunnistaminen
- Keskeisten vaatimusten toteutumisen varmistaminen (hankintaprosessissa, sopimuksissa ja auditoinnissa)
- Rajaaminen (mitä kaikkea pyritään ratkaisemaan nyt ja mitä voidaan jättää osaksi muuta kehittämistä)
- Tavoitteiden määrittely (mitä hyötyä tai arvoa kehittämisellä pyritään saamaan aikaiseksi)
- Päävaatimusten, riippuvuuksien, toiminnallisten kokonaisuuksien ja palveluiden tunnistaminen (asiakkaat tai käyttäjät, vastuut ja roolit, tietovirrat, prosessit, tiedot, järjestelmät, integraatiot, teknologiat ja laitteet) sekä ylätason vaikutustenarviointi
- Olemassa olevien sopimusten kokoaminen ja analysointi

- Keskeisten tietoturva-, tietosuoja- ja varautumisvaatimusten tunnistaminen
- Toteutustavan arviointi ja linjaaminen (esim. kehitetään itse, ostetaan järjestelmä tai tekninen ratkaisu, hankitaan koko palvelu ulkoa teknisine ratkaisuineen)

Vinkit yksittäisen SaaS-hankinnan läpivientiin

- Resursoi hankinta riittävästi
- Selvitä hankittavan kokonaisuuden erityistarpeet – erityisesti jatkuvuus, tietoturva, tietosuoja, toiminnallisuudet
- Panosta markkinakartoitukseen / esiselvitykseen ennen varsinaista hankintailmoitusta – selvitä ratkaisuvaihtoehtojen soveltuvuus tarpeeseesi – ole valmis joustamaan
- Hyödynnä valmiita sopimusmalleja, mallivaatimuksia ja arviointipohjia
- Muista: hankinta tehdään substanssitoimintaa varten, ei yleensä tietohallintoa tai tietoturvatoimintoa varten
- Etsi kompromisseja

Hyödynnettävät pohjat

Voit hyödyntää kohteen määrittelyssä esikonseptointipohjaa. Esikonseptoinnin tarkoituksena on kiteyttää ratkaisua tarvitsevan organisaation ja tietohallinnon yhteistyönä

- Mitä ollaan hankkimassa tai kehittämässä
- Mitä ongelmaa ollaan ratkaisemassa
- Mitä hankinnalla tai kehittämisellä tavoitellaan
- Mitä erityispiirteitä ratkaisussa tai hankinnassa tulee ottaa huomioon – myös SaaS-ratkaisun suhteen
- Mitä riippuvuuksia hankinnan kohteella on muihin projekteihin tai kohteisiin

➔ A: Esikonseptointipohja (.pptx)

2) KOHTEEN VAATIMUSTEN MÄÄRITTELY

Tässä vaiheessa tunnistetaan kehittämiskohteen ylätason vaatimukset, myös riskien ja varautumisen näkökulmasta.

Tässä vaiheessa tunnistetaan keskeisimmät hankinnan kohteen vaatimukset, keskeiset riskit ja riskienhallinnan päävaatimukset, joita voidaan tarkentaa myöhemmin hankintavaiheessa. Käydään läpi seuraavaa vaihetta varten pilvipalvelujen käytön tyypilliset riskit ja tarkistetaan, miten ne suhtautuvat kyseiseen kehittämiskohteeseen.

Vaatimukset tulee sovittaa kehitettävän kohteen luonteeseen ja kehitettävään tavoitteeseen. Toteutettavan ratkaisun vaatimuksia voidaan tarkastella ylätasolla seuraavista näkökulmista: strategia ja pilvistrategia, arkkitehtuuri, toiminnalliset ja tekniset vaatimukset, integraatiot, tietoturva ja tietosuoja, käyttöönotto ja toimitus, toiminnan prosessit ja käsiteltävät tiedot, jatkuvuus ja varautuminen, valmius, jatkuvat palvelut ja kehittäminen.

Voit hyödyntää kohteen vaatimusten määrittelyssä oheisia SaaSec-hankkeen ja valtiovarainministeriön pohjia ja tarkastuslistoja.

Hyödynnettävät pohjat

- ➔ C: Tietoturvan, tietosuojan ja jatkuvuuden erityisvaatimusten kokoamispohja (.xlsx)
- ➔ D: Käyttötapausten kuvauspohja (.docx)
- ➔ E: Integraatioiden kuvauspohja (.xlsx)

Hybridihankinnat – palvelut ja laitteet SaaS-hankintoina

Palveluhankinnat

Lähes kaikissa palveluhankinnoissa käsitellään tietoa ja tätä tietoa tallennetaan tietojärjestelmiin. Vaikka kunta ei olisikaan hankkimassa mitään tietojärjestelmää osana palveluhankintaa, kunnan tai kuntalaisten tietoja usein käsitellään osana palvelua palvelutoimittajan valitsemissa tietojärjestelmissä. Lisäksi palvelutoimittajan palvelussaan käyttämistä välineistä on usein kytkentöjä – integraatioita kunnan tietojärjestelmiin, esimerkiksi laskutusjärjestelmiin, kuntatietojärjestelmiin tai pääsynhallintaan. Tästä syystä myös informaatiotekniikkaa hyödyntävissä palveluhankinnoissa (ns. hybridihankinnoissa) on hyvä hallitusti huolehtia keskeisimpien teknisten sekä tietosuojaa, tietoturvaa ja jatkuvuutta koskevien päävaatimusten täyttymisestä.

Hybridihankintoja voi olla joskus vaikea tunnistaa. Esimerkiksi jo olemassa olevan ratkaisun digitalisointi voi näyttäytyä vain palveluhankintana, jota ei ehkä pidetä IT-hankintana. Usein kuitenkin näissä hankinnoissa esimerkiksi palvelutasojen, saavutettavuuden, tietoturvan, tietosuojan ja datan omistajuuden tai datan käsittelyn merkitys on keskeinen.

Laite- ja tavarahankinnat

Verkkoyhteydet, erilaiset verkottuneet laitteet, ohjelmistot ja data ovat tulleet osaksi hyvin perinteisiä työkaluja. Yhä useammat perinteiset laitteet ja ratkaisut ovat jollain tapaa verkottuneita ja kokoavat dataa, joka toimitetaan joko suoraan hankintayksikölle tai pilvipalveluun toimittajan valitsemaan ratkaisuun. Laitteet, tarvikkeet ja ratkaisut voivat sisältää sellaisia toiminnallisuuksia, joihin tarvitaan esimerkiksi liityntää kunnan ICT-järjestelmiin. Usein niissä myös käsitellään arkaluontoista dataa, kuten henkilötietoja.

Jos et ole varma, onko palvelu-, laite- tai tavarahankinnassasi edellä kuvattuja ns. hybridihankinnan piirteitä, ole yhteydessä kuntasi tietohallintoon, jolloin asiaa voidaan arvioida yhdessä.

Hyödynnettävät pohjat

Tällaisissa ns. hybridihankinnoissa voit hyödyntää SaaSec-hankkeen pohjaa:

➔ B: Hybridihankintojen tarkistuslista ja tiivisvaatimukset (.xlsx)

Pilvipalvelujen yleiset riskit ja kontrollit -pohja

Pohjaan on koottu listaus tyypillisistä pilvipalveluiden riskeistä ja yleisistä niihin liittyvistä kontrolleista. Nämä tulee aina käsitellä ja tarkentaa tapauskohtaisesti. Pohjaa voidaan hyödyntää tunnistettaessa kehitettävän kohteen vaatimuksia. Tyypillisiä pilvipalveluriskejä voidaan verrata kohteen vaatimusten näkökulmasta vaiheessa 3) Ratkaisuvaihtoehtojen arviointi.

> Pilvipalvelujen yleiset riskit ja kontrollit -pohja (.xlsx)
> Ladattavissa täältä: Pilvipalvelujen soveltamisohje, valtiovarainministeriö

Pilvipalvelujen riskienhallinnan vaatimusten tunnistamispohja

Pohjaan on koottu tyypillisiä tarkastelunäkökulmia ja kysymyksiä, joiden avulla voidaan tunnistaa kehitettävän tai hankittavan kohteen riskienhallintaan liittyviä vaatimuksia. Listaa voidaan täydentää kehitettävän kohteen ja toiminnan erityispiirteiden pohjalta.

> Pilvipalvelujen riskienhallinnan vaatimusten tunnistamispohja (.xlsx)
> Ladattavissa täältä: Pilvipalvelujen soveltamisohje, valtiovarainministeriö

Oppaan sivulla ”Arkkitehtuurin kuvaaminen” voit perehtyä arkkitehtuurin kuvaamisen hyötyihin osana hankintaan liittyvää määrittelyä ja ottaa mallipohjat käyttöösi.

Arkkitehtuurin kuvaaminen

Oppaan sivulta ”Tarjouspyyntö” löydät tietoa tarjouspyynnön laatimisesta ja kokoamisesta, vaatimusmäärittelyn tarkentamisesta ja muista tarjouspyynnön liitteistä.

Tarjouspyyntö

3) RATKAISUVAIHTOEHTOJEN ARVIOINTI

Tässä vaiheessa tunnistetaan ja selvitetään ratkaisuvaihtoehtoja ja vertaillaan pilvipalveluita, jotka täyttävät kehittämiskohteelle asetetut vaatimukset.

Hankinnan kohde ja se, kuinka valmiiksi hankinnan kohde on jo määritelty ja kuvattu, ratkaisevat, millä tavoin ratkaisuvaihtoehtojen arviointi on järkevää toteuttaa. **Markkinakartoituksella** tarkoitetaan yleisesti kaikkea sitä markkinoilla olevan tiedon selvittämistä, jota hankintayksikön on mahdollista saada ja hyödyntää hankintaa suunnitellessaan ja valmistellessaan. Ohjeita ja reunaehtoja markkinakartoituksen toteuttamiseen asettaa ns. hankintalaki eli Laki julkisista

hankinnoista ja käyttöoikeussopimuksista (1397/2016). **Markkinavuoropuhelu** tarkoittaa markkinoiden kartoittamiseksi järjestettäviä tapaamisia potentiaalisten tarjoajien kanssa sekä hankinta-asiakirjojen tai muun materiaalin kommentointikierrosta tarjoajien kanssa.
(Lähde: KEINO-osaamiskeskus)

Markkinakartoitus

Menetelmiä markkinakartoituksen tekemiseen:

- Kirjallinen tutkimus, mitä markkinoilta on saatavissa
- Analyysi vertaisryhmien tai muiden julkisten organisaatioiden kokemuksista
- Itsenäinen tutustuminen ratkaisujen ominaisuuksiin, sopimusehtoihin ja teknisiin kuvauksiin
- Kokeileva eteneminen: ratkaisujen itsenäinen demoaminen ja kokemusten dokumentointi
- Toimittajatapaamiset, joissa toimittajat esittelevät omia ratkaisumallejaan

Markkinavuoropuhelu

Markkinavuoropuhelua voidaan käydä monin eri tavoin, kuten kaikille avoimina tai rajattuina infotilaisuuksina, kirjallisina kommentointipyyntöinä, tietopyyntöinä ja kahdenvälisinä keskusteluina. Toimittajia voidaan kutsua mukaan vuoropuheluun esimerkiksi julkaisemalla ennakkoilmoituksia.

Huomioitavaa: Kaikille vuoropuheluun osallistuville tulee toimittaa samat tiedot valmisteilla olevasta hankinnasta. Vuoropuhelun tulee aina olla tasapuolista ja läpinäkyvää. Keskustelut tulee dokumentoida kirjallisesti.

Tutustu tarkemmin markkinakartoituksen ja -vuoropuhelun suunnitteluun ja toteuttamiseen KEINO-osaamiskeskuksen tuottaman kattavan ”Hankinnan markkinakartoitus” -oppaan avulla oheisesta linkistä:

Hankinnan markkinakartoitus

Hyödynnettävät pohjat

➔ F: Hinnan kokoluokka-arviopohja (.xlsx)
➔ G: Pilviratkaisun riskiarviopohja (.xlsx)
Pilvipalvelujen soveltuvuuden tarkistuslista (.xlsx)
Ladattavissa täältä: Pilvipalvelujen soveltamisohje, valtiovarainministeriö

Hyödyllistä tietoa ja lisää pohjia myös oppaan osioissa:

Tietosuojan vaikutustenarviointi DPIA
PiTuKri - vaatimukset ja vastuut

4) HANKINTA JA SOPIMUS

Tässä vaiheessa kilpailutetaan ja hankitaan pilvipalveluratkaisu. Huomioidaan pilvipalveluiden hankinnan erityispiirteet, lainsäädännölliset vaatimukset ja sopimukselliset haasteet.

Tehtäväkokonaisuudet

- Keskeisten riskienhallinnan vaatimusten määrittäminen (tietoturva, henkilötietojen käsittely, jatkuvuus) jo tarjouspyyntöön
- Toimittajien sopimusehtoihin tutustuminen ja vertailu
- Asiakkaan kannalta keskeisten ja ehdottomien sopimusehtojen listaaminen
- Yhteisen tiiviin sopimusmallin luonti, mikäli mahdollista
- Omien (riskienhallinnan) vaatimusten ottaminen osaksi sopimusta

Vaatimukset jo tarjouspyyntöön

Tarjouspyyntöön on hyvä koota riskienhallinnasta, pilvipalvelujen tyypillisistä riskitekijöistä ja PiTuKri-kriteeristöstä täsmällinen lista tarjottavaa ratkaisua ja siihen liittyvää palvelua koskevista vaatimuksista. Vaatimukset on hyvä jakaa pakollisiin vaatimuksiin ja pisteytettäviin, ei-pakollisiin vaatimuksiin. Vaatimuksia luokiteltaessa on tärkeää huomioida, että julkisissa hankinnoissa tarjoukset on lähes poikkeuksetta hylättävä, jos tarjous ei täytä jokaista pakollista vaatimusta. Tästä syystä tulee välttää sellaisia pakollisia vaatimuksia, joita ei aidosti tarvita pakollisina. Tarjouspyyntöön tuotetut vaatimukset tulee hankintapäätöksen jälkeen sisällyttää myös solmittavaan sopimukseen. *(Lähde: Pilvipalvelujen soveltamisohje)*

Pilvipalvelujen soveltamisohjeen suositukset

- Tunnista pilvipalvelujen hankkimisen periaatteiden ero perinteisiin hankintoihin verrattuna – erityisesti globaalit pilvipalvelut eivät juuri pysty tinkimään vakiosopimusmalleistaan tai toimitusehdoistaan.
- Tee vaatimusmäärittely huolellisesti, hyödynnä SaaSec-hankintapohjia soveltaen
- Muista, että palveluntoimittajat harvoin pystyvät tinkimään omista toimitus- ja sopimusehdoistaan. Tutustu eri palveluntoimittajien ehtoihin ja luo tiivis sopimusmalli tai listaa vain keskeisimmät sopimusehdot, joista et voi tinkiä.
- Arvioi, voitko hyödyntää yhteishankintayksikön tai sidosyksiköiden olemassa olevia sopimuksia.
- Jos olet hankkimassa laajoja SaaS-palveluja, tutustu toimitusmalliin – mikä on paikallisten integraattorien ja palveluntoimittajien keskinäinen roolitus ja miten tämä vaikuttaa tulevan sopimuksen rakenteeseen.
- Varmista keskeisten riskien hallintakeinot määrittämällä riittävä, mutta ei liioiteltu joukko tietoturvaa, henkilötietojen käsittelyä ja jatkuvuutta koskevia vaatimuksia tarjouspyyntöön. Hyödynnä tässä hankinnan kohteeseen ja sen suojaustarpeisiin sovitettuja vaatimuksia. Hyödynnä tarpeen mukaan myös PiTuKri-kriteeristöä.
- Muista ottaa vaatimukset osaksi sopimusta.

Tiedonhallintalautakunnan suositukset

Valtiovarainministeriön yhteydessä toimiva julkisen hallinnon tiedonhallintalautakunta suosittelee tarkistamaan, että vähintään seuraavat tietoturvallisuuteen ja tietosuojaan liittyvät asiat on kirjattu pääsopimukseen:

- Oikeus tarkastaa kohteen kannalta riittävät tietoturvallisuusjärjestelyt
- Tietoturvallisuuden vastuuhenkilöt yhteystiedoissa
- Sopimuksen ja liitteiden soveltamisjärjestyksen huomiointi (erityisesti tietoturva- ja tietosuojaliitteet)
- Riittävät sakko- ja vahingonkorvauslausekkeet (myös tietoturvallisuus- ja tietosuojavaatimuksiin liittyvissä poikkeamissa)
- Millainen purku- tai välittömän irtisanomisen ehto liittyy tietoturvallisuusliitteen velvoitteen rikkomiseen
- Tietojen sijainti/käsittely Suomessa ja ETA-alueella
- Mahdollisten yrityskauppatilanteiden huomiointi

Vaiheessa ”4) Hankinta ja sopimus” hyödynnettävät pohjat täyttöohjeineen löytyvät oppaan osioista:

Tarjouspyyntö
Pääkäyttötilanteet
PiTuKri - vaatimukset ja vastuut

5) PALVELUN TOTEUTUS JA MUUTOSTEN HALLINTA

Tässä vaiheessa on tavoitteena hallita pilvipalvelun käyttöä turvallisesti koko pilvipalvelun käytön ajan, huomioiden mahdolliset muutokset ja päivitykset.

Palvelun käyttöönotto ja ylläpito huomioidaan jo kilpailutusdokumenteissa

Pilvipalvelun käyttöönottoon ja ylläpitoon liittyvät tehtävät ja vastuut on suositeltavaa huomioida jo hankinnan kohteen vaatimusten määrittelyssä ja kilpailutusdokumenteissa, joista vaatimukset siirretään sopimusasiakirjoihin. Palvelun käyttöönotto kannattaakin aloittaa sopimuksen tarkastelulla ja varmistaa, että kaikki tietoturvaan, jatkuvuuteen, teknisiin vaatimuksiin sekä toiminnallisuuksiin liittyvät sovitut toimenpiteet täyttyvät myös todellisuudessa. Sopimuksenmukaisuuden seurantaa ja vaatimusten toteutumista on hyvä jatkaa koko palvelun käytön ajan. Poikkeamiin kannattaa reagoida nopeasti ja muuttaa rohkeasti kurssia, jos siihen on tarve.

Sopimuksen vaatimukset voi tarkistaa osana määrittelyä ja testausta, tutustumalla palvelusta aikaisemmin tehtyihin auditointeihin sekä toimittajan toimittamaan dokumentaatioon ja kuvauksiin kontrolleista. Vaatimustenmukaisuuden tarkistuksen tulisi olla käyttöönoton hyväksymisen keskeinen kriteeri.

Tietoturvallisuuden huomioimisen tarkastuslista palvelun käytön aikana

- Tietoturvallisuuden jatkuva hallinta
    - Sopimukselliset tarkastukset palveluntoimittajan kanssa
    - Säännölliset tietoturva-auditoinnit ja haavoittuvuuksien tarkistukset

- Käyttöoikeuksien ja käyttäjäroolien hallinta
    - Määrittele selkeät käyttöoikeudet ja vastuut
    - Varmista, että käyttäjien pääsynhallinta on ajantasaista ja tarpeenmukaista

- Tunnistautuminen
    - Monivaiheinen tunnistautuminen (MFA) suositeltavaa
    - Vahvat salasanavaatimukset käyttäjille

- Lokien hallinta
    - Kerää ja tallenna lokitiedot turvallisesti
    - Seuraa ja analysoi lokia mahdollisten uhkien havaitsemiseksi

- Matalan kynnyksen tuki
    - Tarjoa koulutusta ja tukipalveluita käyttäjille
    - Luo helppoja tapoja raportoida mahdollisista tietoturvaongelmista

- Operatiivinen hallinta
    - Päivitä arkkitehtuurikuvaukset uuden palvelun käyttöönoton ja muutosten yhteydessä
    - Pidä sopimukset ja lisenssit ajan tasalla
    - Seuraa ja hallinnoi kustannuksia
    - Dokumentoi muutokset ja poikkeamat käytännöissä
    - Huomioi tiedonohjaussuunnitelman mukaiset tallennettavien asiakirjojen ja aineistojen säilytystä ja hävittämistä koskevat määräykset

Huomioitavaa: SaaS-palvelussa suuri osa turvallisuudesta on palveluntoimittajan vastuulla, mutta tämä ei kuitenkaan vapauta kuntaa vastuusta tietoturvan, varautumisen, jatkuvuudenhallinnan ja tietosuojan suhteen.

Tähän oppaaseen on koottu hyödyllistä tietoa SaaS-palvelun tietoturvallisen käyttöönoton ja hallinnan tueksi. Alla olevista linkeistä voit tutustua esimerkiksi tietoturvallisuuden arviointiin eri kriteeristöjen avulla, arkkitehtuurikuvausten päivittämiseen käyttöönoton yhteydessä ja RACI-taulukon hyödyntämiseen vastuiden ja roolien määrittelyssä.

Tietoturvallisuuden arviointi
Arkkitehtuurin kuvaaminen
RACI-vastuunjakotaulukko

SaaS-palvelun tietoturvallisen käyttöönoton, toteutuksen ja muutosten hallinnan tukena kannattaa hyödyntää DVV:n tuottamaa opasta ”Digitaalisen turvallisuuden arkkitehtuuri”, joka avautuu oheisesta linkkipainikkeesta.

Digitaalisen turvallisuuden arkkitehtuuri

Mikäli SaaS-palveluun ei ole tehty tietosuojaa koskevaa vaikutustenarviointia (DPIA = Data Protection Impact Assessment) hankintaprosessin aiemmissa vaiheissa, tulee se tehdä palvelun käyttöönoton yhteydessä. Näin pystytään tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Tarkemmin DPIA:n tekemiseen voi perehtyä oheisen linkkipainikkeen kautta tässä oppaassa.

Tietosuojan vaikutustenarviointi DPIA

6) PALVELUN PÄÄTTÄMINEN TAI SIIRTO

Tässä vaiheessa huolehditaan käytössä olleen pilvipalvelun hallitusta ja turvallisesta päättämisestä sekä jatkossa tarvittavien tietojen talteen ottamisesta.

Tehtäväkokonaisuudet:

- Sopimuksen irtisanominen sopimusehtojen mukaisesti
- Pilvipalvelun alasajo organisaatiossa
- Pilvipalveluun tallennetun aineiston taltiointi, siirtäminen ja/tai hävittäminen asianmukaisesti
- Jäljitettävyyden varmistaminen (henkilötietojen käsittelylokin tallentaminen)
- Tietoturvasta, tietosuojasta ja varautumisesta huolehtiminen
- Viestintä

Palvelun päättymisen syyt

Pilvipalvelun päättäminen voidaan tehdä useammasta syystä. Palvelun päättymisen syitä voivat olla esimerkiksi:

1. **Asiakaslähtöinen muutos**

- Tarve loppuu ⇒ ei siirretä toiseen järjestelmään
- Teknologinen muutos ⇒ palvelusta toiseen tai omaan järjestelmään siirtyminen
- Kilpailutuksen tulos ⇒ palvelusta toiseen tai omaan järjestelmään siirtyminen

2. **Toimittajalähtöinen muutos**

- Palvelun toimitus päättyy
    - Toimittajan asettama määräaika
    - Palvelusta toiseen tai omaan järjestelmään siirtyminen
- Sopimus irtisanotaan muista syistä
    - Taustalla olevat syyt?
    - Palvelusta toiseen tai omaan järjestelmään siirtyminen

- Toiminnan päättyminen (konkurssi tms.)
    - Toimittajan konkurssi tai muu toiminnan estää syy tulee usein yllättäen eikä hallittua siirtymää voida tehdä. Suosituksena on tehdä riskiarvio tilanteesta ja suunnitella toimet poikkeustilanteeseen.

Alasajosuunnitelma

Palvelun päättäminen tulee aloittaa huolellisella alasajosuunnittelulla. Suunnittelun aluksi on hyvä tarkistaa sopimuksesta palvelun irtisanomista koskevat ehdot sekä muut mahdolliset vaatimukset palvelun päättämisen käytännön tehtäville ja vastuille. Irtisanomisilmoitus tulee tehdä aina kirjallisena ja pyytää toimittajalta kuittaus ilmoituksen vastaanottamisesta. Mikäli pilvipalvelu vaihdetaan toiseen palveluun, tulee tässä vaiheessa varmistaa, että myös korvaavasta palvelusta on tehty tai viimeistään tässä vaiheessa tehdään asianmukainen sopimus.

Alasajosuunnitelmassa on hyödyllistä kuvata ainakin seuraavat osa-alueet:

- Tavoitteet
- Roolitus, organisointi ja vastuutus
- Vaiheistus ja aikataulu
- Tehtävien tarkempi kuvaaminen
- Tuotokset ja tulokset
- Kustannukset ja työmäärät
- Keskeisimmät palvelun alasajon riskit ja niiden hallinta
- Alasajon ohjaus, seuranta ja raportointi

Hyödynnettävät pohjat

Pilvipalvelujen päättämisen tarkistuslista

Pilvipalvelujen päättämisen tarkistuslistan avulla voidaan seurata kaikkein keskeisimpien ja yleisimpien tehtävien toteutumista palvelun alasajon yhteydessä.

> Pilvipalvelujen päättämisen tarkistuslista (.xlsx)
> Ladattavissa täältä: Pilvipalvelujen soveltamisohje, valtiovarainministeriö

RACIn käyttö pilvipalvelun päättämisen yhteydessä

Alasajosuunnitelman tehtävien vastuuttaminen on olennaisen tärkeää. Roolien ja vastuiden määrittelyssä voi käyttää apuna RACI-vastuunjakotaulukkoa. Voit tutustua RACI-malliin oheisen linkin kautta tässä oppaassa.

RACI-vastuunjakotaulukko

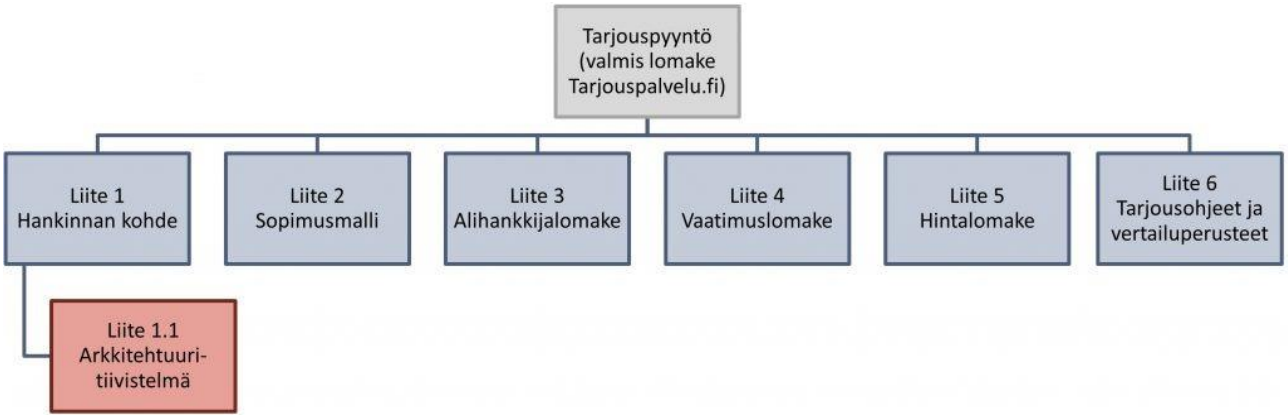
SaaS-palvelun digitaalinen turvallisuus aiheittain

TARJOUSPYYNTÖ

Tältä sivulta löydät tietoa tarjouspyynnön laatimisesta ja kokoamisesta, vaatimusmäärittelyn tarkentamisesta ja muista tarjouspyynnön liitteistä. SaaSec-hankkeessa tuotetut pohjat täydentävät valtiovarainministeriön ohjeita pilvipalveluiden hyödyntämisestä. Voit ladata pohjia omaan käyttöösi.

Tarjouspyynnön rakenne

SaaSec-hankkeen hankintapohjat on jäsennetty alla olevan varsin yleisen tarjouspyyntörakenteen mukaisesti. Tässä ohjeessa ei käsitellä ”Tarjouspyyntö (valmis lomake Tarjouspalvelu.fi)” -kohtaa, sillä lähes aina varsinainen tarjouspyyntö laaditaan Cloudian Tarjouspalvelu.fi -portaaliin vakiomuotoon. Tarjouspalvelu.fi:n tarjouspyyntölomake sisältää lähinnä hankintajuridisia osuuksia ja vain otteita varsinaisesta hankinnan sisällöstä. SaaSec-hanke suosittelee, että varsinainen hankinnan sisältö laaditaan liitteisiin 1-5 (katso alla oleva kuvio). Tarjouspyyntöön tuotetut vaatimukset tulee hankintapäätöksen jälkeen sisällyttää myös solmittavaan sopimukseen.



Kuviosta voi myös havaita, kuinka arkkitehtuurikuvaukset liittyvät osaksi tarjouspyyntöä SaaS-palvelun hankinnassa (*Liite 1.1 Arkkitehtuuritiivistelmä*). Arkkitehtuurikuvausten käyttö SaaS-palveluiden hankintojen tukena parantaa sekä hankkivan organisaation että tarjoajan/toimittajan ymmärrystä siitä, mitä hankinnassa ollaan hankkimassa, mitä toimintaa hankittava ratkaisu tukee ja minkälaiseen ympäristöön hankittava kohde sijoittuu, eli mitä hankittavalta ratkaisulta odotetaan.

Arkkitehtuurin kuvaaminen

VAATIMUSMÄÄRITTELY

Tässä vaiheessa vaatimusmäärittely tarkennetaan täsmälliseksi ja kattavaksi. Tarkista, että vaatimusmäärittely ja tarjouspyyntö vastaavat toiminnan tarpeita. Arvioi tarkasti, mutta kriittisesti pakollisia toiminnallisia vaatimuksia sekä muita vaatimuksia, jotka vaikuttavat toiminnan tavoitteisiin. Vältä tarpeettomia pakollisia vaatimuksia ja muuta ne pisteytettäviksi vaatimuksiksi. Muista myös, että globaalien pilvitoimittajien yleisiin sopimusehtoihin voidaan saada olennaisia muutoksia vain erityistapauksissa.

Hyödynnettävät pohjat

➔ K: Vaatimuslomakepohja (.xls) (tarjouspyynnön liite 4)

Tässä dokumentissa kuvataan toimittajan asiakkaalle tarjoaman palvelun ja toimituksen sisältöä ja laatua koskevat vaatimukset ja selvityspyynnöt. Tämä dokumentti ja tarjoajien näihin antamat vastaukset muodostavat keskeiset arviointi- ja vertailuperusteet tarjouspyynnössä esitetyllä tavalla.

Vaatimuslomakkeen rakenne:

1. Palveluyhteistyö, tietoturva, tietosuoja
2. Toiminnalliset vaatimukset
3. Tekniset vaatimukset
4. Tuki ja ylläpito
5. Käyttöönotto
6. Asiantuntijapalvelut
7. Saavutettavuus ja käytettävyys

Hyödyllistä tietoa vaatimusmäärittelyn laatimisen tueksi

Hyvän vaatimusmäärittelyn tunnusmerkkejä

- Vaatimukset on muotoiltu täsmällisesti ja yksityiskohtaisesti
- Vaatimukset EIVÄT ole passiivimuodossa – tehdään, toimitetaan
- Vaatimukset on selkeästi jaettu pakollisiin ja pisteytettäviin
- Vaatimukset on ylätasolla jäsennetty selkeisiin pääluokkiin
- Vaatimukset on jäsennetty selkeisiin alaluokkiin / ryhmiin
- Myös käytettävyydelle ja saavutettavuudelle on asetettu vaatimuksia / selvityspyyntöjä
- Vaatimuksissa hyödynnetään yleisiä tai toimialan standardeja (esim. Vahti, JHS-suositukset, Inspire)
- Vaatimukset on validoitu – haluammeko me aidosti tätä vaatimusta vai ”tämä me on aina laitettu mukaan”
- Vaatimuslistaus on kattava
- Vaatimusmäärittelyä on täydennetty prosessikuvauksilla
- Vaatimusmäärittelyä on täydennetty käyttötapauksilla

- Vaatimusmäärittelyä on täydennetty arkkitehtuurikuvauksilla

Vaatimusmäärittelyssä tulee vaatia

Vaatimusmäärittelyssä tulee oikeasti vaatia jotakin – käytä tähän aikaa ja vaivaa

- Älä jätä liian paljon avoimeksi. Osa tarjoajista osaa hyödyntää vaatimusmäärittelyn puutteita ja painaa keinotekoisesti hintaa näin alas: ”Pyysitte autoa, mutta ette erikseen vaatineet siihen rattia. Sen ratin saa kyllä lisähintaan myöhemmin.”
- Liian avoimet vaatimukset johtavat siihen, etteivät tarjoukset ole vertailukelpoisia eikä niistä saa selvää, mitä ne tarkkaan ottaen tarjottuun hintaan sisältävät.

Pakolliset ja ei-pakolliset vaatimukset

Kuvaa tarkasti ja yksilöiden, mitkä vaatimukset ovat pakollisia ja mitkä pisteytettäviä.

- **Hankintalain mukaan jokainen pakollinen vaatimus tulee täyttää**
- **Tarjous, jossa on puute yhdessäkin pakollisessa vaatimuksessa, on aivan pakko hylätä**

- Tästä syystä on oltava tarkkana, miten pakolliset vaatimukset muotoillaan. Jos vaatimusmäärittelyssä on yksikin vaatimus, jota kukaan tarjoaja ei täytä, tarjouskilpailu menee uusiksi.
- Huom. Pakollista vaatimusta ei saa muiden arvioitavien seikkojen joukossa enää pisteyttää. Ole tarkkana tässäkin. Älä laadi edes osittain päällekkäisiä pakollisia ja pisteytettäviä vaatimuksia.

Mihin vaatimusmäärittelyä ja tarkkoja vaatimuksia itse asiassa tarvitaan?

1. Kattavalla vaatimusmäärittelyllä saadaan toimittajille hyvä kuva, mitä oikein halutaan.
2. Kattava vaatimusmäärittely asettaa tarjoukset ”samalle viivalle”. Niiden sisällöt vastaavat toisiaan ja pystytään vertaamaan ”omenoita omenoihin” eikä ”omenoita appelsiineihin”.
3. Saadaan ymmärrys (pisteytettävissä vaatimuksissa), mitkä vaatimukset/toiminnallisuudet kuuluvat toimitettuun kokonaisuuteen ja mitkä eivät.
4. Saadaan yksityiskohtaiset vaatimukset sopimuksiin – joihin voidaan palata sopimuskaudella.
5. Saadaan ko. vaatimukset ja vaatimusten mukainen palvelu **kuulumaan annettuun tarjoushintaan** – kaikki toimittajat jättävät kaiken muun kuin vaaditun ”erillishinnoiteltavaksi” sopimuskaudella.

- **Mieluummin yksityiskohtainen joukko vaatimuksia, kuin löysät yleisvaatimukset**

- Tilanne on kuitenkin toinen ketterän kehittämisen hankinnassa
- SaaS-hankinnoissa tulee välttää alustan teknisten ratkaisujen yksityiskohtia koskevia vaatimuksia

Vaatimusten muotoilu

Hyvä vaatimus on kuvattu täsmällisesti, ilman porsaanreikiä ja aktiivimuodossa

- Muista, että vaatimukset viedään lopulta sopimukseen
- Kirjoita vaatimukset vaatimusten muotoon:
    - ”Tarjotun ratkaisun tulee sisältää…” tai ”tarjoajan prosessin tulee kattaa X” tai ”Toimituksen tulee sisältää” – ei muodossa ”laadukas tuote”, josta ei käy ilmi, ketä vaatimus koskee, onko se edes vaatimus ja miten määritetään laadukas.
    - Vältä passiivimuotoja: toteutetaan, kuvataan, mallinnetaan tms., koska siitä ei sopimuksessa käy ilmi, kenen vastuulla ko. kokonaisuus on.

Toiminnallisissa vaatimuksissa on hyvä muistaa vaatia, että vaatimus ei koske pelkästään ”järjestelmän kyvykkyyttä” vaan että ”toimitus sisältää XYZ”

- Joskus kannattaa jakaa tämä kahteen vaatimukseen: ”Järjestelmällä on mahdollista kuvata XXX” ja ”Järjestelmätoimituksen tulee sisältää kuvauksen YYY toteutus”
- Kannattaa myös yleisesti kuvata, että Kyllä-vastattujen vaatimusten tulee kuulua tarjoushintaan

Toiminnallisissa vaatimuksissa joskus vielä pyydetään kuvaamaan valmiusaste

- Vakiotoiminnallisuus, asiakkaalle parametroitava, räätälöitävä, ei sisälly

Toiminnalliset vaatimukset

- Toiminnalliset vaatimukset ovat toimialalle keskeisimmät. Toiminnallisia vaatimuksia ovat sellaiset vaatimukset, jotka kuvaavat, mitä hankittavalla tietojärjestelmällä tulee pystyä tekemään = mitä toiminnallisuuksia siinä pitää olla.
- Toiminnalliset vaatimukset sisältävät suorat toiminnallisuuksia koskevat vaatimukset. Esimerkkejä:
    - ”Järjestelmällä tulee pystyä hyväksymään vielä hyväksymättömiä asiakirjoja hyväksytyksi”
    - ”Vain kyseisen prosessin hyväksyjäroolissa olevat käyttäjät voivat hyväksyä asiakirjoja”
    - ”Järjestelmään on mahdollista määrittää rajoitus, että asiakirjan hyväksyminen edellyttää kahden hyväksyjäkäyttäjän hyväksyntää, ennen kuin asiakirja tulee järjestelmässä hyväksytyksi”
    - ”Hyväksyttyä asiakirjaa ei tule pystyä muokkaamaan järjestelmän toiminnallisuksilla”
- Toiminnalliset vaatimukset sisältävät sellaiset teknisluontoiset toiminnallisuudet, jotka kuvaavat järjestelmän kyvykkyyksiä (näitäkin järjestelmän pitää pystyä tekemään). Esimerkkejä:
    - Käyttövaltuushallinta
    - Raporttienhallinta
    - Arkistointikyky
    - Lokitus (*

*) Lokituksessa kyky lokittaa on toiminnallinen vaatimus, mutta lokia koskeva teknologia (esim. salausteknologia) on tekninen vaatimus

➔ L: Mallivaatimukset – SaaS-hosting (.xlsx)

Huom. Pohja L on tarkoitettu hyödynnettäväksi pääkäyttötilanteessa ”Olemassa olevan palvelun siirtäminen On-premisestä SaaSiksi”.

➔ M: SaaS-hintalomake (.xlsx) (tarjouspyynnön liite 5)
➔ N: Hankinnan kohde -kuvauspohja (.docx) (tarjouspyynnön liite 1)
➔ P: Tarjousohjeet ja vertailuperusteet (.docx) (tarjouspyynnön liite 6)

ARKKITEHTUURIN KUVAAMINEN

Hankinnan kohteena oleva SaaS-ratkaisu sijoittuu aina osaksi laajempaa toimintaympäristöä. Hankinnan onnistumisen kannalta on olennaista, että tämä kokonaisuus kuvataan jo tarjouspyynnön liitteeksi. Kokonaisarkkitehtuurin kuvauksia voidaan hyödyntää osana hankintaan liittyvää määrittelyä.

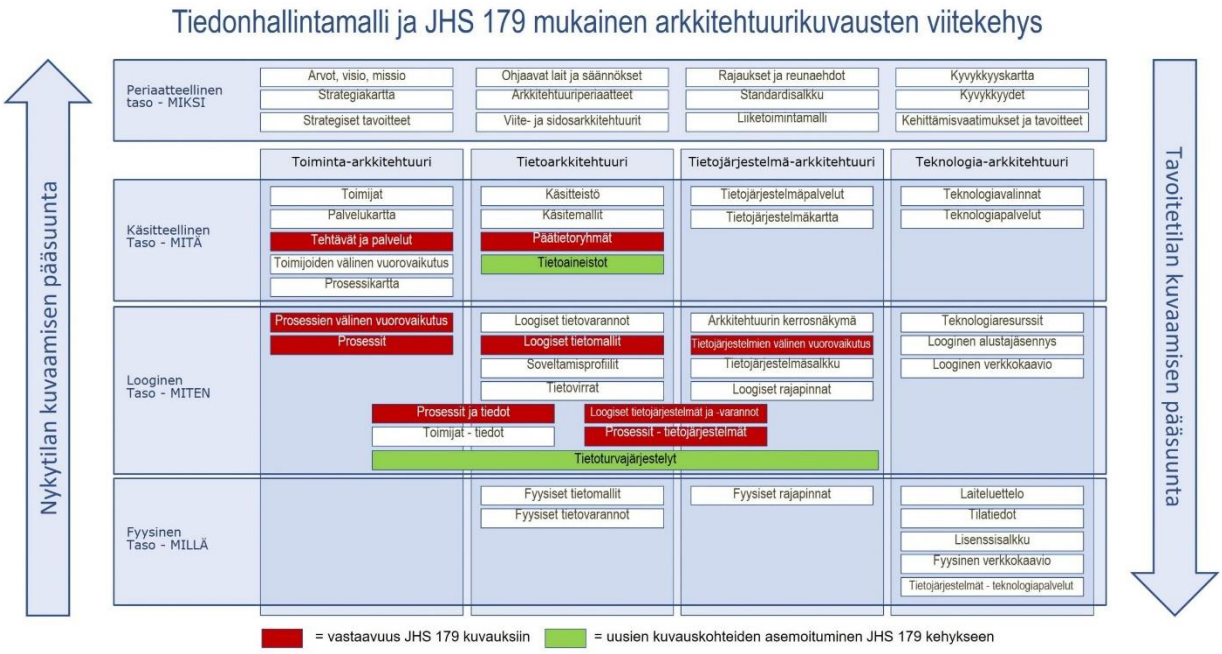
Kokonaisarkkitehtuuri (KA) kuvaa sitä, miten organisaation tietojärjestelmät, toimintaprosessit, rakenteet ja ihmiset toimivat kokonaisuutena. Se on systemaattinen lähestymistapa organisaation toiminnan ja sen rakenteiden jäsentämiseen, kehittämiseen ja hallinnoimiseen.

Kokonaisarkkitehtuurin avulla voidaan luoda toiminnallis-tekninen ympäristö, jossa kaikki osat sopivat toisiinsa, keskeiset komponentit tarvitsee toteuttaa vain kerran (uudelleenkäytettävyys) ja joka on hallittavissa ja muunneltavissa toiminnan muuttuvien tarpeiden mukaan.

Kokonaisarkkitehtuuri ja tiedonhallintamalli

Julkishallinnon toimijoita suositeltiin vuodesta 2011 lähtien kuvaamaan kokonaisarkkitehtuuriaan tietohallintolain mukaan. Tietohallintolaissa näitä kuvauksia ohjasi JHS 179 -suositus. Tammikuussa 2020 voimaan tullut tiedonhallintalaki korvasi vanhan tietohallintolain. Tiedonhallintalaki ei enää suosittele organisaatioita kuvaamaan kokonaisarkkitehtuuria, vaan se vaatii tiedonhallintayksiköitä (eli lain piirissä olevia julkishallinnon organisaatioita) toteuttamaan tiedonhallinnan kuvaukset tiedonhallintamallin muodossa. Menetelmänä arkkitehtuuri ei kuitenkaan poistu tiedonhallintalain myötä, vaan tiedonhallintamallin kuvaamisessa voidaan hyödyntää arkkitehtuurin kuvaamisen menetelmiä.

Alla oleva valtiovarainministeriön tuottama kuvauskehys esittää tiedonhallintamallin ja kokonaisarkkitehtuurin yhteyden:



Lisätietoa kokonaisarkkitehtuurista: näkökulmat ja tasot

Kokonaisarkkitehtuurin näkökulmat

Kokonaisarkkitehtuurissa asioita tarkastellaan neljästä keskeisestä näkökulmasta, jotka ovat:

1. Toiminta-arkkitehtuuri
Toiminta-arkkitehtuurin näkökulma sisältää organisaation kannalta merkittävimmät ulospäin näkyvät asiat eli toimijat, toiminnan palvelut ja toimijoiden välisen vuorovaikutuksen. Toimijoihin kuuluvat organisaation asiakkaat eli tahot, joille organisaatio tarjoaa palveluitaan. Toimijoita ovat myös sisäiset osapuolet eli työntekijät sekä prosessien eri vaiheissa mukana olevat kumppanit, yritykset, alihankkijat, naapurikunnat, valtio jne. Toimintanäkökulmassa huomioidaan myös prosessit, palvelupolut ja toimintatavat, joiden tuella organisaatio tuottaa palveluitaan.

2. Tietoarkkitehtuuri
Tietoarkkitehtuuri kuvaa organisaation käyttämät tiedot sekä niiden rakenteet ja suhteet. Tietoarkkitehtuurin tärkeimpiä tehtäviä on hallita, kuvata ja mallintaa tietovirtoihin liittyviä käsitteitä, tietomalleja, tietovarantoja ja prosesseja. Tietoarkkitehtuuri tukee muun muassa semanttista yhteentoimivuutta.

3. Tietojärjestelmäarkkitehtuuri
Tietojärjestelmäarkkitehtuuri tarkastelee asioita liiketoimintasovellusten ja sovelluskokonaisuuksien näkökulmasta. Tietojärjestelmäarkkitehtuuri kuvaa esim. tietojärjestelmien tarjoamat palvelut, rajapinnat ja liittymät (integraatiot) eli tietojärjestelmien väliset suhteet ja roolit.

4. Teknologia-arkkitehtuuri
Teknologia-arkkitehtuuri kuvaa organisaation teknologista infrastruktuuria ja teknologiavalintoja. Teknologia-arkkitehtuurissa kuvataan organisaation ICT-infrastruktuuri, standardit ja rakenteet siten, että kokonaisuus tukee parhaalla mahdollisella tavalla organisaation tavoitteita.

Lisäksi: Ihmisnäkökulma
Digitalisaation aikana asiakkailla on monia eri kanavia ja mahdollisuuksia. Asiakas- ja käyttökokemus on aito palveluiden menestystekijä. Kokonaisarkkitehtuuri ei käsittele tätä aihetta. Asiakkaan tai työntekijän kokemusta ei mallinneta lainkaan perinteisissä kokonaisarkkitehtuurimenetelmissä. SaaSec-hanke suositteleekin myös ihmisnäkökulman huomioimista arkkitehtuurityöskentelyssä. Ihmisnäkökulma tuo palvelumuotoilun pääperiaatteet ja dokumentaation osaksi kokonaisarkkitehtuuria, eli käyttökokemuksen yhteentoimivuuden varmistamiseksi. Ihmisnäkökulman osakuvauksia voivat olla mm:

- Asiakaskokemusvisio tai työntekijäkokemusvisio
- Muotoiluperiaatteet (design principles)
- Muotoilumallit (design patterns)
- Asiakas- ja käyttäjäpersoonakuvaukset
- Asiakas- ja palvelupolut
- Saavutettavuus ja käytettävyys

Kokonaisarkkitehtuurin tasot

Kokonaisarkkitehtuuri sisältää neljä eri tasoa, jotka helpottavat asioiden jäsentelyä näkökulmien sisällä. Tasot ovat:

- Periaattellinen taso ohjaa suunnittelua ja kuvaamista eli vastaa kysymykseen MIKSI
- Käsitteellinen taso kuvaa tarpeita ja palveluja eli vastaa kysymykseen MITÄ
- Looginen taso kuvaa rakenteita eli vastaa kysymykseen MITEN
- Fyysinen taso kuvaa ratkaisuja eli vastaa kysymykseen MILLÄ

Lisätietoa tiedonhallintamallista

Tiedonhallintayksikössä (tässä yhteydessä = kunta) on ylläpidettävä sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia.

Tiedonhallintamallilla tavoiteltavat hyödyt ovat mm.:

- parempi palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelu
- tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttaminen
- moninkertaisen tietojen keruun vähentäminen
- tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttaminen
- parempi tietoturvallisuuden ylläpitäminen

Tiedonhallintamallin on sisällettävä vähintään tiedot:

- toimintaprosesseista
- tietovarannoista
- tietoaineistoista sekä niiden arkistoinnista
- tietojärjestelmistä
- tietoturvallisuustoimenpiteistä

(Lähde: Tiedonhallintamalli.fi)

Suositus tiedonhallintamallista (Valtiovarainministeriö)
Laki julkisen hallinnon tiedonhallinnasta (Finlex)

Nykytila ja Tavoitetila

Kokonaisarkkitehtuurityön voi aloittaa analysoimalla nykytilan riittävällä tasolla toiminnan tarpeisiin nähden. Sen jälkeen suunnitellaan tavoitetila, jota kohti pyritään. Nykytilan analysointi ja kuvaaminen on ensimmäisellä kerralla melko suuri kertaluonteinen ponnistus, joten se kannattaa vaiheistaa. Näin tavoitetilan suunnittelussa selviydytään kevyemmällä aiempien kuvausten päivittämisellä.

Nykytila

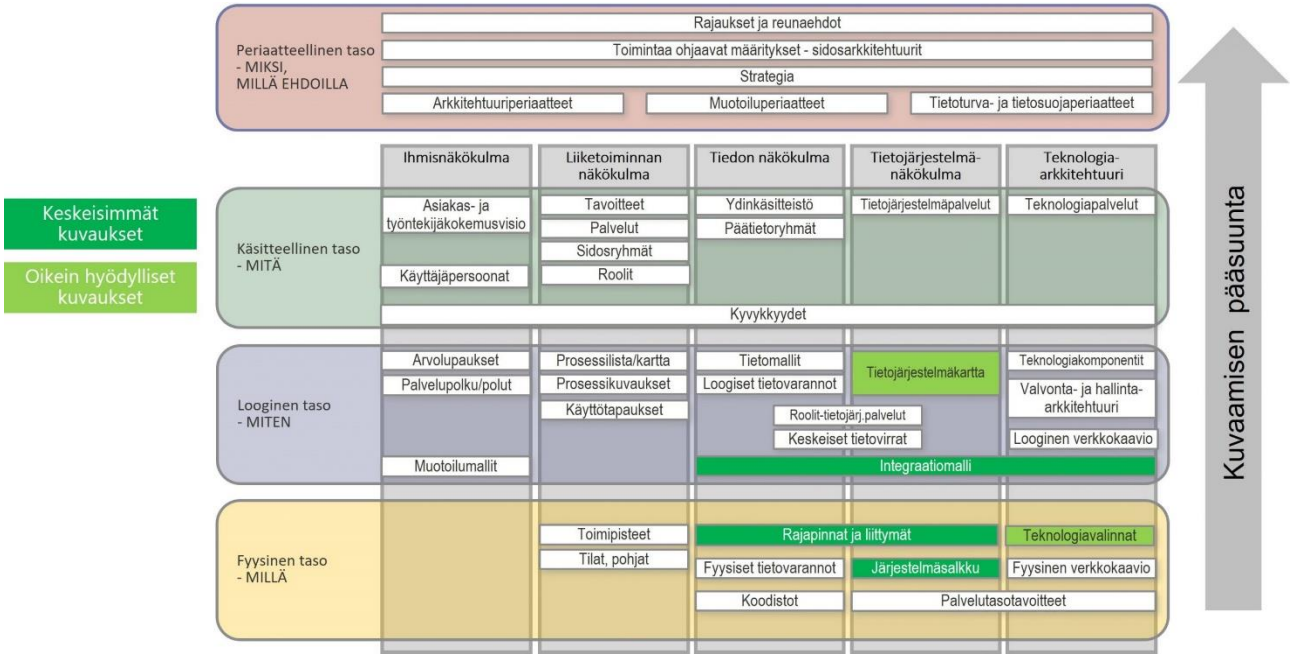
Nykytila kuvaa, kuinka kokonaisuuden osa-alueet liittyvät **tällä hetkellä** toisiinsa ja toimivat kokonaisuutena. Nykytilan kuvausten tarkoitus on auttaa ymmärtämään paremmin organisaatioiden välisiä yhteyksiä ja sisäisiä rakenteita, mikä parantaa olemassa olevan ympäristön hallintaa. On tärkeää kuvata nykytila aina rehellisesti kuten se on (As-Is) – ei muodossa ”näin sen olisi pitänyt olla” (As Wish).

Kokonaisarkkitehtuurimenetelmä luo yhteistä kieltä kuvata hankittavan kohteen keskeisiä piirteitä ja käyttötarkoitusta. KA-menetelmän avulla voidaan laatia erityisesti osaksi hankinnan kohdekuvausta kuvaus siitä:

- Mitä ratkaisulla tavoitellaan
- Mitkä periaatteet ovat hankittavan ratkaisun pohjalla – mitä vaatimuksia sen tulee täyttää
- Mitä toimintaa kyseisellä järjestelmällä tuetaan (ja miten)
- Minkälaisia käyttäjärooleja järjestelmän tulee palvella
- Mitä tietoa järjestelmällä käsitellään
- Mitä toiminnallisia kokonaisuuksia järjestelmältä odotetaan (ns. tietojärjestelmäpalvelut)
- Mihin järjestelmä integroidaan, mitä tietoja eri järjestelmien välillä liikkuu
- Miten järjestelmä sijoittuu teknologiaympäristöönsä

Kokonaisarkkitehtuurissa nykytilaa kuvattaessa kannattaa aloittaa kysymyksellä ”Millä?” eli fyysiseltä tasolta ylöspäin edeten.

Arkkitehtuurikuvaukset nykytilasta



Tavoitetila

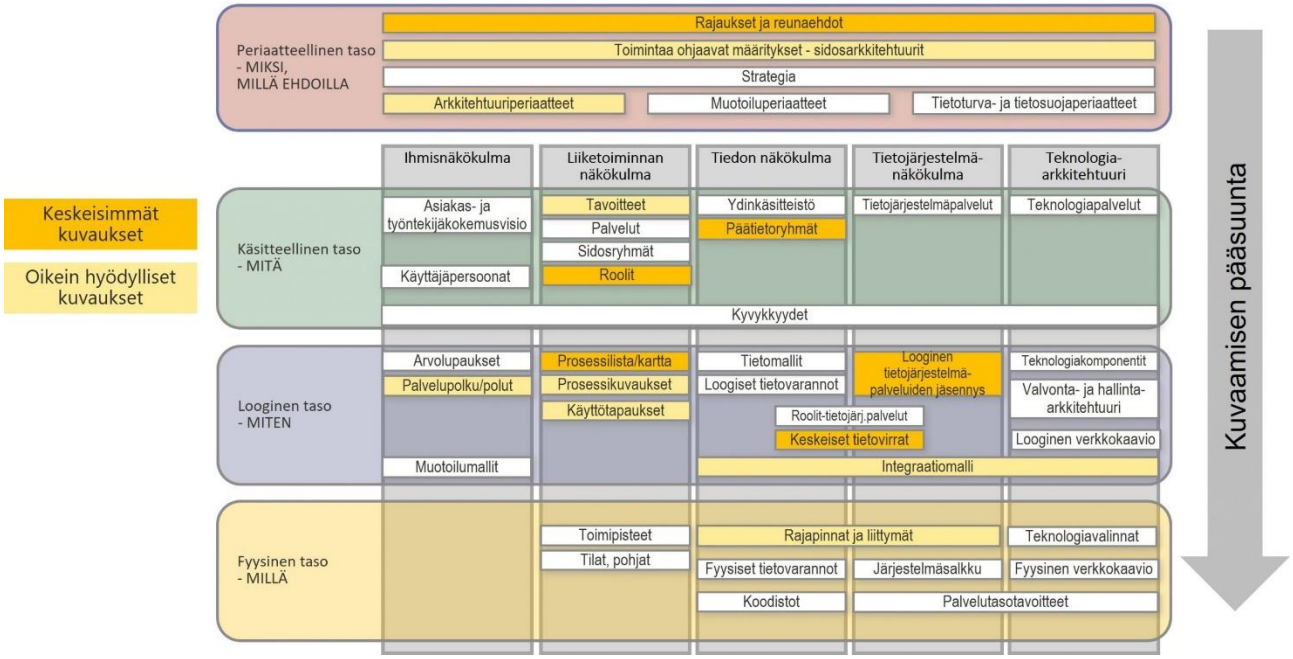
Tavoitetila on kehittämistoimenpiteiden ja toimintaympäristön muutosten kautta syntyvä **tulevaisuuden tilanne** – realistinen tahtotila, jota lähdetään toteuttamaan. Tavoitetila on hallittavissa ja muunneltavissa toiminnan muuttuvien tarpeiden mukaan.

Tavoitetilan arkkitehtuuriin kuvataan lisäksi täsmällisemmin:

- Mitä prosesseja järjestelmällä tulee pystyä tukemaan tai mitä käyttötapauksia järjestelmällä tulee pystyä toteuttamaan
- Mitä toimintoja toteutetaan internetin yli, mitkä ovat toimittajan ympäristön vastuulla
- Mitkä kytkettävät palvelut ovat kunnan ympäristöissä ja konesaleissa (SaaS-hankinnoissa ei kuitenkaan kuvata tarkasti konesalipalveluiden yksityiskohtia)
- Mitä palveluita on muissa pilviympäristöissä tai internetissä (esim. Azure AD -pääsynhallinta)
- Mahdolliset tarvittavat ympäristöt (esim. tuotantoympäristö + testi-/koulutusympäristö)

Kokonaisarkkitehtuurissa tavoitetilaa kuvattaessa kannattaa aloittaa kysymyksellä ”Miksi?” eli suunta on periaatteelliselta tasolta alaspäin edeten.

Arkkitehtuurikuvaukset tavoitetilasta



Arkkitehtuurikuvaukset osana tarjouspyyntöä

SaaSec-hanke on tilannut asiantuntijatyönä esimerkkejä ja mallipohjia sisältävän arkkitehtuuritiivistelmän, jota voit hyödyntää SaaS-hankinnan valmistelussa. Arkkitehtuuritiivistelmän tarkoituksena on kuvata ylätasolla hankittavan järjestelmän tukema toiminta, käyttäjäroolit ja kytkentä muihin järjestelmiin. Varsinaiset vaatimukset on koottu tarjouspyynnön vaatimuslomakkeeseen.

Voit ladata materiaalin omaan käyttöösi. Pohjien avulla voit kuvata nykytilaa ja tavoitetilaa. Arkkitehtuuritiivistelmä liitetään tarjouspyynnön liitteeksi ”Hankinnan kohde” -kuvauspohjan yhteyteen. Voit arkkitehtuuritiivistelmän lisäksi hyödyntää KA-taulukoita keskeisimpiin osakuvauksiin.

- ➔ O3 Liite 1.1: Arkkitehtuuritiivistelmä (.pptx)
- ➔ O4 Liite 1.1.1: KA-taulukot (.xlsx)

Nykytilan ja Tavoitetilan arkkitehtuurikuvausten lisäksi on hyvä tarkentaa ”Hankinnan kohde” -kuvauspohjaan volyymejä:

- Käyttäjien määrä rooleittain
- Järjestelmässä käsiteltävien kohteiden (data) määriä (esim. kuinka monta kustannuspaikkaa, laskua, rakennuslupaa, kiinteistöä, toimipistettä, oppilasta ym.)
- Luonnehdinta, mitä tietoa vanhasta järjestelmästä tulee siirtää hankittavaan uuteen järjestelmään osana käyttöönottoprojektia

Hyödyllistä lisätietoa saat tämän oppaan sivulta Tarjouspyyntö.

TIETOTURVALLISUUDEN ARVIOINTI

Arviointimenetelmiä

Pilvipalvelujen turvallisuuden arvioinnissa voidaan käyttää erilaisia menetelmiä. Joidenkin tietojen suojaamisen arvioinnissa saattaa olla riittävää nojautua esimerkiksi pilvipalveluntarjoajan tuottamaan itsearviointiin, mahdollisiin muihin sertifiointeihin sekä sopimusteknisiin sitoumuksiin. Joidenkin tietojen suojaamisen arvioinnissa on perusteltua edellyttää lisäksi ulkopuolisen riippumattoman tahon tekemää todennusta.

Todennuksen tuottamien tulosten luotettavuus riippuu merkittävästi todennuksessa käytettyjen menetelmien luotettavuudesta. Esimerkiksi **dokumentaatioon tutustuminen** eroaa luotettavuudeltaan siitä, että pilvipalvelun suojaus todennettaisiin myös **teknisen testaamisen** keinoin. Todennuksessa voidaan usein hyödyntää myös esimerkiksi jatkuvan auditoinnin mahdollisuuksia lisänäytön lähteinä. Joidenkin tietojen suojaamisen arvioinnissa on perusteltua käyttää kansallisen tietoturvallisuusviranomaisen arviointipalvelua.
(Lähde: Pilvipalveluiden turvallisuuden arviointikriteeristö, Traficom)

Huomioitavaa: Pilvipalveluissa suuri osa turvallisuudesta on palveluntoimittajan vastuulla, mutta tämä ei kuitenkaan vapauta kuntaa vastuusta tietoturvan, varautumisen, jatkuvuudenhallinnan ja tietosuojan suhteen.

Arvioinnit voidaan jakaa suorittajan mukaan seuraavasti:

- **Itsearviointi**: Arvioinnin kohteen vastuuhenkilön tai työryhmän toteuttama arviointi. Vastuuhenkilö ei välttämättä ole tietoturvahenkilöstöä.
- **Sisäinen arviointi**: Organisaation tietoturvahenkilöstön tai asiantuntijoiden toteuttama arviointi.
- **Sisäinen tarkastus**: Organisaation oma järjestelmällinen ja riippumaton arviointi.
- **Vertaisarviointi**: Arvioijina toimivat henkilöt, jotka työskentelevät samankaltaisen kohteen parissa toisessa organisaatiossa tai yksikössä.
- **Ulkoinen arviointi**: Organisaation ulkopuolisen, riippumattoman toimijan suorittama arviointi.
  (Lähde: Tietoturvallisuuden arviointiohje, Valtiovarainministeriö)

Vinkkejä kriteerien ja standardien käyttöön:

Kysyttäessä neuvoa ChatGPT:ltä, se antaa seuraavanlaisia, varsin viisaita vinkkejä kriteerien ja standardien tehokkaaseen käyttöön pilvipalvelun auditoinnissa:

- **Ymmärrä standardit ja kriteerit**
  Ennen kaikkea on tärkeää ymmärtää perusteellisesti ne standardit ja kriteerit, joita aiot noudattaa. Selvitä, mitä ne sisältävät, mitä vaatimuksia ne asettavat ja millaisia prosesseja ja käytäntöjä ne edellyttävät.

- **Räätälöi vaatimukset ympäristöösi**
  Vaikka standardit antavat yleiset vaatimukset, muista räätälöidä ne omaan toimintaympäristöösi. Jokainen organisaatio ja pilvipalvelu voi olla erilainen, joten varmista, että standardin vaatimukset sopivat käytäntöihisi.

- **Käytä auditointityökaluja**
  Hyödynnä mahdollisia auditointityökaluja, kuten tarkastuslistoja, pohjia ja valmiita dokumentteja. Näitä työkaluja on usein saatavilla standardin tarjoajilta ja muilta asiantuntijoilta.

- **Luo selkeä toimintasuunnitelma**
  Laadi toimintasuunnitelma, joka määrittelee vaiheet, aikataulut ja vastuut standardien ja kriteerien noudattamiseksi. Selkeä suunnitelma auttaa varmistamaan, että et jää jumiin vaatimusten täyttämisessä.

- **Jaa vastuuhenkilöt**
  Nimitä vastuuhenkilöt, jotka ovat vastuussa eri osa-alueiden noudattamisesta ja valmistelusta. Näin varmistetaan, että jokainen tärkeä näkökohta otetaan huomioon.

- **Tee tarvittavat muutokset**
  Jos havaitset aukkoja tai puutteita nykyisissä käytännöissäsi, tee tarvittavat muutokset noudattaaksesi standardin vaatimuksia. Tämä voi liittyä tietoturvaan, dokumentaatioon, prosesseihin jne.

- **Dokumentoi prosessit ja käytännöt**
  Tärkeää on dokumentoida kaikki prosessit ja käytännöt, joilla vastaat standardin vaatimuksiin. Selkeä ja kattava dokumentaatio helpottaa auditointiprosessia ja osoittaa, että noudatat vaatimuksia.

- **Kouluta henkilöstöä**
  Kouluta organisaation henkilöstöä standardin ja kriteerien vaatimuksista sekä siitä, miten heidän odotetaan toimivan. Tietoisuus ja ymmärrys ovat avainasemassa vaatimusten noudattamisessa.

- **Suorita sisäinen arviointi**
  Ennen varsinaista auditointia suorita sisäinen arviointi. Tämä auttaa tunnistamaan mahdolliset ongelma-alueet ja korjaamaan ne ennen kuin ulkopuolinen auditointi alkaa.

- **Ole valmis yhteistyöhön**
  Jos käytät ulkopuolista auditoijaa, ole valmis yhteistyöhön ja avoimeen vuorovaikutukseen auditoijien kanssa. Vastaa heidän kysymyksiinsä ja tarjoa tarvittava dokumentaatio.

- **Seuraa toimintaasi**
  Vaikka auditointi on yksi tapahtuma, standardien ja kriteerien noudattaminen on jatkuva prosessi. Seuraa jatkuvasti toimintaasi ja päivitä käytäntöjä tarpeen mukaan.

- **Hyödynnä oppimista**
  Auditointiprosessista voi oppia paljon organisaation vahvuuksista ja heikkouksista. Käytä saamiasi palautteita ja havaintoja parantaaksesi tietoturvaa, tietosuojaa ja muita prosesseja jatkossa.

Huomioitavaa: Standardien ja kriteerien noudattaminen ei ole yksittäinen tapahtuma, vaan jatkuva pyrkimys parantaa organisaation toimintaa ja varmistaa luotettavuus, tietoturva ja tietosuoja.

Kriteeristöjä ja standardeja

ISO 27001

Tietoturvan hallinnan johtava kansainvälinen standardi, joka keskittyy tietoturvan hallintajärjestelmän toteuttamiseen. Standardi on jaoteltu neljään hallintateemaan:

1. Organisaatio
2. Henkilöstö
3. Fyysinen
4. Teknologia

Hallintateemat sisältävät vaatimuksia liittyen mm. seuraaviin osa-alueisiin: tietoturvapolitiikat, tietoturvallisuuden organisointi, henkilöstöturvallisuus, suojattavan omaisuuden hallinta, pääsynhallinta, salaus, fyysinen turvallisuus, käyttöturvallisuus, viestintäturvallisuus, järjestelmien hankkiminen, kehittäminen sekä ylläpito, suhteet toimittajiin, tietoturvahäiriöiden hallinta, liiketoiminnan jatkuvuuden hallinta ja vaatimustenmukaisuus.

ISO 27017

Tietoturvastandardi, joka on kehitetty erityisesti pilvipalveluntarjoajille ja käyttäjille turvallisemman pilvipohjaisen ympäristön luomiseksi ja tietoturvahäiriöiden riskin vähentämiseksi. Laajentaa ISO 27001 -standardia, joten näitä kahta viitekehystä tulee käyttää yhdessä.

ISO 27018

Tietoturvastandardi, joka on kehitetty erityisesti pilvipalveluntarjoajille, jotta voidaan varmistaa riskien arvioiminen ja valvonnan toteuttaminen henkilötietojen suojaamiseksi julkisissa pilviympäristöissä. Laajentaa ISO 27001 -standardia, joten näitä kahta viitekehystä tulee käyttää yhdessä.
(Lähde: Digiturvamalli.fi)

CSA STAR

CSA (Cloud Security Alliance) on pilvipalveluiden tietoturvaan keskittynyt avoin yhteisö. CSA on julkaissut globaalin ja luotettavaksi tunnustetun läpinäkyvän sertfiointimenettelyn pilvitoimittajille. Sertifiointiin liittyvän kyselyn suorittaneet pilvitoimittajat ja heidän antamansa tiedot on julkaistu CSA:n julkisessa STAR-rekisterissä (Security, Trust, Assurance, Risk). Rekisterin

avulla asiakas voi arvioida pilvipalvelun tietoturvatasoa. Rekisteriä voi hyödyntää itsearvioinnissa tai ulkoisessa arvioinnissa.

PiTuKri

Tutustu pilvipalveluiden turvallisuuden arviointikriteeristöön (PiTuKri) Traficomin verkkosivuilla. Voit myös ladata käyttöösi PiTuKri-arviointityökalun (Excel).

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

Julkri

Tutustu julkisen hallinnon tietoturvallisuuden arviointikriteeristöön (Julkri) Valtioneuvoston verkkosivuilla. Voit myös ladata käyttöösi Julkri-arviointityökalun (Excel). Ennalta määritelty käyttötapaus ”SaaS-pilvipalvelun arviointi” on tarkoitettu juuri SaaS-palveluiden turvallisuuden arviointiin.

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)
Ota Julkri haltuun! Julkri-koulutus eOppivassa (linkki) (Digi- ja väestötietovirasto)

TIETOSUOJAN VAIKUTUSTENARVIOINTI (DPIA)

Tietosuojaa koskevan vaikutustenarvioinnin (DPIA = Data Protection Impact Assessment) tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. DPIA on osa tietosuojalainsäädännön vaatimusten noudattamista ja dokumentointia.

DPIA tulee tehdä ennen kuin SaaS-palvelu otetaan käyttöön ja sitä on päivitettävä tarvittaessa. Organisaatiossa jo olemassa olevat SaaS-palvelut kannattaa kartoittaa ja niille tulee laatia DPIA pikimmiten.

DPIA:n avulla voi osoittaa asiakkaille ja yhteistyökumppaneille, miten tietosuojasta on huolehdittu. DPIA sitouttaa myös henkilöstöä tietosuojariskien tunnistamiseen ja hallintaan.

Hyödynnettävät pohjat

SaaSec-hanke on tuottanut ohjeen, työkalun alkuarviointiin ja raporttipohjan DPIA:n tekemisen tueksi.

- ➔ Ohje – DPIA Tietosuojan vaikutustenarviointi (.pdf)
- ➔ Pohja – DPIA Tietosuojan vaikutustenarviointi (.docx)

Jos alkuarviointi on osoittanut, että henkilötietoja käsitellään, mutta varsinaista vaikutustenarviointia ei tarvitse tehdä, apuna projekteissa ja hankinnoissa voidaan käyttää

tietoturvan ja tietosuojan tarkastuslistaa. Tarkastuslista on laadittu Espoon, Kuopion, Tampereen ja Oulun kaupunkien tietoturva- ja tietosuojayhteistyössä (versio 1.02/2018).

Huomioitavaa: Pilvipalveluissa suuri osa turvallisuudesta on palveluntoimittajan vastuulla, mutta tämä ei kuitenkaan vapauta kuntaa vastuusta tietoturvan, varautumisen, jatkuvuudenhallinnan ja tietosuojan suhteen.

Tietoa DPIA:sta tietosuojavaltuutetun toimiston verkkosivuilta

TIETOJEN SIIRRON VAIKUTUSTENARVIOINTI (TIA)

Tietojen siirtoa koskevan vaikutustenarvioinnin (TIA = Transfer Impact Assessment) tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen siirtoon sisältyviä riskejä tilanteessa, jossa tietoja siirretään Euroopan talousalueen ulkopuolelle ns. kolmansiin maihin (= EU/ETA-alueen ulkopuolisiin maihin). TIAn avulla voidaan tarkistaa, onko siirrolle lainmukaiset edellytykset.

Vaikutustenarviointi on suositeltavaa tehdä silloin, kun suunnitellaan henkilötietojen käsittelyä, tai viimeistään SaaS-palvelun käyttöönoton yhteydessä. Organisaatiossa jo olemassa olevat SaaS-palvelut kannattaa kartoittaa ja niille tulee laatia TIA pikimmiten. Vaikutustenarvioinnin päivittämisen tarvetta on lisäksi suositeltavaa arvioida säännöllisesti, esimerkiksi kahden vuoden välein.

Hyödynnettävät pohjat

SaaSec-hanke on tuottanut arviointipohjan täyttöohjeineen TIA:n tekemisen tueksi.

➔ Pohja ja ohje – TIA Tietojen siirron vaikutustenarviointi (.docx)

SaaSec-hankekunnat voivat käyttää TIA-arviointipohjaa ja täyttöohjeistusta itsenäisesti TIA-arviointien dokumentointiin. TIA-arvioinnin laatiminen vaatii kuitenkin aina tietosuojaosaamista ja ymmärrystä tapauskohtaisesti mm. tiedonsiirtoja suojaavien suojakeinojen riittävyydestä suhteutettuna kunkin kohdemaan lainsäädännöstä arvioinnissa saatuihin havaintoihin.

Tietoa TIA:sta tietosuojavaltuutetun toimiston verkkosivuilta

Siirto tietosuojan riittävyyttä koskevan päätöksen perusteella

Tilanne US-EU -välisten tiedonsiirtojen osalta muuttui merkittävästi, kun Euroopan komissio hyväksyi heinäkuussa 2023 päätöksen Yhdysvaltojen tietosuojan riittävästä tasosta. Riittävyyspäätös koskee niitä yhdysvaltalaisia organisaatioita, jotka ovat sertifioituneet osaksi US-EU -tietosuojakehystä (Data Privacy Framework). Sertifioituneet yritykset voi tarkistaa Yhdysvaltain hallinnon ylläpitämältä sivulta (linkki sivulle: https://www.dataprivacyframework.gov/s/participant-search).

Riittävyyspäätöksen nojalla henkilötietoja voidaan siirtää sertifioituneille yhdysvaltalaiselle yritykselle, jotka ovat sitoutuneet EU:n ja Yhdysvaltojen välisessä tietosuojakehyksessä sovittuihin suojatoimiin. Riittävyyspäätöstä ei voi käyttää tiedonsiirtoihin julkisen sektorin toimijoiden välillä. TIA-arvioinnin laatiminen on edelleen tarpeen niiden tiedonsiirtojen osalta, joissa yhdysvaltalainen vastaanottava henkilötietojen käsittelijä ei ole osa US-EU -tietosuojakehystä sekä niissä tapauksissa, joissa tiedonsiirto tapahtuu johonkin muuhun 'kolmanteen maahan' kuin Yhdysvaltoihin – esimerkiksi Intiaan.

Tietoa riittävyyspäätöksestä tietosuojavaltuutetun toimiston verkkosivuilta

PILVIPALVELUIDEN TURVALLISUUDEN ARVIOINTIKRITEERISTÖ (PITUKRI)

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) sisältää pilvipalveluiden turvallisuuteen liittyviä hyviä käytäntöjä ja tulkintoja sekä ohjeistuksia pilvipalveluihin liittyvien riskien käsittelyyn. PiTuKri on liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen julkaisu.

Kriteeristö on tarkoitettu käytettäväksi pilvipalveluiden turvallisuuden arvioinnissa. Sitä voidaan käyttää myös pilvipalveluntarjoajien omaehtoisen turvallisuustyön tukena. Kriteeristön tarkoituksenmukainen käyttö edellyttää käyttötapauskohtaista soveltamista.

PiTuKri on jaettu 11 osa-alueeseen (katso taulukko alla). Osa-alueet koostuvat vaatimuskorteista. Vaatimuskortteihin on kuvattu vaatimuksen teema, konkreettinen vaatimus, vaatimuksen soveltamiskohteet, suojaustavoite, sekä vaatimuksen toteuttamisen ja tulkinnan tueksi tarkoitettuja lisätietoja.

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)
Osa-alue 1: Esiehdot
EE-01 - Järjestelmäkuvaus
EE-02 - Lainsäädäntöjohdannaiset riskit
Osa-alue 2: Turvallisuusjohtaminen
TJ-01 - Turvallisuusperiaatteet
TJ-02 - Turvallisuuden vastuut
TJ-03 - Turvallisuusriskien hallinta
TJ-04 - Turvallisuushäiriöiden hallinta
TJ-05 - Jatkuvuudenhallinta
TJ-06 - Tietojen ja muiden suojattavien kohteiden luokittelu ja merkintä
TJ-07 - Vaatimustenmukaisuus ja tietosuoja
TJ-08 - Palveluntarjoajien ja toimittajien turvallisuus
Osa-alue 3: Henkilöstöturvallisuus
HT-01 - Työsuhteen elinkaaren huomioiminen
HT-02 - Henkilöstön luotettavuuden arviointi

HT-03 - Salassapito- ja vaitiolositoumukset
HT-04 - Turvallisuustietoisuus
HT-05 - Tiedonsaantitarpeet ja tehtävien erottelu
Osa-alue 4: Fyysinen turvallisuus
FT-01 - Monitasoinen suojaaminen ja riskienhallinta
FT-02 - Rakenteet ja turvallisuusjärjestelmät
FT-03 - Luvattoman pääsyn estäminen
FT-04 - Palveluntuottajat ja vierailijat
FT-05 - Varautuminen ja jatkuvuudenhallinta
Osa-alue 5: Tietoliikenneturvallisuus
TT-01 - Tietoliikenneverkon rakenne
TT-02 - Yleisiä verkkohyökkäyksiä vastaan suojautuminen
Osa-alue 6: Identiteetin ja pääsyn hallinta
IP-01 - Käyttöoikeushallinta
IP-02 - Käyttäjätunnistus
IP-03 - Hallintayhteydet
Osa-alue 7: Tietojärjestelmäturvallisuus
JT-01 - Jäljitettävyys ja havainnointikyky
JT-02 - Järjestelmäkovennus
JT-03 - Tiedon erottelu
JT-04 - Haittaohjelmasuojaus
JT-05 - Suojattavien kohteiden siirtäminen
Osa-alue 8: Salaus
SA-01 - Salauskäytännöt ja avainhallinta
SA-02 - Salaus fyysisen turvallisuusalueen ulkopuolella
SA-03 - Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella
Osa-alue 9: Käyttöturvallisuus
KT-01 - Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi
KT-02 - Suorituskyvyn hallinta
KT-03 - Varmistus- ja palautusprosessit
KT-04 - Haavoittuvuuksien hallinta
Osa-alue 10: Siirrettävyys ja yhteensopivuus
SI-01 - Siirrettävyys ja yhteensopivuus
SI-02 - Tietoaineistojen tuhoaminen
Osa-alue 11: Muutostenhallinta ja järjestelmäkehitys
MH-01 - Muutostenhallinta
MH-02 - Järjestelmäkehitys

PiTuKri – vaatimukset ja vastuut -tiedoston avulla voit tutustua PiTuKri:ssä kuvattuihin vaatimuksiin. Pilvipalveluntarjoajan on vastattava kaikkiin vaatimuksiin, kun kyseessä on SaaS-mallin pilvipalvelu. Asiakasympäristön eli kunnan vastuulla olevat vaatimukset on merkitty tiedostossa oikeanpuoleiseen sarakkeeseen.

➔ PiTuKri - vaatimukset ja vastuut (.pdf)

Huomioitavaa: Asiakkaan vastuulle kuuluviin osuuksiin sisältyy tyypillisesti sekä pilvipalvelun asiakasjärjestelmän osuus, että asiakkaan muiden tiedonkäsittely-ympäristöjen osuus.

Kriteeristössä kuvatut vaatimukset ovatkin useimmiten perusteltuja kohdentaa

- pilvipalveluntarjoajan vastuulla olevaan osuuteen,
- joissain sekä pilvipalveluntarjoajan että pilvipalvelun asiakkaan osuuksiin, ja
- joissain vain asiakkaan vastuulla olevaan osuuteen.

Kriteeristön tarkoituksenmukainen käyttö edellyttää riittävää osaamista turvallisuuden arvioijalta, pilvipalveluntarjoajalta ja pilvipalvelun asiakkaalta.

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

Klikkaamalla yllä olevasta linkkipainikkeesta voit tutustua pilvipalveluiden turvallisuuden arviointikriteeristöön (PiTuKri) kokonaisuudessaan Traficomin verkkosivuilla. Voit myös ladata käyttöösi PiTuKri-arviointityökalun (Excel).

RACI-VASTUUNJAKOTAULUKKO

RACI-vastuunjakotaulukko on projektinhallinnan työkalu, jonka avulla roolit ja vastuut voidaan dokumentoida tiivistetyssä muodossa. RACIn avulla voidaan varmistaa, että kaikki tietävät omat ja muiden vastuut, mitä tehtäviä millekin roolille kuuluu ja kenen kanssa tehtävät tehdään. RACI-nimen jokaisella neljällä kirjaimella on merkitys:

R = responsible (vastuullinen)
- R-roolissa oleva henkilö/taho suorittaa annetun tehtävän tai on osa suoritustiimiä
- jokaisella tehtävällä on **ainakin yksi** R-rooli

A = accountable (vastuussa oleva, päätöksen tekijä)
- A-roolissa oleva valvoo ja vastaa siitä, että tehtävä tulee valmiiksi
- jokaisella tehtävällä on **vain yksi** A-rooli

C = consulted (konsultoitava, neuvoja)
- C-roolissa olevalta voidaan kysyä ohjeita, neuvoja ja mielipiteitä
- jokaisella tehtävällä voi olla nolla – rajaton määrä C-rooleja
- kommunikointi on 2-suuntaista

I = informed (tiedotettava)

- I-roolissa olevia tiedotetaan tehtävän suorittamisesta
- jokaisella tehtävällä voi olla nolla – rajaton määrä I-rooleja
- kommunikointi on 1-suuntaista

Roolit

Vastuita tehtävistä voi jakaa rooleille tarvittaessa ylätasolla tiimeittäin ja tarkentaa sitten pienempiin osiin ja konkreettisemmin ammattinimikkeittäin. SaaS-palvelun elinkaaren hallinnassa roolien ammattinimikkeet voivat olla esimerkiksi seuraavia:

- Tietohallintojohtaja
- Tekninen asiantuntija
- ICT-arkkitehti
- Tietosuojavastaava
- Tietoturvavastaava
- Projektipäällikkö
- Hankinta-asiantuntija / -osasto
- Viestintäasiantuntija / -osasto
- Toimialan substanssiasiantuntija
- Johto ja esihenkilöt
- Henkilöstön pääkäyttäjä
- Henkilöstön peruskäyttäjä
- Palveluntoimittaja

Tässä esitetyt roolit ovat esimerkinomaisia ja ne tulee muokata vastaamaan organisaation omaa tarvetta.

RACI-taulukon hyötyjä

- Auttaa määrittelemään selkeästi kaikkien osallistuvien tahojen roolit ja vastuut sekä tasapainottamaan työmäärät.
- Mahdollistaa SaaS-palvelun elinkaaren vaiheiden ja tehtävien edistämisen ja seurannan hallitusti.
- Tehostaa tekemistä ja viestintää sekä nopeuttaa päätöksentekoa.

RACI-taulukon rakentaminen

1. Määrittele suoritettavat tehtävät ja kirjaa tiedot riveille.
2. Tunnista roolit eli osallistuvat henkilöt sekä tahot ja kirjaa tiedot sarakkeisiin.
3. Kirjaa RACIn mukaiset vastuut (kirjain R A C I) taulukkoon.
4. Tarkastele taulukkoa: jakaantuvatko tehtävät oikein ja tasapuolisesti, onko puutteita vastuissa tai onko päällekkäisyyksiä.
5. Huolehdi taulukon käyttöönotosta ja päivittämisestä.

Missä vaiheessa RACIa kannattaa käyttää?

Voit hyödyntää RACIa työkaluna SaaS-palvelun elinkaaren hallinnan useissa vaiheissa: määrittelyvaiheen ja hankinnan resursoinnissa, palvelun käyttöönotossa ja toteutuksessa sekä palvelun päättämisen yhteydessä.

Hyödynnettävät pohjat

➔ Esimerkkipohja: RACIn käyttö pilvipalvelun päättämisen yhteydessä (.xlsx)

SaaS-palveluntoimittajien vinkit

SaaSec-hanke järjesti syksyllä 2022 työpajan, johon osallistui hankekuntien digihallinnon ja SaaS-palveluita toimittavien yritysten edustajia. Mukaan kutsuttiin kuusi kuntien yhteistä SaaS-palveluntoimittajaa (joista neljä osallistui), ja he kaikki edustivat alueellisia SaaS-ratkaisuja. Toimittajat esittelivät omien SaaS-ratkaisujensa teknologiaa, periaatteita ja digitaalista turvallisuutta. Heiltä pyydettiin myös kommentteja ja vinkkejä kuntien SaaS-hankintoihin. Tässä kooste vinkeistä.

Tehkää näin, ottakaa nämä huomioon:

- Keskittykää siihen, mitä haluatte ratkaista – ei suoraan siihen, mikä on ratkaisutapa
    - Ei vaatimusta: ”Täsmälleen sama kuin nyt, mutta ei kuitenkaan niin sama, että se olisi yhtä huono kuin nykyinen”
- Tunnistakaa keskeiset tarpeet ja core ja etsikää ratkaisua tämän ympärille
- Määritelkää alustava budjetti – edellyttänee tutustumista siihen, millä hintatasolla järjestelmiä myydään
- Määritelkää hankintaan ja SaaS-hankintoihin vastuuhenkilö
- Olkaa hyvissä ajoin liikenteessä
    - Esim. käyttöönotolle tulee jättää riittävästi aikaa
- Ottakaa selvää etukäteen tuotteista ja palveluista – kartoittakaa ja selvittäkää
- Vaatimukset kannattaa määritellä siten, että ne vastaavat haasteen ratkaisuun, eikä niinkään siihen, miten haaste pitäisi ratkaista
    - Miettikää kriittisesti, mitkä ovat pakolliset vaatimukset
- Tutustukaa SaaS-palveluiden ostoprosesseihin ja sopimuksiin
- Hankintaprosessissa olisi hyvä olla mukana eri alojen asiantuntijoita – yhteistyö ja vuorovaikutus välillä hankintayksikkö & tietohallinto & substanssi on tärkeää
- Referenssivaatimukset voivat olla hyödyllisiä
- Neuvottelumenettelyä kannattaisi suosia (konsultin kommentti: ns. kilpailullinen neuvottelumenettely voi olla myös joustava vaihtoehto)
- Markkinavuoropuheluun on kiinnostusta, siitä on saatu hyvää kokemusta
- Järjestelmähankintojen tulisi korvata aikaisempia järjestelmiä – tämä pitäisi olla käyttöönottoprojektin vaatimuksena
- Vaatimusten visualisointi esimerkkien avulla ja standardien käyttö helpottaa toimittajien vastaamista
    - Mieluiten tarkasti, jotta näihin voidaan helposti sitoutua
    - Tässä on hyvä kuvata tavoite, ei täsmälleen toteutustapaa
- Usein kuntien keskinäinen yhteistyö on hyödyllistä

Älkää tehkö näin, välttäkää näitä:

- IT:n tulee olla mukana – jos hankinnan toteuttaa yksin substanssi tai hankintayksikkö, niin eteen voi tulla suuria haasteita (esim. kokonaiskustannukset)
- Älkää tehkö kohtuuttomia vaatimuksia, jotka eivät ole suhteessa hankinnan kohteeseen tai kokoon

    - Esim. käytettävyys, vahingonkorvaukset ja sanktiot
- Älkää luottako kuvaamattomiin varmuuskopiointiratkaisuihin
    - Esim. pisteytettävät kuvaukset
- Ei mallia, jossa pelkkä hinta ratkaisee
    - Hinnan painotusosuuden pitäisi olla korkeintaan 30 %
    - Esim. toimittaja- ja ratkaisu-arviointi on ihan hyvä tapa arvioida ratkaisuja
    - Kun laatua pisteytetään, tällä saadaan kunnalle paremmin sopivia tuotteita
    - Huomioikaa myös käytettävyyden osuus tarjousvertailussa
- Älkää ostako vain hienoa ja kiiltävää uutta ”järjestelmäihastusta”, vaan hankkikaa järjestelmiä tarpeeseen

Toimittajien vinkkejä ja toiveita on huomioitu

Toimittajien antamia vinkkejä ja toiveita on huomioitu mm. vaatimuslomakkeessa, tarjousohjepohjassa, arkkitehtuuritiivistelmässä ja mallivaatimuksissa, joiden rakenne ja ohjeistus erityisehtoineen auttavat käyttäjää. SaaSec-hankkeen hankintapohjia on kehitetty ja testattu yhdessä kuuden kunnan toimialojen edustajien, hankintayksiköiden ja tietohallinnon asiantuntijoiden kesken.

Linkkivinkit muihin aineistoihin

Tälle sivulle on koottu tietoa eri tahojen tuottamista tausta-aineistoista ja koulutusmateriaaleista, joita on hyödynnetty SaaS-palvelun hankinta- ja digiturvaoppaan lähteinä ja tuotannossa.

Pilvipalvelujen soveltamisohje - Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille

Tutustu soveltamisohjeeseen tästä

Pilvipalvelujen soveltamisohje perehdyttää lukijan pilvipalvelujen hyödyntämisen elinkaareen, käy läpi kunkin elinkaarenvaiheen keskeiset tehtävät sekä vaiheissa huomioitavat asiat sekä tuo julkisen hallinnon asiantuntijoiden käyttöön valmiita pohjia ja malleja.
(Valtiovarainministeriö 2020)

Polku vaikuttaviin ICT-hankintoihin – Pelikirja hankintayksiköille ja tarjoajille

Tutustu pelikirjaan tästä

ICT-hankintojen pelikirja tarjoaa mallin vaikuttaviin ICT-hankintoihin ja ketterään yhteistyöhön. Pelikirjaan on koottu yhteistyössä tunnistettuihin hyviin käytänteisiin perustuvia ohjeita, joita ICT-hankintoja toteuttavat ja hankintoihin osallistuvat henkilöt voivat käyttää työnsä tukena.
(Valtiovarainministeriö ja Kuntaliitto 2023)

Suositus tietoturvallisuudesta hankinnoissa

Tutustu julkaisuun tästä

Tämä tiedonhallintolautakunnan antama suositus opastaa viranomaisia ja erityisesti hankintayksiköitä tietojärjestelmien ja soveltuvin osin muiden palveluiden hankintoihin liittyvien tietoturvallisuusvaatimusten määrittelyssä sekä niiden täyttymisen varmistamisessa.
Suositus sisältää kuvauksen hankinnan tietoturvallisuuden varmistamisen prosessista, esittelyt sopimukseen liitettävistä tietoturvallisuusvaatimuksista sekä ohjeen hankintaehtotyökalun käyttämisestä. Suosituksen liitteinä ovat tietoturvallisuusvaatimukset (suppea ja laaja) sekä hankintaehtotyökalu, jonka avulla hankintayksikkö voi muodostaa hallinnollisen turvallisuuden, fyysisen turvallisuuden, teknisen turvallisuuden sekä varautumisen ja jatkuvuudenhallinnan liitteet. Hankintaehtotyökalu perustuu Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön Julkriin.
(Valtiovarainministeriö 2023)

Hankinnan markkinakartoitus

Tutustu oppaaseen tästä

Tämä markkinakartoitusta käsittelevä opas on tarkoitettu kaikille julkisissa organisaatioissa

hankintoja toteuttaville. Opas on hyödyksi myös julkisten hankintojen strategisen ja operatiivisen tason suunnittelussa sekä substanssiasiantuntijoille, jotka osallistuvat julkisten hankintojen toteuttamiseen.

Oppaan tarkoitus on kasvattaa ymmärrystä markkinavuoropuheluiden suunnittelusta ja antaa varmuutta niiden toteuttamiseen: miten saada markkinoiden ymmärrys tuotua tehokkaasti osaksi omaa hankintaa? Oppaassa kuvataan hankintojen valmisteluun kuuluvaa toimittajamarkkinoiden kartoittamista ja tarjonnan analysointia.
(KEINO-osaamiskeskus 2020)

Digitaalisen turvallisuuden arkkitehtuuri

Tutustu sivustoon tästä
Suorita eOppivan koulutus: Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla

Digitaalisen turvallisuuden arkkitehtuuri on suunnittelutyötä helpottava työväline, jolla digitaalista turvallisuutta voidaan kehittää ja jäsentää. Arkkitehtuuri muodostaa käsityksen organisaation suojattavasta omaisuudesta ja toimintaympäristöstä sekä niihin kohdistuvista uhista ja riskeistä. Lisäksi se kattaa ymmärryksen organisaatioon kohdistuvista vaatimuksista ja strategisista linjauksista sekä niitä toteuttavista digitaalisen turvallisuuden rakennusosista.

Viitekehys on tarkoitettu kaikille julkisen hallinnon toimijoille digitaalisen turvallisuuden kokonaisuuden suunnittelun ja hahmottamisen työvälineeksi. Viitekehys kokoaa käytäntöjä useasta eri standardista ja se koostuu viidestä avaintoiminnosta: tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen.
(Digi- ja väestötietovirasto 2022)

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

Tutustu arviointikriteeristöön tästä

Kriteeristö on tarkoitettu käytettäväksi pilvipalveluiden turvallisuuden arvioinnissa. Sitä voidaan käyttää myös pilvipalveluntarjoajien omaehtoisen turvallisuustyön tukena. Kriteeristön tarkoituksenmukainen käyttö edellyttää käyttötapauskohtaista soveltamista.
(Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus 2020)

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)

Tutustu arviointikriteeristöön tästä
Suorita eOppivan koulutus: Ota Julkri haltuun!

Julkri tukee koko julkishallinnon tietoturvallisuuden kehittämisen ja arvioinnin tarpeita. Sitä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä. Ennalta määritelty käyttötapaus ”SaaS-pilvipalvelun arviointi” on tarkoitettu juuri SaaS-palveluiden turvallisuuden arviointiin.
(Valtiovarainministeriö 2023)

Toimintaohje - Pilviympäristöjen poikkeamanhallinta

Tutustu ohjeeseen tästä

Tämän Traficomin Kyberturvallisuuskeskuksen laatiman ohjeen tavoitteena on neuvoa organisaatioita varautumaan pilvipalveluita koskeviin tietoturvapoikkeamiin, sekä toimimaan tilanteissa, jossa epäillään pilviympäristöön kohdistunutta tietoturvapoikkeamaa. Ohje on tarkoitettu kaikille organisaatioille koosta tai toimialasta riippumatta.

Tämä ohje kattaa tietoturvapoikkeaman elinkaaren seuraavat vaiheet:

- Tietoturvapoikkeaman havainnointi
- Poikkeamatilanteessa toimiminen
- Poikkeamasta palautuminen

(Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus 2023)

Digi- ja väestötietoviraston Digiturvapalvelut

Tutustu palveluihin tästä

Digi- ja väestötietoviraston Digiturvapalvelut kehittää julkisen hallinnon digitaalisen turvallisuuden hallintaa järjestämällä koulutuksia, tapahtumia ja käytännön harjoituksia, rakentamalla ja ylläpitämällä yhteistyöverkostoja sekä tuottamalla julkaisuja ja digitaalisen turvallisuuden hallinnollista tilannekuvaa.
(Digi- ja väestötietovirasto)

Hankintapohjien esittely ja käyttöohjeita

SaaSec-hankkeessa on tuotettu SaaS-hankintojen turvallista ja tuloksellista läpivientiä varten joukko esiselvitykseen, vaatimusmäärittelyyn, tarjouspyyntöön, vaikutustenarviointiin ja sopimukseen liittyviä pohjia SaaS-hankintaprosessin tueksi. Oppaan sisältämiä uusia sisältöjä ja pohjia on kehitetty hankkeessa järjestetyissä koulutuksissa ja työpajoissa pilvipalveluiden ja digitaalisen turvallisuuden asiantuntijoiden johdolla. Voit vapaasti ladata pohjia omaan käyttöösi. Pohjat ovat ladattavissa valtiovarainministeriön Tiimeri-työtilasta SaaSec-hankkeen kansiosta (vaatii kirjautumisen) sekä sipoo.fi-verkkosivuilta SaaS-palvelun hankinta- ja digiturvaoppaasta.

Lataa tästä: SaaSec-pohjat kootusti sipoo.fi:ssä

Pohjat täydentävät toinen toisiaan ja niitä tulee tarkastella aina kokonaisuutena, tapauskohtaisesti ja hankinnan laajuus huomioiden. Pohjat sisältävät täyttöohjeita. Hankintaprosessiin kannattaa osallistaa useita eri asiantuntijoita, kuten toimialojen substanssi-, IT-, tietoturva- ja tietosuoja-asiantuntijoita sekä lainsäädäntöä tuntevia hankinta-asiantuntijoita.

A: ESIKONSEPTOINTIPOHJA

Pohjan sisältö

- Pohja on tarkoitettu tietohallinnon ja substanssitoiminnan keskusteluun kiteyttämään, mitä hankinnassa tavoitellaan ja miten digitalisaatiolla voitaisiin uudistaa toimintaa

Pohjan käyttö

- Hyödynnetään tarvittaessa heti hankintaprosessin aluksi kiteyttämään, mitä tavoitellaan, mitä hankintaan kuuluu ja mitä ongelmaa käytännössä ratkaistaan

Hyödyt

- Saadaan dokumentoitua hankinnan käytännön tavoitteet ja kohde, jotta ratkaisuvaihtoehtoja voidaan arvioida tarkemmin

Kenelle

- Hankintaa tarvitsevalle substanssiyksikölle ja tietohallinnon vastuuhenkilölle

B: HYBRIDIHANKINTOJEN TARKISTUSLISTA JA TIIVISVAATIMUKSET

Pohjan sisältö

- Pohjassa on tiivis lista kysymyksiä ns. normaalille hankinnalle. Pohjan avulla voidaan tunnistaa, liittyykö yleiseen palvelu- tai laitehankintaan pilvipalveluita tai riippuvuuksia tietotekniikkapalveluihin.
- Pohjan avulla voidaan määrittää näiden alueiden päävaatimukset myös näihin hankintoihin.

Pohjan käyttö

- Käytetään tarkistuslistana hankinnoissa, joihin liittyy tavalla tai toisella tietotekniikan käyttöä (vaikka kunta ei itse ostaisikaan järjestelmää tai IT-palveluja)

Hyödyt

- Pystytään varmistamana tietoturvan, tietosuojan ja yhteentoimivuuden minimiehtojen täyttyminen myös muissa kuin ICT-hankinnoissa

Kenelle

- Hankinnan vastuuhenkilö, tietohallinnon yhteyshenkilö

C: TIETOTURVAN, TIETOSUOJAN JA JATKUVUUDEN ERITYISVAATIMUSTEN KOKOAMISPOHJA

- SaaS-hankintapaketissa on valmisteluvaiheeseen koottu yksinkertainen pohja tietoturvaa, tietosuojaa ja liiketoiminnan jatkuvuutta koskeville erityisvaatimuksille
- Huom. Hankintapohjissa on jo hyvä joukko valmiita perusvaatimuksia tietoturvalle ja tietosuojalle. Tähän pohjaan on tarkoitus koota vain tiivis joukko ERITYISvaatimuksia
- Selvitä tietoturva- ja tietosuojan erityisvaatimukset sekä erityisesti jatkuvuutta ja varautumista koskevat vaatimukset toimialalta. Näiden erityisvaatimusten tulisi heijastella erityisesti toimialan substanssitoiminnan erityistarpeita
- Näiden perusteella voit laatia tarkempia kysymyksiä järjestelmätoimittajille sekä arvioida, voidaanko järjestelmähankintaasi ylipäätään käyttää SaaS-ratkaisumallia

D: KÄYTTÖTAPAUSTEN KUVAUSPOHJA

Pohjan sisältö

- Järjestelmän käyttötapausten kuvaamisen pohja

Pohjan käyttö

- Tunnista esim. prosessikuvausten tai käyttötutkimuksen kautta keskeisimmät järjestelmän käyttötapaukset ja listaa ne ensin ko. pohjaan
- Kuvaa yksitellen omaan osakokonaisuutensa käyttötapaukset
- Hae palaute ja kommentit käyttötapauksiin toiminnalta

Hyödyt

- Saadaan täsmällinen malli, miten tietyissä tapauksissa järjestelmän odotetaan toimivan
- Ko. käyttötapauksia voidaan hyödyntää sekä järjestelmän käytettävyysarviossa että testitapauksina käyttöönotossa

Kenelle

- Käyttötapausten kuvaaja(t)

E: INTEGRAATIOIDEN KUVAUSPOHJA

- Pohjassa on sekä yksinkertainen listamuotoinen taulukko integraatioiden perustiedoista että toisella välilehdellä tarkempi yksittäisen integraation kuvauspohja
- Listaa vähintään keskeiset integraatiot listaan
- Kuvaa mahdollisuuksien mukaan tarkemmin kunkin integraation perustiedot sekä tekniset tiedot (kentät, sanomat, virheilmoitukset) excel-pohjan välilehdille siten, että yksi integraatio kuvataan aina omalle välilehdelleen. Tämä tarvitaan viimeistään toteutusvaiheessa.
- Hyödynnä mahdollisuuksien mukaan olemassa olevaa aineistoa (tekniset kuvaukset voidaan myös linkittää ko. pohjaan ja kuvata pohjaan vain perustiedot)

F: HINNAN KOKOLUOKKA-ARVIOPOHJA

Pohjan sisältö
Tähän pohjaan koottavan kustannusarvion tarkoitus on tuoda hankintayksikölle osana tarvemäärittelyä ja ratkaisuvaihtoehtojen kartoitusta kuva mahdollisesti hankittavan järjestelmäkokonaisuuden kustannuksista ylätasolla.
Pohjan käyttö
Tätä kustannusarviota käytetään hankittavan kohteen analyysin sekä budjetoinnin tukena sekä mahdollisesti tarjouspyynnön laatimisen tukena.
Pyytäkää tarjoajakandidaatteja täyttämään heidän ratkaisunsa hinnan kokoluokka-arvio tähän pohjaan.

G: PILVIRATKAISUN RISKIARVIOPOHJA

Pohjan sisältö
- Työkalu, jolla voidaan kattavasti arvioida pilviratkaisun (muidenkin kuin SaaS-palveluiden) riskejä. Sisältää valmiit riskiväittämät arvioitavaksi.

Pohjan käyttö
- Käykää tarvittaessa hankittavan pilviratkaisun riskien arvioimiseksi kaikki valmiit riskiluokat ja riskit läpi. Merkitkää arvionne riskin todennäköisyydestä, vahingon laajuudesta ja toipumisajasta.
- Pohja laskee riskikohtaisen riski-indeksin (0-100) ja ohjeistaa, milloin riskin vähentämisen keinot tulee käynnistää.
- Vastaava riskiarvio kannattaa tarvittaessa tehdä vertailun vuoksi myös On-premise -ratkaisusta.

Hyödyt
- Kattava riskiarvio valmiin mallin pohjalta

Kenelle
- Päätöksentekoa varten – voidaanko pilviratkaisu valita ratkaisuvaihtoehdoksi

K: VAATIMUSLOMAKE – YLEISET SAAS (TARJOUSPYYNNÖN LIITE 4)

Tässä dokumentissa kuvataan toimittajan asiakkaalle tarjoaman palvelun ja toimituksen sisältöä ja laatua koskevat vaatimukset ja selvityspyynnöt. Tämä dokumentti ja tarjoajien näihin antamat vastaukset muodostavat keskeiset arviointi- ja vertailuperusteet tarjouspyynnössä esitetyllä tavalla.

Vaatimuslomakkeen rakenne:

1. Palveluyhteistyö, tietoturva, tietosuoja
2. Toiminnalliset vaatimukset
3. Tekniset vaatimukset
4. Tuki ja ylläpito
5. Käyttöönotto
6. Asiantuntijapalvelut
7. Saavutettavuus ja käytettävyys

Pohjan sisältö

- Pohja sisältää yhdistettynä vaatimuslomakepohjan alueellisille SaaS-järjestelmille sekä joukon mallivaatimuksia ko. hankintaan

Pohjan käyttö

- Tarkista, että käytät oikeaa pohjaa oikeaan SaaS-hankintaan
- Tarkista pohjaan jätetyt mallivaatimukset ja niiden vaatimusluokat – muokkaa tarpeen mukaan
- Määritä ”Toiminnalliset vaatimukset” – näihin ei juuri ole valmiita mallivaatimuksia
- Laadi ”Selvitykset” ja niissä arvostettavat asiat – vain ko. arvostettavat asiat voidaan hyödyntää pisteytyksessä
- Päivitä Kooste-välilehdeltä vertailukriteerien painoarvot

Hyödyt

- Yhtenäinen, tarjouspyyntöön sovitettu vaatimusmalli

L: MALLIVAATIMUKSET – SAAS-HOSTING

Huom. Pohja L on tarkoitettu hyödynnettäväksi pääkäyttötilanteessa ”Olemassa olevan palvelun siirtäminen On-premisestä SaaSiksi”.

Pohjan sisältö

- Pohja on tarkoitettu olemassa olevan järjestelmäsopimuksen SaaS-hosting -liitesopimuksen erityisehtoliitteeksi siirryttäessä On-premise → SaaS

Pohjan käyttö

- Pohja olettaa, että järjestelmän ja yhteistyön pääehdot on jo kuvattu olemassa olevassa sopimuksessa
- Pohja sisältää keskeiset päävaatimukset SaaS-hostingille

- Muokkaa ja täydennä tarpeen mukaan

Hyödyt

- Mahdollistaa yksinkertaisen tavan täydentää olemassa olevaa sopimusta siirryttäessä kesken sopimuskauden On-premise → SaaS

M: SAAS-HINTALOMAKE (TARJOUSPYYNNÖN LIITE 5)

Pohjan sisältö

- Hintalomakkeella kootaan järjestelmän ja palvelujen hinnat sekä lasketaan automaattisesti näistä vertailuhinta, jonka mukaan tarjouksen hintapisteet määräytyvät

Pohjan käyttö

- Käytetään tarjouspyyntöä koottaessa. Suositellaan kuitenkin, että jo markkinakartoituksessa pyydetään karkeita kustannusarvioita sekä hintakomponentteja (esim. hinnoiteltavat moduulit) pohjalla F
- Täytä kunnan volyymit ja tarkista rakenne

Hyödyt

- Yhtenäinen pohja, jossa on eritelty tarjousvertailun vertailuhintaosuus sekä sopimukseen tuleva yksikköhinnoittelu toisistaan

N: HANKINNAN KOHDE -KUVAUSPOHJA (TARJOUSPYYNNÖN LIITE 1)

Pohjan sisältö

- Pohjan tarkoituksena on kuvata tarjoajille, mitä olet hankkimassa ja minkälaiseen ympäristöön.

Pohjan käyttö

- Täydennä pohjan tekstit olemassa oleviin otsikoihin. Hankinnan kohde palvelunäkökulmasta on jo listattu valmiiksi lukuun 2. Tämä kuvaa siis hankittavat palvelut, mutta EI MIHIN KOHTEESEEN = minkälaiseen järjestelmään ne kohdistuvat. Kuvaa tämä vielä erikseen.
- Huom. Kuvaa hankinnan kohdekuvauksessa VAIN: mitä ollaan hankkimassa, mistä se koostuu + lähtötilanne (mitä järjestelmiä tai integraatioita on lähtötilanteessa) + tavoitetilaa vain ylätasolla ja tavoitearkkitehtuuritasolla. ÄLÄ listaa tähän Hankinnan kohdeliitteeseen vaatimuksia, vaan kokoa kaikki vaatimukset tarjouspyynnön Vaatimuslomake-exceliin.

Hyödyt

- Tarjoajille syntyy selkeä kuva, mitä olet ostamassa

O: ARKKITEHTUURITIIVISTELMÄ

➔ O3 Liite 1.1: Arkkitehtuuritiivistelmä (.pptx)
➔ O4 Liite 1.1.1: KA-taulukot (.xlsx)

Voit arkkitehtuuritiivistelmän lisäksi hyödyntää KA-taulukoita keskeisimpiin osakuvauksiin.

P: TARJOUSOHJEET JA VERTAILUPERUSTEET (TARJOUSPYYNNÖN LIITE 6)

Pohjan sisältö

- Kuvaa tarjouspyynnössä tarjoajalle, miten sen tulee laatia tarjouksensa ja miten kunta arvioi tarjoukset

Pohjan käyttö

- Käy pohja läpi ja päivitä:
  - Painoarvot
  - Tarkista pisteytyskaavat
  - Tarkista tuleeko mukaan tiimihaastattelu ja tiimitehtävä tai työnäyte tai käytettävyysarviointi – muokkaa tämän pohjalta
- Älä tee juurikaan muita muutoksia kuin ohjeistetut – tätä terminologiaa ja pisteytysmallia on hiottu markkinaoikeuden päätösten pohjalta hartaasti. Jos olet epävarma, kysy ja pyydä vahvistusta.

Hyödyt

- Täsmällinen malli varmistaa hankintalainmukaisuuden

Tutustu myös tiedostoon

➔ Lisävihjeet hankintapohjien käyttö (.pdf)

SaaSec-hanke lyhyesti

Kuinka kunnan tulee toimia, jotta SaaS-mallin pilvipalvelun digitaalinen turvallisuus voidaan varmistaa palvelun elinkaaren kaikissa vaiheissa? SaaSec-hankkeen tuotoksena valmistuu SaaS-palvelun hankinta- ja digiturvaopas, joka sisältää ohjeita ja työkaluja palvelun määrittelyvaiheen, hankintavaiheen ja päättämisvaiheen lisäksi palvelun käytön aikaisen valvonnan sekä auditoinnin järjestämisen tueksi.

Tietoa SaaSec-hankkeesta Sipoon kunnan verkkosivuilta

SaaSec-hanke on saanut avustusta valtiovarainministeriöltä kuntien digitalisaation kannustinjärjestelmästä.

Tietoa digitalisaation kannustinjärjestelmästä valtiovarainministeriön verkkosivuilta

Hankkeeseen osallistuvat kunnat: Hyvinkää, Kirkkonummi, Nurmijärvi, Sipoo, Tuusula ja Vihti
Hankkeen toiminta-aika: 1.10.2021 – 30.9.2023
Kokonaisbudjetti: 250 000 €, josta VM:n myöntämä tuki 85 % ja kuntien rahoitusosuus 15 %

Käsitteitä ja sanastoa

Tähän osioon on koottu SaaSec-hankkeen oppaassa käytettyjä käsitteitä ja sanastoa. Käsitteitä ja lyhenteiden merkityksiä on avattu oppaassa myös tapauskohtaisesti niiden maininnan yhteydessä. Lisäksi kannattaa tutustua Digi- ja väestötietoviraston Sanastot-työkaluun erityisesti kokonaisarkkitehtuurin, lokihallinnan, tiedonhallintalautakunnan suositusten sekä VAHTI-riskienhallintasanastojen osalta.

Tutustu Sanastot-työkaluun tästä

Pilvipalvelut (Cloud Services)

Pilvipalvelut ovat ’pilvessä’ tarjottavia, tarvittaessa käyttöönotettavia palveluita. Pilvipalvelua voi käyttää tietokoneella ja mobiililaitteilla internetin kautta – sen käyttö vaatii vain nettiyhteyden. Pilvipalvelu ei ole konkreettisesti käyttäjän omalla tietokoneella, tai organisaation omalla palvelimella, vaan pilvipalvelun tarjoavan yrityksen palvelimella.

Useimmiten pilvipalvelusta puhuttaessa tarkoitetaan SaaSia, eli palvelua, jossa asiakkaan vastuulla on ainoastaan käyttäjähallinta sekä palveluun syötetty tieto.

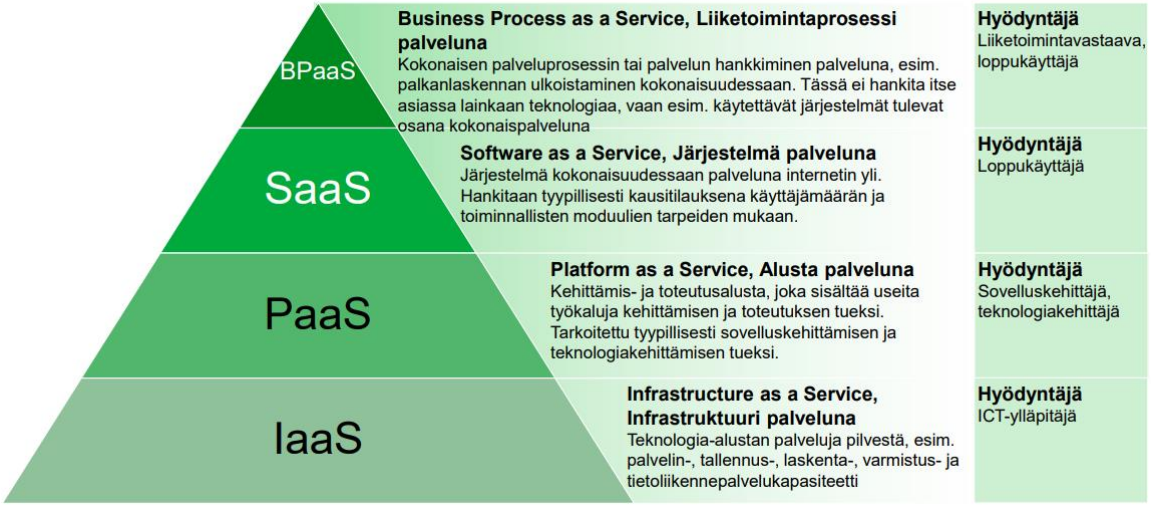
Pilvipalveluiden palvelumallit

BPaaS (Business Process as a Service = Liiketoimintaprosessi palveluna)
Kokonaisen palveluprosessin tai palvelun hankkiminen palveluna, esim. palkanlaskennan ulkoistaminen kokonaisuudessaan. Tässä ei hankita itse asiassa lainkaan teknologiaa, vaan esim. käytettävät järjestelmät tulevat osana kokonaispalvelua.

SaaS (Software as a Service = Ohjelmisto palveluna)
Pilvessä sijaitseva ohjelmisto, johon organisaatio tai yritys ostaa käyttöoikeuden palveluntarjoajalta. SaaS-palvelussa tietokoneelle ei yleensä tarvitse asentaa mitään ohjelmia, vaan se toimii internetin välityksellä. Hankitaan tyypillisesti kausitilauksena käyttäjämäärän ja toiminnallisten moduulien tarpeiden mukaan.

PaaS (Platform as a Service = Alusta palveluna)
Kehittämis- ja toteutusalusta, joka sisältää useita työkaluja kehittämisen ja toteutuksen tueksi. Tarkoitettu tyypillisesti sovelluskehittämisen ja teknologiakehittämisen tueksi.

IaaS (Infrastructure as a Service = Infrastruktuuri palveluna)
Teknologia-alustan palveluja pilvestä, esim. palvelin-, tallennus-, laskenta-, varmistus- ja tietoliikennepalvelukapasiteetti.



Kuvio: Pilvipalvelujen soveltamisohje - Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille (Valtiovarainministeriö)

Pilvipalveluiden toteutusmallit

Julkinen pilvi (Public)

- Koko pilvi-infrastruktuuri ja sen palvelut ovat rajoittamattomasti sopimusasiakkaiden käytössä.
- Palveluntarjoaja toteuttaa täysin läpinäkyvästi ratkaisun ja palvelujen fyysisen alustan. Asiakas maksaa vain käyttämästään palvelusta.

Hybridipilvi (Hybrid)

- Julkisen ja oman pilven yhdistelmäratkaisu
- Julkinen pilvi on jatkettu omaan pilveen

Yhteiskäyttöpilvi (Community)

- Usean saman viiteryhmän tai yhteisön toimijan yhteinen pilvipalvelu (esim. valtion pilvipalvelu, turvallisuustoimijoiden pilvipalvelu).

Oma yksityinen ratkaisu (On-premise)

- On Premise -ratkaisussa laitteet sijaitsevat omassa konesalissa oman organisaation tiloissa.
- On Premise -ratkaisu ei täytä edellä kuvattuja pilvipalveluiden ominaisuuksia. Käytännössä kyse on organisaation virtuaalialustasta tai virtuaalipalvelusta.

Lähde: Tuottavuutta pilvipalveluilla – Ohje julkisen hallinnon pilvipalvelujen hyödyntämiseen (Valtiovarainministeriö)

Digitaalinen turvallisuus

Tietoturva

Tietoturvalla varmistetaan tietojen luottamuksellisuus, eheys ja käytettävyys. Tietoturvaan sisältyy muun muassa tietojen, tietoaineistojen, laitteistojen,

ohjelmistojen, tietoliikenteen, tilojen ja toiminnan turvaaminen. Tietoturva liittyy läheisesti tietosuojaperiaatteiden toteuttamiseen.

Tietosuoja
Tietosuoja tarkoittaa perusoikeutta, joka turvaa jokaisen oikeuksia ja vapauksia henkilötietojen käsittelyssä. Tietosuoja määrittelee ne periaatteet, milloin, millä edellytyksillä ja miten henkilötietoja voidaan käsitellä.

Kyberturvallisuus
Siinä missä tietoturvalla tarkoitetaan tiedon käytettävyyttä, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta. Kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Kybertoimintaympäristö on yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö.
(Lähde: Turvallisuuskomitea – Kyberturvallisuuden sanasto)

Auditointi
Auditointi on suunnitelmallinen arviointi / selvitys, jossa verrataan toimintaa, ohjeistusta ja vaatimuksia. Auditoinnin avulla selvitetään toiminnan ja ohjeistuksen mahdolliset puutteet ja kehittämiskohdat. Jotta auditoinnissa saadut tulokset olisivat luotettavia, auditoinnin on oltava järjestelmällistä ja riippumatonta. Organisaatio voi itse arvioida, onko vaatimuksia noudatettu (sisäinen auditointi) tai palkata työhön kolmannen osapuolen (ulkoinen auditointi).

Standardisointi
Standardisointi on yhteisten toimintatapojen laatimista ja niiden kirjaamista lopputuotteeseen, standardiin. Standardi on määritelmä siitä, miten jokin asia tulisi tehdä. Standardisointi lisää parhaiden ratkaisujen käyttöä ja samalla laatua, yhteentoimivuutta ja turvallisuutta. Tärkeää on myös toteutusten läpinäkyvyys eli se, että vaatimukset ovat avoimesti saatavilla ja että vaatimusten täyttyminen voidaan todentaa.

Akkreditointi
Akkreditointi tarkoittaa toimijan pätevyyden toteamista puolueettomasti ja riippumattomasti. Akkreditointi yhdenmukaistaa vaatimusten tulkintaa ja lisää yhteentoimivuutta. Akkreditoidun toimijan tuottamien palveluiden laatuun ja standardin tulkintaan voidaan luottaa. Sertifioinneissa tulisi käyttää vain akkreditoituja toimijoita.

Sertifiointi
Sertifioinnin tarkoituksena on osoittaa organisaatiolle tai tuotteelle määriteltyjen vaatimusten täyttyminen. Vaatimukset perustuvat useimmiten kansainvälisiin standardeihin. Sertifioinnista myönnetään kirjallinen todistus, sertifikaatti, joka on todistus vaatimusten täyttymisestä.

Esimerkki, kuinka määritelmät liittyvät toisiinsa:

1. Sertifiointi perustuu tehtävään arviointiin (auditointi).
2. Arvioinnin kriteereinä käytetään useimmiten yhtä tai useampaa kansainvälisesti tunnettua standardia (esimerkiksi ISO 9001 -laatujärjestelmä) tai jotakin toimiala- tai aihekohtaista muuta standardia (esimerkiksi ISO 27001 - tietoturvallisuusstandardi).
3. Virallinen, kansainvälisesti tunnustettu sertifiointi edellyttää, että arvioinnin tekee ja sertifikaatin myöntää taho, jolla on hyväksyntä (akkreditointi) suorittaa kyseistä arviointia ja todistusten myöntämistä.

Henkilötietojen käsittely

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilötietoja ovat esimerkiksi nimi, puhelinnumero, sijaintitiedot ja isovanhempien perinnöllisiä sairauksia koskevat tiedot.

Erityisiin henkilötietoryhmiin kuuluvia henkilötietoja ovat sellaiset tiedot, joista ilmenee henkilön rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveyttä koskevia tietoja, seksuaalinen suuntautuminen tai käyttäytyminen, geneettisiä ja biometrisiä tietoja henkilön tunnistautumista varten. Erityisiin henkilötietoryhmiin kuuluvia tietojen käsittely on lähtökohtaisesti kielletty. Tietoja on suojeltava erityisen tarkasti, koska niiden käsittely voi aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille.

Rekisterinpitäjä on ihminen tai organisaatio, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjä voi olla esimerkiksi jäsenistään tietoja keräävä yhdistys, potilastietoja käsittelevä sairaala, verkkokauppa tai sosiaalisen median palvelu.

Henkilötietojen käsittelijä on ihminen tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi olla esimerkiksi toisen yrityksen markkinointia hoitava markkinointitoimisto tai IT-palveluntarjoaja, jolla on pääsy rekisterinpitäjän henkilötietoihin.
(Lähde: Tietosuojavaltuutetun toimisto)