# Huoltovarmuutta pilvipalveluilla

- päättäjän opas ja kortit liiketoiminnan jatkuvuuden hallintaan ja varautumiseen

Huoltovarmuusorganisaatio

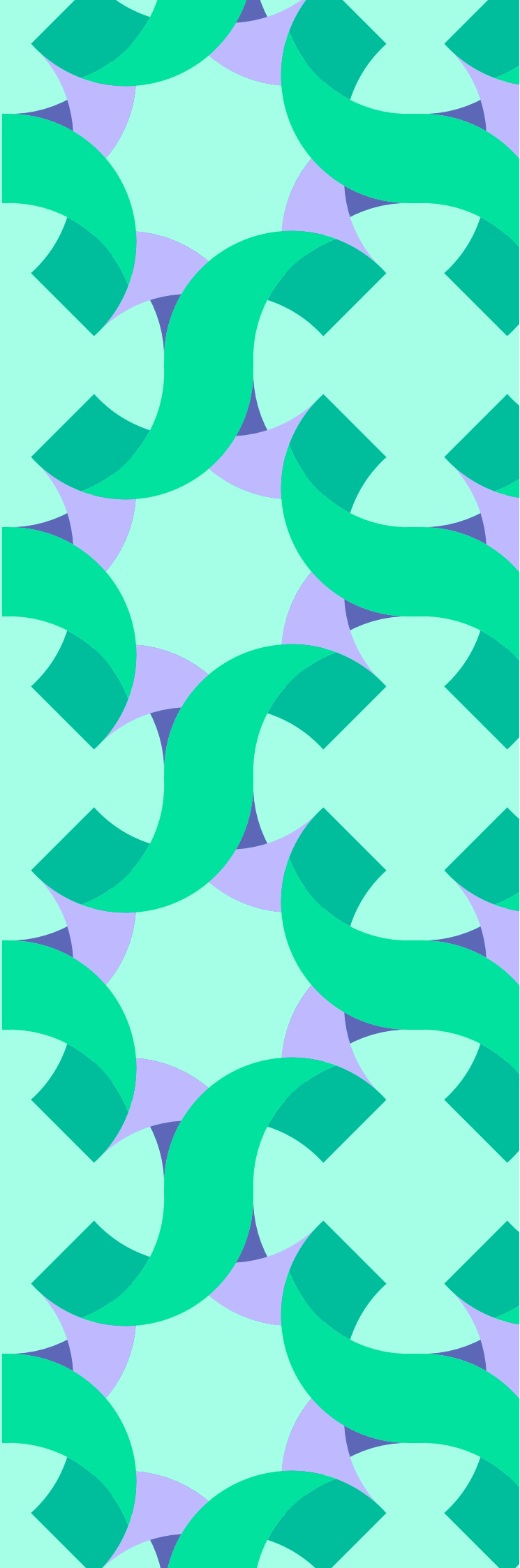
Huoltovarmuusorganisaatio

## www.huoltovarmuuskeskus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa. Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

**Julkaisija:**
Huoltovarmuusorganisaatio, Digipooli.
Huoltovarmuusorganisaatio on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus ja sen hallitus, huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit.

**Kuvat:** GettyImages
**Taitto:** LM Someco Oy
**Julkaisuvuosi:** 2023
**ISBN:** 978-952-7470-22-0



# Sisältö

# Johdanto

Voinko viedä yritykseni liiketoiminta- ja huoltovarmuuskriittisiä toimintoja ja tietoja pilveen? Ovatko pilvipalvelut aina riski vai voiko niitä käyttää jopa varautumisen välineenä?

Tämä opas on tarkoitettu yrityspäättäjille, jotka harkitsevat pilvipalveluiden käyttöönottoa tai käytön laajentamista kriittisiin toimintoihin. Oppaan tarkoitus on auttaa sinua tunnistamaan millä tiedoilla ja perusteilla päätöksiä pilvipalveluiden käyttöönotosta kannattaa tehdä ja miten varmistua, että jatkuvuudenhallinta ja huoltovarmuus on päätöksissä huomioitu.

Pilvipalveluja käytetään yrityksissä jo laajalti. Pilvipalveluiden hyödyt kuten erinomainen skaalautuminen, ketteryys, kustannukset käytön mukaan ja hyvät tietoturvatyökalut houkuttavat. Kriittisten toimintojen osalta pilvipalveluiden käyttöönotolle on ymmärrettävästi suurempi kynnys.

Päätöstä pilvipalveluiden käytöstä ei pidä tehdä pelkkien hyötyjen perusteella. Pilvipalveluiden käyttöönotto voi aiheuttaa muutoksia jatkuvuudenhallintaan ja se muuttaa yrityksen riskiprofiilia ja osaamistarvetta. Pilvipalvelumalleja ja palveluntarjoajia on lukuisia ja ne sopivat eri tarpeisiin.

Pilvipalvelut eivät sovi jokaiseen tarkoitukseen, mutta välillä niiden käytön tai harkinnan esteenä on liian negatiiviset tulkinnat ja uskomukset. Kansainvälinen ja Suomen lainsäädäntö ei suoraan estä pilvipalveluiden käyttöä. Suurin osa määräyksistä ei ota kantaa pilvipalveluihin, vaan luo vaatimuksia toteutustavasta riippumatta. Tuntemalla lait, määräykset sekä oman alan erityissääntelyn on mahdollista tehdä tietoon perustuvia päätöksiä.

Tarvitset päätöksentekoa varten ymmärryksen yrityksesi kriittisistä toiminnoista ja datasta, lainsäädännön ja toimialan vaatimuksista, toimintaanne kohdistuvista uhkista ja riskeistä, sekä mahdollisista muista erityispiirteistä, jotka asettavat vaatimuksia ratkaisuvaihtoehdoille.

Tämä opas ja sen päätöksenteon avuksi luotu korttipakka auttavat sinua läpi päätösprosessin kuvaamalla päätösprosessin vaiheet ja kunkin vaiheen tarvittavat tiedot, tehtävät ja roolit. Opas auttaa huomioimaan jatkuvuudenhallinnan ja huoltovarmuuden päätöksenteossa riippumatta päädytkö pilvipalveluihin vai et.

## Pilvipalvelut jatkuvuudenhallinnan ja huoltovarmuuden välineenä

Huoltovarmuus on yrityksesi kriittisten toimintojen jatkuvuuden varmistamista ja häiriöihin varautumista. Pilvipalveluita ei tarvitse nähdä vain riskinä huoltovarmuudelle, vaan oikein käytettynä ne voivat olla jatkuvuudenhallinnan ja huoltovarmuuden edistäjiä.

Jatkuvuudenhallinnan keskiössä on ongelmiin varautuminen ja jos mahdollista, niiden ratkaisu jo ennen kuin ne muuttuvat todeksi. Esimerkiksi jos yritykselläsi on kriittinen tietojärjestelmä, sen ongelmat voivat estää tai vakavasti haitata liiketoimintaa.

Pilvipalvelut tarjoavat välineitä jatkuvuudenhallintaan. Perinteisissä konesalitoteutuksissa järjestelmän kuormituksen lisääntymiseen täytyy varautua etukäteen ja mitoittaa ne suurimman kuormituksen mukaan. Pilvipalveluissa kasvavaan ja laskevaan kuormitukseen reagointi eli skaalautuminen on nopeampaa ja helpompaa. Tämä vähentää tilanteita, joissa kriittinen järjestelmä ei ole ylikuormituksen takia käytettävissä. Pilvipalveluissa kustannukset syntyvät käytön mukaan, mikä tarjoaa kustannussäästöjä ja vähentää suuria etukäteisinvestointeja.

Järjestelmien kahdennus ja siten yksittäiseen maantieteelliseen sijaintiin perustuvan riskin pienentäminen, varmuuskopioiden tai edelliseen toimivaan versioon nopeasti palaaminen ja esimerkiksi palvelunestohyökkäyksiin varautuminen on pilvipalveluissa yleensä mutkatonta eikä vaadi kohtuuttomia investointeja.

Etenkin suuret pilvipalveluntarjoajat ovat investoineet miljardeja tietoturvaan. Pilvipalveluista löytyy tietoturvatyökaluja ja -mekanismeja joiden saavuttaminen perinteisessä konesalimaailmassa olisi vaativaa. Asianmukaisten kovennusten toteutus vaatii toki molemmissa ympäristöissä aiheeseen liittyvää osaamista.

Perinteiseen konesaliin verrattuna pilvipalvelut muuttavat yrityksesi riskiprofiilia. Tietyt riskit pienenevät, kun taas toiset vaativat enemmän huomiota. Myös osaamistarve muuttuu. Pilvipalveluiden hyötyjen kotiuttamisessa ja riskien välttämisessä kaiken keskiössä on oikeanlainen osaaminen. Pilvipalveluiden vastuunjakomalli eroaa usein perinteisestä konesalista. Tilaajalla on vähemmän näkyvyyttä ja kontrollia “pellin alle”, jolloin vaatimuksenmukaisuuden todentaminen perustuu enemmän sopimuksiin, sertifiointeihin, riskiarviointeihin ja vastaaviin.

Pilvipalvelumalleja ja palveluntarjoajia on useita erilaisia ja kullekin niistä on käyttötarkoituksensa. Tämä opas keskittyy julkipilvipalveluihin, mutta käy läpi muutkin mallit. Itse päätöksentekoprosessi, jonka lopputuloksena valitaan konesali, julkipilvipalvelu tai jokin välimuoto, pysyy kuitenkin kaikissa tapauksissa samana.

## Lukijalle

Tämän Huoltovarmuusorganisaation toteuttaman oppaan tarkoitus on edistää yritysten pilvipalveluiden ja erityisesti julkipilvipalveluiden käyttöä jatkuvuudenhallinta ja huoltovarmuus huomioiden sekä niiden välineenä.

Tämä opas ja sen "Tunnista ja turvaa" -korttipakka auttavat sinua tekemään valistuneita päätöksiä, milloin ja millä reunaehdoilla kriittisiä toimintoja ja tietoja voi viedä pilveen siten, että olet myös huomioinut riittävät huoltovarmuuden, jatkuvuudenhallinnan, tietoturvan ja tietosuojan näkökulmat. Opas auttaa yritystäsi tekemään hyviä, tietoon ja hallittuihin riskeihin perustuvia päätöksiä myös muunlaisissa tietojärjestelmien uudistuksissa ja käyttöönotoissa.

### Oppaan sisältö

Opas koostuu kahdesta osasta. Ensimmäisen osan keskeinen sisältö on

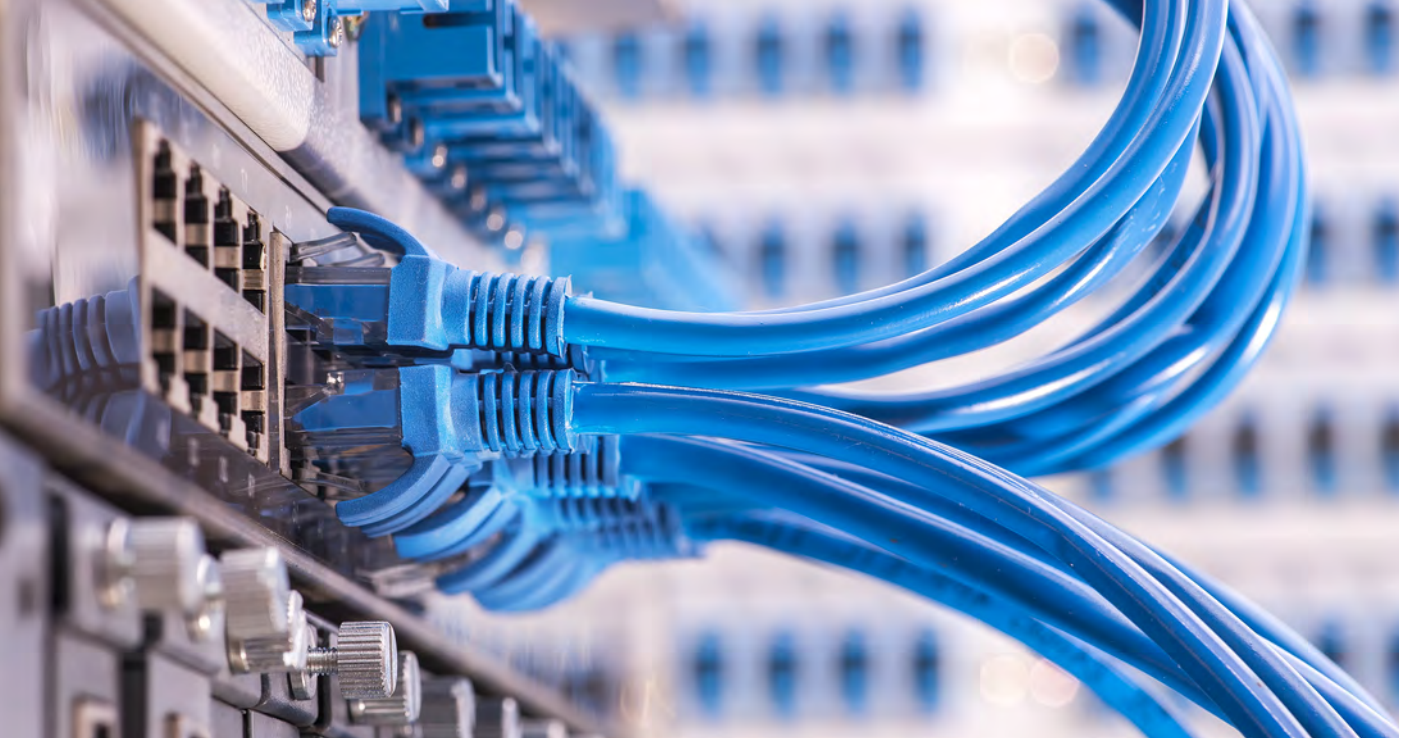
- **Johdanto** kertoo miksi tämä opas kannattaa lukea ja avaa tärkeimmät käytetyt termit
- **Pilvipalveluiden käyttö kriittisissä toiminnoissa** auttaa silloin kun yritys pohtii pilvipalveluiden käyttöönottoa. Se auttaa ymmärtämään:
  1) mitä pilvipalvelut tarkoittavat, mitkä ovat niiden hyödyt ja mitä eri palvelumalleja on,
  2) miten sääntely vaikuttaa niiden käyttöönottoon,
  3) miten päätösprosessi menee ja
  4) miten niitä käytetään turvallisesti
- **Jatkuvuudenhallinta kriittisissä toiminnoissa** auttaa tunnistamaan ja priorisoimaan kriittiset toiminnot sekä niiden uhat ja miten pilvipalveluiden käyttö vaikuttaa uhkiin varautumiseen

Toinen osa on "Tunnista ja turvaa" -korttipakka. Korttien esimerkkien avulla sinun on helpompi ymmärtää mitä päätösvaiheessa tulisi konkreettisesti tehdä ja ketä tarvitaan mukaan. Voit käydä kaikki kortit läpi tai poimia juuri sinun yrityksesi tilanteelle oleelliset kortit.

### Tämä opas vastaa seuraaviin kysymyksiin

- Mitä pitää huomioida, jos harkitsemme pilvipalveluita liiketoiminta-, huoltovarmuus- tai regulaatiokriittisten tietojen ja toimintojen kohdalla?
- Miten pystymme tekemään tietoon perustuvia päätöksiä pilvipalveluiden käyttöönotosta?
- Mitä tehtäviä, tietoja ja rooleja kuhunkin päätöksentekovaiheeseen liittyy?
- Miten varmistamme, että huoltovarmuus ja liiketoiminnan jatkuvuus on huomioitu riippumatta, mihin teknologisiin ratkaisuihin päädymme?

Oppaan toteutuksessa on ollut mukana kattavasti eri toimialoilta pääosin suomalaisia huoltovarmuuskriittisiä ja niille palveluja tarjoavia organisaatioita: Avanade, Digia, DigiFinland, Digi- ja väestötietovirasto (DVV), Elisa, Elo, Enerim, Ficom, Fingrid, Futurice, Huoltovarmuuskeskus, IBM, Kela, Microsoft, Nixu, Päijät-Hämeen hyvinvointikuntayhtymä, Reaktor, Sanoma, SK ID Solutions (Viro), Suomen Pankki, Säästöpankkiryhmä, Teknologiateollisuus, TietoEvry, WithSecure ja YTK.



## Keskeiset määritelmät

Alla määritelmät oppaassa useasti käytetyistä termeistä ja mitä niillä tässä oppaassa on tarkoitettu. Tarkemmat määrittelyt ja lisää määritelmiä löydät liitteestä 1.

**Huoltovarmuus**
Huoltovarmuudella tarkoitetaan kykyä ylläpitää sellaisia yhteiskunnan perustoimintoja, jotka ovat välttämättömiä yhteiskunnan toimivuuden, väestön elinmahdollisuuksien, turvallisuuden ja maanpuolustuksen turvaamiseksi poikkeusoloissa ja vakavien häiriötilanteiden aikana. Se tarkoittaa myös sellaisen yritysten toimintaedellytysten varmistamista, jotka osallistuvat edellä mainittuihin toimintoihin tai toimitusketjuihin.

**Huoltovarmuuskriittinen organisaatio**
Organisaatio, joka on merkittävä yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta, on huoltovarmuuskriittinen. Huoltovarmuuskriittinen organisaatio voi olla yritys tai muu organisaatio. On myös paljon yrityksiä, jotka tuottavat palveluita huoltovarmuuskriittisille organisaatioille, esim. tietoliikennepalveluita viranomaiselle. Tällöin yrityksen näitä palveluita tuottava osa tai toiminto on huoltovarmuuskriittinen.

**Kriittinen toiminto**
Tässä oppaassa keskitytään kolmenlaisiin yrityksen kriittisiin toimintoihin: liiketoimintakriittisiin toimintoihin, huoltovarmuuskriittisiin toimintoihin ja regulaatiokriittisiin toimintoihin. Niihin kaikkiin viitataan tässä oppaassa termillä *kriittinen toiminto*. Sama toiminto voi olla kaikkea kolmea yhtä aikaa tai vain osaa näistä. Esimerkiksi regulaatiokriittinen toiminto ei ole välttämättä liiketoimintakriittinen, mutta sen jatkuvuuden turvaaminen on silti tärkeää.

Liiketoimintakriittinen toiminto on yrityksen liiketoiminnan jatkuvuudelle välttämätön toiminto, jota ilman yritys ei voi toimia. Esimerkiksi pääasiassa verkkokauppaa tekevälle yritykselle verkkokaupan tilausjärjestelmä on **liiketoimintakriittinen toiminto.**

Huoltovarmuuskriittisellä toiminnolla on vaikutusta Suomen huoltovarmuuteen, eli kykyyn ylläpitää yhteiskunnan perustoimintoja. Esimerkiksi teleoperaattorin matkapuhelinverkon ylläpito on **huoltovarmuuskriittinen toiminto.**

Regulaatiokriittiseen toimintoon liittyy sellainen viranomaisvelvote, jota oletuksena täytyy noudattaa myös kriisin aikana. Esimerkiksi finanssialan viranomaisraportointivelvollisuus on regulaatiokriittinen toiminto.

**Pilvipalvelu**
Pilvipalvelu tarkoittaa palvelumallia, jossa palveluntarjoaja tarjoaa tietojenkäsittelykapasiteettia tai -palvelua, jonka tuottamisessa hyödynnetään tyypillisesti jaettuja ja skaalautuvia resursseja. Usein pilvipalveluista maksetaan käytön mukaan ja niiden käyttöönotto tai käyttäminen voi olla osin automatisoitua. Pilvipalveluista löytyy erilaisia palvelu- ja toteutusmalleja.

# Pilvipalveluiden käyttö kriittisissä toiminnoissa

Tämä luku pyrkii käymään tiiviissä muodossa läpi sen, mitä pilvipalveluista täytyy tietää ennen päätöksentekoa. Tässä luvussa käydään läpi mitä pilvipalvelut ovat, eri pilvipalvelumallit ja pilvipalveluiden hyödyt. Sääntelyn vaikutus pilvipalveluiden käyttöönottoon esitetään tiiviisti. Tässä luvussa on myös erillinen kappaleensa pilvipalveluiden turvallisen käytön perusperiaatteisiin niihin tilanteisiin, jossa pilvipalveluiden käyttöönottoon on päädytty tai päätymässä.

## Mitä pilvipalvelut ovat?

Jokainen ICT-järjestelmä ja digipalvelu, oma tai muualta hankittu, pyörii jollain palvelimella. Karkeasti ottaen voidaan tehdä jako kahteen: **konesali**-termi tiivistettynä tarkoittaa, että yrityksellä on oma tai vuokrattu konesali, jossa he itse tai palveluntarjoajan toimesta pyörittävät palvelimia ja palveluita. **Pilvipalvelu**-termi taas eroaa konesalista siten, että konesali on palveluntarjoajan vastuulla ja tilaajalle tarjotaan korkeampaa jalostusastetta.

Suurin erottava tekijä konesalin ja pilvipalvelun välillä on vastuu ja palveluaste. Vaikka yrityksellä olisi vuokrattu konesali, jota operoi palveluntuottaja, joudutaan silti ratkomaan kysymyksiä fyysisiin palvelimiin ja konesalitiloihin liittyen. Esimerkiksi varautumaan jonkun palvelun kuormituksen kasvamiseen hankkimalla lisää palvelimia tai varautumalla konesalirikkoon vuokraamalla toinen konesali fyysisesti eri paikasta. Nämä vaativat usein suuria etukäteisinvestointeja ja esimerkiksi varalle hankittu palvelin aiheuttaa jatkuvia kustannuksia vaikkei sille olisi käyttöä.

Pilvipalveluissa palveluntarjoaja vastaa tästä fyysisestä tasosta. Mitä korkeamman jalostusasteen pilvipalvelu, sitä suuremman osan vastuusta palveluntarjoaja kantaa. Korkeampi palveluaste mahdollistaa myös kustannukset käytön mukaan. Kun kasvaneeseen kuormitukseen voidaan reagoida nopeasti ja automaattisesti, kustannukset syntyvät aidon käytön mukaan, mikä voi tarjota suuria kustannushyötyjä ja parempaa varautumisen astetta.

Pilvipalveluita tarjoavat pienemmät ja suuremmat, kansalliset ja kansainväliset yritykset. Suurimpien palveluntarjoajien kohdalla puhutaan “hyperskalaareista”, joiden etuna on lähes rajaton skaalautuminen sekä todella laaja paletti eri palveluita esimerkiksi tietokantaratkaisujen, verkotuksen tai ajoympäristöjen osalta. Yleensä palvelut hinnoitellaan käytön mukaan, mikä mahdollistaa kustannustehokkaat ratkaisut.

### Pilvipalvelut muuttavat vastuunjakoa - kontrollista luottamukseen

Pilvipalveluiden käyttö tarkoittaa, ettei yrityksellä ole enää välttämättä suoraa määräysvaltaa tai kontrollia siihen, miten palvelua tuotetaan. Vain harva pilvipalveluntarjoaja päästää konesaliinsa yrityksiä tai heidän kumppaneitaan tekemään auditointeja. Tilaaja joutuu luottamaan palveluntarjoajaan ja muilla keinoin, kuten sopimuksin, sertifioinnein ja vastaavin, varmistumaan palveluntarjoajan luotettavuudesta ja määräysten mukaisuudesta.

Pilvipalveluita tuleekin lähtökohtaisesti käsitellä kuin mitä tahansa muita ulkoistuksia tai ICT-palveluiden hankintaa. Jos yritys on ennen käyttänyt vain omaa konesaliaan ja omaa IT-osastoaan sen ylläpitoon, palvelumallin muutos voi olla suuri. Tämän oppaan “Tunnista ja turvaa” -korttipakka auttaa kartoittamaan ja hallitsemaan tätä riskiprofiilin muutosta.

Tämä opas keskittyy etenkin julkisiin pilvipalveluihin, joskin päätöksentekoprosessi sopii kaikkiin eri pilvipalvelumalleihin ja myös konesaliin.

### Tärkeimmät termit

**Oma konesali (on-prem)** tarkoittaa, että organisaatiolla on oma palvelintila ja he itse tuottavat konesalipalvelua. Vaihtoehtoisesti yrityksen omaa konesalia operoi ulkoinen palveluntuottaja, organisaatio itse operoi palveluntuottajan konesalin heille varattua osaa tai palveluntuottajalta on vuokrattu sekä konesali että sen operointi.

**Julkiset pilvipalvelut (public cloud)** ovat kaikille tarkoitettuja palveluita, jossa palveluntarjoaja hoitaa osan tai lähes kaiken palvelimiin liittyvästä ylläpidosta ja vastuusta ja tarjoaa asiakkailleen korkeampaa abstraktiotasoa palveluna. Esimerkiksi virtuaalipalvelimia (IaaS), jolloin fyysisistä palvelimista ei tarvitse huolehtia,

ajoalustaa toteutukselle (PaaS) tai jopa valmista ohjelmistoa palveluna (SaaS).

**Yksityinen pilvipalvelu (private cloud)** on tietylle yritykselle tuotettu palvelu. Palveluntarjonta on rajatumpaa kuin julkisissa pilvipalveluissa, samoin kustannukset voivat olla korkeammat. Yksityinen pilvipalvelu voi olla rakennettu turvallisuus edellä, esimerkkinä Suomen Huoltovarmuusdatan pilvipalvelu.*[1]

**Hybridipilvi (hybrid cloud)** tarkoittaa oman konesalin ja pilvipalvelun yhdistämistä. Hyötynä on se, ettei pilvipalveluun tarvitse monistaa niitä palveluita, joita konesalista jo tarjotaan.

Lue lisää liitteestä 1, kohdasta “Pilvipalvelu ja konesali”

## Päätös pilvipalveluiden käyttämisestä

Päätös pilvipalveluiden käyttämisestä kriittisissä toiminnoissa tai varautumisen välineenä on harvoin helppo. Hyvä uutinen on kuitenkin se, että päätöksentekoprosessi itsessään ei suuremmin eroa muista ulkoistus- tai teknologiapäätöksistä. Päätösprosessi pysyy varsin samana riippumatta siitä, päädyttekö julkipilveen, yksityiseen pilvipalveluun vai omaan konesaliin.

### Päätösprosessi tiivistettynä

Tämän oppaan “Tunnista ja turvaa” -korttipakka auttaa sinua läpi päätösprosessin. Se kuvaa mitä vaiheita päätöksentekoprosessiin kuuluu, mitkä ovat kunkin vaiheen tarvittavat esitiedot ja tehtävät ja mitä rooleja prosessiin tarvitaan mukaan. Korttipakan avulla varmistat, että päätökset pohjautuvat tietoon ja jatkuvuudenhallinnan sekä huoltovarmuuden teemat on huomioitu.

Alla esimerkki, miten korttipakkaa voi hyödyntää pilvipalveluiden käyttöönottoon liittyvässä päätöksentekoprosessissa:

1) Varmista, että yrityksellläsi on elementit hyvään päätöksentekoprosessiin, esimerkiksi tarvittavat pohjatiedot ja oikeanlaista osaamista.
   - Katso “Tunnista ja turvaa” -korttipakan kortti “Aloita tästä kortista”.
2) Kiteytä liiketoimintatarve ja -hyöty.
   - Katso kortti “Aloita muutos tästä”.
3) Tarkastele muutoksen kohteena olevaa toimintoa. Ymmärrä mitä tietoa, prosesseja ja tietojärjestelmiä teillä on jo nyt, ja mikä on muuttumassa.
   - Katso kortit “Tunnista kriittiset toiminnot”, “Tunnista kriittiset tiedot”, “Tunnista muutoksen kohteena oleva tieto”.
4) Selvitä, mitä reunaehtoja laki ja määräykset asettavat toiminnallenne.
   - Katso kortti “Tunnista lainsäädännön ja toimialan vaatimukset”.
5) Kartoita ja rajaa toteutusvaihtoehtoja aiemmin kartoitettujen tarpeiden, hyötyjen ja reunaehtojen avulla.
   - Katso kortti “Tunnista toteutusmahdollisuudet ja teknologiat”.
6) Kartoita mitä tarpeita muutokseen liittyy, esimerkiksi muuttuuko osaamistarve tai riskiprofiili ja riskienhallintakäytännöt.
   - Katso kortit “Tunnista muutoksessa tarvittava osaaminen ja resurssit”, “Tunnista kriittisten toimintojen uhkat ja riskit”.
7) Nyt kun on tiedossa mikä, miten ja miksi muuttuu sekä mitä muutos vaatii onnistuakseen, on päätöksen aika. Pelkkä valistunut päätös ei vielä takaa onnistumista. Muutoksen läpivienti, tarvittavan osaamisen hankinta ja mahdolliset yrityksen toimintatapojen muutokset ovat haastavia tehtäviä ja ne vaativat resursointia ja huomiota.
   - Katso kortti “Varmista onnistunut muutos”.

### Päätösprosessin mahdolliset lopputulemat

Jokaisen yrityksen eri vaatimukset, painotukset ja lähtötilanne vaikuttavat päätösprosessin lopputulokseen. Alla on kuvattu vaatimuksia ja rajauksia, jotka karsivat mahdollisia ratkaisuvaihtoehtoja.

**Tiedon sijainti sekä lainsäädäntö**
Tämän oppaan lainsäädäntöluku käy läpi, miten lait eivät tällä hetkellä ota pahemmin kantaa pilvipalveluihin itsessään, mutta voivat rajata esim. missä tieto voi fyysisesti sijaita:

- Ei rajoitusta: Kaikki kansainväliset pilvipalveluntarjoajat käyvät.
- EU/ETA-alue: Useimmat kansainväliset pilvipalveluntarjoajat mahdollistavat resurssien luonnin halutulle maantieteelliselle alueelle.
- Suomi: Nykyään myös monelta isoimmalta pilvipalveluntarjoajalta löytyy konesali Suomesta. Suomessa on myös paljon paikallisia pilvipalveluntarjoajia.

*1 Suomen Huoltovarmuusdata Oy on Huoltovarmuuskeskuksen omistama yritys, joka tarjoaa erityisen turvallisia konesali- ja yksityispilvipalveluita huoltovarmuuskriittisille organisaatioille.

**Tietoturva ja luottamus**

Pilvipalveluntarjoajat investoivat massiivisesti palveluidensa tietoturvaan ja tarjoavat työkaluja ja parhaita käytäntöjä heidän asiakkailleen. Maineriskin takia on palveluntarjoajien etu, asiakkaiden tietoturva on hyvässä kunnossa. Pilvipalvelut vaativat kuitenkin aina luottamuksen palveluntarjoajaan, koska usein tilaajalla ei ole mahdollista tehdä tai teettää auditointeja. Riippuen kontrollin tarpeesta, ratkaisuvaihtoehdot muuttuvat:

- Luottamus palveluntarjoajiin: kaikki ratkaisut käyvät.
- Suurempi vaatimus omalle kontrollille: yksityiset pilvipalvelut, konesalit sekä sellaiset pienemmät pilvipalveluntarjoajat, joiden toimintaa voi auditoida.
- Suurin vaatimus omalle kontrollille: vain oma tai sopivin ehdoin vuokrattu konesali.

**Riskiprofiili**

Kyky sietää riskejä on yrityskohtaista. Kyse ei ole vain riskin määrästä, vaan riskien tyypistä. Esim. mediatalon tärkein tehtävä on jakaa informaatiota ja tällöin tiedon saatavuus on tärkeintä. Jollekin toiselle yritykselle tietojen luottamuksellisuus on saavutettavuutta tärkeämpää.

- Tiedon saatavuus tärkeintä: julkiset pilvipalvelut helpottavat hyvää tiedon saatavuutta.
- Tiedon eheys tärkeintä: pilvipalveluissa tiedon eheyden varmistus on usein omaa konesalia helpompi toteuttaa. Esim. yhden konesalin tai maantieteellisen sijainnin tuhoutuminen ei hävitä tietoa, kun se on pilvipalvelussa oikein hajautettu.
- Tiedon luottamuksellisuus tärkeintä: yksityinen pilvipalvelu sekä konesalit parempia vaihtoehtoja.

Muita riskiin vaikuttavia tekijöitä voivat olla:

- Jos palveluiden täytyy toimia myös silloin kun kansainväliset tietoliikenneyhteydet ovat poikki, sopivia ratkaisuja ovat kansalliset konesalit, kansalliset pilvipalvelut sekä hybridiratkaisut.
- Jos edes teoreettinen mahdollisuus valtiolliseen tiedusteluun on mahdotonta sietää, sopivia ratkaisuja ovat tällöin konesalit sekä ne kansalliset pilvipalveluntarjoajat, jotka eivät itse käytä kansainvälisiä tai tietyn alueen palveluita oman toimintansa pohjalla.
- Lainsäädäntöriski. Esim. EU:n ja Yhdysvaltojen väliset sopimukset tietojen vapaasta liikkuvuudesta ovat jatkuvassa käymistilassa, mikä voi vaikuttaa joidenkin yritysten haluun käyttää yhdysvaltalaisia palveluntarjoajia.

**Yrityksen tilanne**

Päätöksentekoon vaikuttaa myös yrityksen tai sen asiakkaiden tilanne.

- Yrityksen osaaminen. Pilvipalvelut vaativat erilaista osaamista kuin konesalit, eikä uudelleenkoulutus ole nopeaa. Osaamista tarvitaan kattavasti ja esimerkiksi pilvipalveluiden erilainen vastuunjako- ja sopimusmalli vaatii osaajaa.
- Kustannukset. Tietyissä tapauksissa kustannukset ohjaavat pilvipalveluihin ja konesalista luopumiseen. Ne yritykset, jotka eivät voi luopua konesalista, eivät välttämättä saa pilvipalveluista suurinta kustannushyötyä.
- Asiakkaiden tilanne. Esimerkiksi asiakkaille on voitu luvata pitää tiedot Suomessa tai yritys tuottaa palvelua julkishallinnon organisaatiolle, jolla voi olla tiukemmat vaatimukset palveluntarjoajiensa toiminnalle.

**Hybridiratkaisut**

Päätöksen ei tarvitse olla joko-tai. Alla esimerkkejä tällaisista tilanteista:

- Yrityksellä on omassa konesalissaan osa kriittisistä palveluista ja loput kansainvälisessä pilvipalvelussa. Pilvessä olevat palvelut voivat hyödyntää konesalin tietoja ennalta määrättyjen sääntöjen mukaisesti.
- Yrityksen asiakkaan tietojen täytyy sijaita omassa konesalissa. Yritys päättää kuitenkin käyttää pilvipalveluita sovelluskehityksessä ja saada sieltä ketteryyshyötyjä.
- Yrityksen kriittisen palvelun täytyy toimia silloinkin, kun kansainväliset tietoliikenneyhteydet ovat poikki, mutta palvelu saa olla hetken kriisitilanteessa pois käytöstä. Tällöin palvelua voidaan tuottaa pilvipalvelusta, mutta hätätilanteessa varalla on konesali, joka saadaan käyttökuntoon tunneissa.
- Yritys ei voi ottaa riskiä tietojen päätymisestä muiden maiden tiedusteluorganisaatioille. Kansainvälisiä pilvipalveluita voi kuitenkin hyödyntää ei-sensitiivisen tiedon osalta tai sensitiivisen tiedon kohdalla varmuuskopioalustana salaamalla tiedot ennen pilvipalveluun lähettämistä (“bring your own key” -malli).

## Pilvipalveluiden hyödyt

Pilvipalveluiden hyödyistä löytyy paljon materiaalia, esimerkiksi Sote-tietojärjestelmät pilvipalveluina -ohjeesta. Alla tiivistettynä keskeisimpiä hyötyjä.

**Ylivertainen skaalautuminen**
Etenkin suuremmat pilvipalvelualustat skaalautuvat lähes loputtomasti. Oikein toteutettuna, pilvipalvelut pystyvät reagoimaan kuormaan nopeasti ja lähes rajoituksetta. Esimerkiksi yritys tarjoaa kriittistä kuluttajapalvelua, jonka kävijämäärä satakertaistuu kuukauden alussa. Pilvipalveluiden avulla palvelu ei suurellakaan kuormalla muutu hitaaksi tai kaadu.

**Ketterä ja joustava tapa käyttää resursseja**
Yksi pilvipalveluiden suurimpia hyötyjä on ketterä resurssien hyödyntäminen. Perinteisessä palvelinympäristössä resurssien hankkiminen kestää, ne pitää mitoittaa suurimman kuormituspiikin mukaan ja muutostyöt vaativat ihmistyötä. Pilvipalveluissa oikein käytettynä resursseja voidaan käyttää aidosti tarpeen mukaan ja resurssimuutokset tapahtuvat usein lähes välittömästi. Esimerkiksi uuden kehitysympäristön ja sen vaatimien resurssien luonti voi tapahtua minuuteissa eikä päivissä.

**Resilienssi ja vikasietoisuus toteutettavissa ilman merkittäviä lisäkustannuksia**
Pilvipalvelualustojen avulla varautuminen tyypillisimpiin ongelmiin ja niistä palautuminen ei vaadi merkittäviä investointeja:

- Maantieteellinen hajauttaminen vähentää yksittäiseen datakeskukseen liittyvää riskiä.
- Kahdentaminen mahdollistaa itsestään palautuvat järjestelmät. Jos esim. tietokantoja on käytössä useita, yhden kaatuessa voidaan automaattisesti nostaa toinen tilalle, eikä loppukäyttäjä välttämättä edes huomaa tätä.

**Pilvipalvelut mahdollistavat nopean ja kustannustehokkaan palautumisen**
Pilvipalveluiden suurimpia valtteja on automaattinen, nopea ja joustava tapa luoda resursseja. Tämä mahdollistaa vikatilanteista palautumisen ilman suuria investointeja:

- Varalla olevat "kylmät" järjestelmät, joihin voidaan siirtyä vikatilanteessa minuuteissa.
- Yksittäinen palvelu tai koko tuotantojärjestelmä voidaan nopeasti palauttaa uuteen sijaintiin ja halutessa jättää vanha jäljelle virheenselvitystä varten.
- Vanhan ja uuden järjestelmän ajo rinnakkain jonkun aikaa ja automaattinen liikenteen ohjaaminen vanhaan järjestelmään, jos uudessa järjestelmässä on ongelmia.

### Pilvipalveluiden hyötyjen konkretisoituminen vaatii osaamista ja suunnittelua

Pilvipalveluiden hyötyjen, kuten ketteryyden ja kustannussäästöjen konkretisoituminen vaatii, että pilvipalveluita osataan käyttää oikein. Samoin hyvän tietoturvan ja tietosuojan saavuttaminen vaatii osaamista siitä huolimatta, että pilvipalveluntarjoajat tarjoavat hyviä työkaluja asiakkaidensa käyttöön.

Pilvipalvelut ovat tehokas työkalu ja jokaista työkalua voi käyttää väärin. Etenkin pilvipalvelualustoissa on lähes rajaton määrä mahdollisuuksia, joiden mukaan palveluita rakentaa. Aivan kuten konesalissakin, on mahdollista tehdä inhimillisiä tai osaamisen puutteesta johtuvia virheitä, joiden takia esimerkiksi luottamuksellinen tieto valuu julkiverkkoon.

Pilvipalvelut kuitenkin tarjoavat usein mekanismeja ja parhaita käytäntöjä, jotka ohjaavat turvalliseen käyttöön ja virheiden ja riskien minimointiin sekä mahdollisten poikkeamien tunnistamiseen.

Pilvipalveluiden hyötyjen konkretisoituminen vaatii siis suunnitelmallisuutta, osaamista ja parhaiden käytäntöjen noudattamista. Usein hyötyjen saaminen vaatii myös yrityksen toimintatapojen muuttamista. Esimerkiksi yritys on ennen voinut rajata palvelimien tilaamisen vain IT:lle, ja liiketoiminnan on erikseen pitänyt sitä heiltä pyytää. Pilvipalveluissa tällaista rajaamista on usein turha tehdä ja sopivilla turvamekanismeilla liiketoimintayksiköt voivat päättää isosta osasta pilviresurssejaan tarpeen mukaan joustavasti. Pilvipalveluiden hallintamalli mahdollistaa tasapainottelun vapauden ja järkevien keskitettyjen päätösten välillä.

Pilvipalveluiden turvallisesta käytöstä löydät tästä oppaasta oman lukunsa.

## Pilvipalveluiden sääntely

Suurimmalta osin EU- ja kansallinen lainsäädäntö ja määräykset eivät ota kantaa pilvipalveluihin itsessään, etenkään silloin kun kyse on yksityisesti yrityksestä. Yritysten täytyy tuntea mitkä lait ja määräykset koskevat heitä ja heidän toimintaansa, koska esimerkiksi tietoturvaan ja tietosuojaan liittyviä määräyksiä pitää noudattaa samalla tavalla oli toteutusvaihtoehtona oma konesali, yksityinen pilvipalvelu tai suuren kansainvälisen pilvipalveluntarjoajan alusta.

Kun puhutaan tiedon säilyttämisestä tai prosessoinnista, on karkeasti kolmenlaisia säädöksiä, jotka voivat aiheuttaa velvoitteita ja reunaehtoja pilvipalveluiden käytölle: henkilötietojen käsittely, tiettyjen alojen erityissääntely ja ne julkiseen hallintoon liittyvät säädökset, joita yritys joutuu noudattamaan jostain syystä.

Alla on kuvattu todella tiiviisti keskeisimpiä näistä. Löydät lisää tietoa Sote-tietojärjestelmät pilvipalveluina -ohjeesta sekä Huoltovarmuusorganisaation Digipoolin FiComilta tilaamasta “Pilvipalveluiden juridinen selvitys” -dokumentista.

Säädökset, eli lait, asetukset, direktiivit ja määräykset ovat velvoittavia. Suositukset eivät ole velvoittavia, mutta suosituksia on voitu antaa helpottamaan säädöksen noudattamista. Ohjeistukset eivät ole koskaan velvoittavia.

On paljon tilanteita, jossa lain tulkinta ei ole selvä. Esimerkiksi valtion eri organisaatiot ovat tehneet hyvin erilaisia tulkintoja ja siten päätyneet eri lopputuloksiin pilvipalveluiden käytöstä. Sääntelyn jatkuva muuttuminen tekee ohjeistuksista vanhentuneita nopeasti. Käytä tarvittaessa lakiapua ajantasaisen tiedon saamiseksi.

### Henkilötietojen käsittely

GDPR on tunnetuin ja keskeisin säädös, joka pitää huomioida myös pilvipalveluita käytettäessä. Se ei ota suoraan kantaa pilvipalveluihin, mutta asettaa vaatimuksia henkilötiedon käsittelylle toteutustavasta riippumatta.

Eurooppalaisten henkilötietojen käsittely ja säilyttäminen tulee tapahtua EU/ETA-alueella ja tarvittaessa rekisterinpitäjän täytyy tehdä tietosuojaa koskeva vaikutusarviointi. Henkilötietoja voi siirtää EU/ETA-alueen ulkopuolelle, mikäli siirrolle on olemassa siirtoperuste.

Löydät siirtoperusteet esim. Pilvipalveluiden juridinen selvitys -dokumentista. Kyseinen selvitys myös avaa ongelmaa henkilötietojen siirtämiseksi Yhdysvaltoihin. Aiemmin Privacy Shield -päätös mahdollisti siirtoperusteen täyttymisen, koska Yhdysvaltojen tietosuojan tason nähtiin olevan EU-komissiolle riittävä. Ns. Schrems II -ratkaisun myötä tämä päätös pyörrettiin.

Euroopan Tietosuojaneuvostolta on tullut 18.1.2023 julkaisu pilvipalveluiden käytöstä julkishallinnossa etenkin GDPR:ään ja sen oikeaoppiseen käyttöön liittyen. Vaikka lausunto onkin julkishallinnolle tarkoitettu, se on erinomainen ohjeistus myös yrityksille ja avaa tarkemmin, miten käsitellä henkilötietoja oikeaoppisesti.

### Tiettyjen alojen erityissääntely

Sosiaali- ja terveysalan erityissääntely on kuvattu hyvin Sote-tietojärjestelmät pilvipalveluina -ohjeessa. Monella muulla alalla ei ole omaa erityistä lainsäädäntöä tiedon säilyttämisestä ja pilvipalveluiden käytöstä. Alalla saattaa olla kuitenkin valvontaviranomainen, jolla on omia ohjeistuksiaan aiheeseen liittyen. Esimerkiksi Finanssivalvonta on ohjeistanut vakuutusalan toimijoita ja Liikenne- ja viestintävirasto päivittää teletoiminnan tietoturvaa koskevaa määräystä. Näitä käydään läpi tarkemmin Pilvipalveluiden juridinen selvitys -dokumentissa.

### Julkishallinnon lainsäädäntö vaikuttaa yrityksiin

Yksityiset yritykset eivät lähtökohtaisesti joudu noudattamaan julkishallinnolle tarkoitettuja määräyksiä. On kuitenkin tilanteita, jossa yritys joutuu huomioimaan nämä säädökset, esimerkiksi toimiessaan palveluntarjoajana julkishallinnon organisaatiolle tai viranomaiselle.

Myöskään julkisella puolella kategorista kieltoa pilvipalveluiden käytölle ei ole. Oikeastaan päinvastoin, valtiovarainministeriön kanta on pilvimyönteinen.

**Valtiovarainministeriön lausunto julkisen hallinnon pilvipalveluiden käytöstä**
Valtiovarainministeriö on antanut lausunnon julkisen hallinnon pilvipalveluiden käytöstä. Lausunnon tärkein sisältö mainitsee mm.

- Pilvipalvelu pitäisi ensisijaisesti valita silloin kun se tarjoaa parhaan hyödyn eikä muita esteitä sen valitsemiselle ole.
- Pilvipalveluita pitäisi käsitellä kuten muitakin ICT-hankintoja tai muutoksia. Erityistä huomiota on kiinnitettävä sopimuksiin, jatkuvuudenhallintaan ja saatavuuteen.
- Julkisen tiedon käyttöä ei rajoiteta. Ei-julkista tietoa voi myös käsitellä pilvipalveluissa, mutta tietoturvan ja tietosuojan täytyy olla riittävällä tasolla.

Vaikka tämä suositus on annettu julkiselle hallinnolle, sen sisältö ja parhaat käytännöt ovat relevantteja myös yksityisyrityksille.

**Asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa**
Valtioneuvoston asetus turvallisuusluokiteltavista asiakirjoista sisältää vaatimuksia, joita julkishallinto joutuu noudattamaan. Se voi välillisesti koskettaa niitä yrityksiä, jotka operoivat tai toteuttavat julkishallinnolle turvallisuusluokiteltuja asiakirjoja käsitteleviä palveluita. Etenkin korkeimpien turvallisuusluokkien kohdalla asetus asettaa sellaisia rajoituksia pilvipalveluille, että se voi estää käyttämästä tiettyjä palveluntarjoajia.

"Pilvipalveluiden juridinen selvitys" -dokumentissa on avattu tarkemmin, miten lainsäädäntö vaikuttaa pilvipalveluiden käyttöön julkishallinnossa.

## Toimialan suosituksiin ja standardeihin tukeutuminen

Yrityksesi voi olla toimialalla, jota valvoo viranomainen. Heiltä voi tulla suosituksia, jotka epäsuorasti vaikuttavat pilvipalveluiden käyttöönottoon. Esimerkkinä tästä on finanssialan Finanssivalvonta. Suositukset eivät ole lakeja, mutta valvottavien yritysten täytyy läpäistä valvojan tarkastukset. Silloin kun suosituksia ei ole noudatettu, yritys joutuu hyväksytysti perustelemaan valitsemansa toimintamallin. Finanssivalvonnalla on valtuus määrätä uhkasakkoja ja rajoittaa toimiluvan mukaista toimintaa.

EU:n NIS2-direktiivi pyrkii kasvattamaan tietoturvan tasoa jäsenmaissa. Tämä näkyy siten, että erityissäänneltyjen alojen määrä kasvaa. Kannattaa selvittää oman yrityksen toimialan osalta, onko uusia vaatimuksia luvassa. Huomaa, että direktiiveistä johtuva lainsäädäntö saa lopullisen muotonsa vasta tullessaan osaksi kansallista lainsäädäntöä. NIS2 ja huoltovarmuuskriittisiin organisaatioihin liittyvä CER-direktiivi luultavasti päätyvät osaksi Suomen lainsäädäntöä kesällä 2024 (NIS2) ja 2025 (CER).

Standardit kuvaavat kansallisia tai kansainvälisiä parhaita käytäntöjä. Osa standardeista on vapaaehtoisia, jolloin niiden noudattaminen ja sertifioituminen auttavat palvelun laadusta ja vaatimustenmukaisuudesta viestimisessä ja arvioinnissa.

Tietyillä toimialoilla standardien noudattaminen on edellytys alalla toimimiseen. Esimerkiksi Payment Card Industry Data Security Standard (PCI DSS) on tietoturvastandardi yrityksille, jotka käsittelevät luottokorttiostoksia. Standardi on suurimpien luottokorttiyhtiöiden yhdessä luoma ja sen noudattaminen on edellytys luottokorttien käyttämiseen.

PCI DSS on tyypillinen esimerkki standardista, joka määrittelee tarvittavan tietoturvan tason ottamatta suoraan kantaa sen toteutukseen. Yritys joutuu täten varmistamaan riippumatta käytetystä teknologiasta, noudattaako toteutus PCI DSS -standardia.

Joskus standardien noudattaminen, esimerkiksi ISO/IEC 27001 -sertifiointi, voi olla käytännössä pakollista yrityksille kilpaillulla markkinalla pärjäämiseksi. Vaikka sertifiointi olisikin yrityksen vapaaehtoisesti hankkima, tulee sen säilyttäminen huomioida tulevissa tietojärjestelmäuudistuksissa.

Sekä yritys ja yrityksen käyttämä palveluntarjoaja molemmat joutuvat täyttämään standardien ehdot. Sertifioinneissa ja standardeissa vastuullanne on selvittää, että käyttämänne palveluntarjoajat ovat myös sertifioituja. Etenkin suurimmat pilvipalveluntarjoajat ovat erittäin laajasti sertifioituja, koska se on heille kilpailuetu.

## Havaintoja lainsäädännön vaikutuksesta pilvipalveluihin

Suomessa on totuttu ajatukseen, että kriittisten tietojen säilyttäminen oman valtion rajojen sisällä omassa konesalissa on aina turvallinen vaihtoehto. Maailmalla on kuitenkin esimerkkejä valtioista, joissa on tietoisesti päätetty toisin.

Ukrainassa on lainsäädännön avulla määrätty osa julkisen hallinnon tiedoista ja toiminnoista siirrettäväksi myös valtion rajojen ulkopuolelle pilvipalveluihin. Tätä siirtoa on valmisteltu vuodesta 2014 ja pantu toimeen sodan sytyttyä. Viron Data Embassy mahdollistaa sen, että varmuuskopiot sekä osa kansalaisille kriittisistä palveluista on ajettavissa valtion rajojen ulkopuolelta. Tällöin kansalaisia voidaan palvella niissäkin tilanteissa, jossa valtion rajojen sisällä olevat konesalit tai infrastruktuuri ei ole enää käytettävissä.

Julkishallinnon asennoituminen pilvipalveluihin vaihtelee maittain. Suomessa suhtautuminen on yhtä aikaa hyvinkin positiivista, esim. Valtiovarainministeriön antama lausunto julkisen hallinnon pilvipalveluiden käytöstä, mutta käytännöt, traditio ja tulkinnat kuitenkin ohjaavat usein perinteisiin ratkaisuihin. Virossa julkishallinnon täytyy käyttää tietyissä tapauksissa pilvipalveluja, mutta samanlaista puskua kohti pilvipalveluja ei yritysmaailmalle ole.

Muuttuva kansallinen suhtautuminen turvallisuuteen voi muuttaa myös suhtautumista pilvipalveluihin. Kun selkeää kansallista päätöstä suosia tai kieltää pilvipalveluiden käyttöä ei ole, yritykset ja organisaatiot joutuvat tekemään omat päätöksensä.

Yritysten kannattaa valmistautua mahdolliseen muuttuvaan lainsäädäntöön. Esimerkiksi pilvipalvelujen kohdalla kyse ei ole vain siitä, mennäänkö pilvipalveluihin, vaan on hyvä varautua muihinkin skenaarioihin:

- Mahdollinen siirtymä pilvipalveluun,
- mahdollinen siirtymä pilvipalvelusta toiseen ja
- mahdollinen siirtymä pilvipalvelusta (takaisin) konesaliin.

Etenkin viimeinen vaihtoehto on tärkeää ottaa huomioon pilvipalveluun siirryttäessä ja yrityksenne kannattaa pohtia jo etukäteen näitä kysymyksiä: Missä tapauksissa siirto takaisin konesaliin olisi perusteltua? Millä tavalla aiomme varautua mahdolliseen siirtoon pilvestä toiseen tai takaisin konesaliin? Miten tasapainottelemme pilvinatiivien toteutusten ja pilvitoimittajariippumattomien toteutusten välillä? Onko riskiä toimittajaloukulle?

## Miten käyttää pilvipalveluita turvallisesti?

Tässä luvussa kuvataan karkeasti julkisten pilvipalveluiden ja -alustojen turvallisen käytön ja suunnittelun peruspilarit. Aihe on tekninen, mutta pyrkii yksityiskohtiin sukeltamisen sijaan ohjaamaan sinut oikeiden termien ja valmiiden konseptien äärelle saadaksesi paremman kokonaiskuvan. Tämän luvun yli voi hypätä ja palata siihen vasta kun päätös pilvipalveluiden käyttöönotosta konkretisoituu.

**Turvallinen pilvipalveluiden käyttö on riskienhallintaa**

Kuten tämän oppaan pilvipalveluiden sääntely -luvussa tuli ilmi, sääntely ottaa harvoin kantaa teknologiaan, vaan asettaa vaatimuksia yrityksille esimerkiksi ratkaisujen turvallisuudesta riittävällä tasolla. Tällöin riippumatta teknologiasta ja palvelumallista, tai siitä onko käytössä pilvipalvelu vai konesali, toteutus lopulta määrittää onko yritys toiminut hyväksyttävällä tavalla.

Turvallinen pilvipalveluiden käyttö tarkoittaa niitä suunnittelu- ja käyttövaiheen toimenpiteitä, joiden avulla voidaan pienentää riskin todennäköisyyttä ja vaikutuksia tietoturva- tai tietosuojapoikkeamille, pilvipalveluiden epäoptimaaliselle käytölle ja sille, että pakollisia vaatimuksia ei täytetä. Riskiin vaikuttaa vahvasti mukana olevien henkilöiden osaaminen koko palvelun elinkaaren ajan. Lue kortilta “Tunnista muutoksessa tarvittava osaaminen ja resurssit” lisää, miten varmistut tarvittavasta osaamisesta.

**Pilvipalveluiden turvallisen käytön peruspilarit**

Pilvipalveluiden turvallinen käyttö ei ole vain tekninen ongelma, vaan asiaan liittyy useita eri ulottuvuuksia. Alla on kuvattu tärkeimmät peruspilarit ja niihin liittyvät konseptit ja käsitteet:

- **Turvallinen jalansija**: miten varmistua heti ensimmäisistä askeleista lähtien, että pilvipalveluja käytetään laadukkaasti ja turvallisesti.
- **Pilven hallintamalli:** ajantasainen (etukäteis-) suunnitelma miten pilvipalveluita yrityksessä aiotaan käyttää ja hallita.
- **Standardien hyödyntäminen:** älä keksi pyörää uudelleen vaan hyödynnä alan parhaita käytäntöjä.
- **Tekninen toteutus:** miten rakentaa ja ylläpitää turvallisia palveluita.
- **Pilvipalveluiden valvonta ja hälytysmekanismit:** miten tunnistaa ja välttää ongelmatilanteet sekä pienentää niiden vaikutusta.
- **Laadukas ulkoistus:** miten varmistaa laadukas ja turvallinen ulkoistus ja alihankintaketju kautta linjan.

**Turvallinen jalansija**

Miten varmistetaan, että pilvipalveluiden käyttöönotto tehdään oikein heti ensimmäisestä askeleesta lähtien? Vaikka etenkin pilvipalvelualustat ovat usein hyvin muokattavia, tiettyjä asioita on vaikea tai erittäin työlästä muuttaa myöhemmin. Esimerkkinä pilvipalveluiden tilausrakenne ja arkkitehtuurin suuret linjat.

Etenkin suurten pilvipalvelualustojen tarjoajat ovat kirjoittaneet seikkaperäisiä ohjeistuksia tätä varten. Löydät ne hakusanalla: “Cloud Adoption Framework”. Kyseiset ohjeistukset auttavat sinua ymmärtämään, mitkä asiat pitää päättää ennen pilvipalvelun käyttöönottoa ja mitkä asiat voidaan päättää turvallisesti myöhemmin.

**Pilven hallintamalli**
Pilven hallintamalli (cloud governance) on yksinkertaisuudessaan sovitut ja dokumentoidut käytännöt, miten yrityksessäsi pilvipalveluita käytetään tai aiotaan käyttää. Päätä etukäteen ne asiat, joiden muuttaminen olisi kaikkein vaikeinta.

Hallintamalli ottaa kantaa mm seuraaviin asioihin:

- kustannusten hallintaan
- identiteetinhallintaan
- ylläpidon hallintaan
- tietoturvan ja lakien/vaatimustenmukaisuuden hallintaan
- datan hallintaan
- suorituskyvyn hallintaan
- resurssien ja konfiguraation hallintaan.

Osana hallintamallia toteutetaan usein "landing zone". Se on konkreettinen toteutus, jonka avulla hallintamallin päätöksiä jalkautetaan ja huolehditaan, että pilvipalvelualustan käyttö tehdään alusta asti oikein.

Esimerkiksi yritykset A ja B päättävät, että pilvipalvelualustassa saa luoda resursseja vain EU:ssa olevaan datakeskukseen. Molemmat yritykset kirjaavat asian hallintamalliinsa. Yritys B haluaa automatisoida tämän vaateen kontrollin. He luovat osana "landing zone" -toteutusta ohjelmallisen rajoituksen, joka estää käyttäjiä luomasta EU:n ulkopuolisia resursseja.

**Standardien hyödyntäminen**
Etenkin suuremmat pilvipalvelualustat ovat nimensä mukaan alustoja: niiden päälle voidaan rakentaa palveluita lukuisilla eri tavoilla. Aivan kuten konesalissakin, osaamispuute, huonot käytännöt tai inhimilliset virheet voivat johtaa huonosti tarpeen täyttävään ratkaisuun tai pahimmillaan tietoturvaongelmiin.

Yritysten omat pyrkimykset rakentaa työkaluja ja työtapoja asioiden oikein tekemiseksi ovat hyvä asia, mutta pyörää ei kannata keksiä uudelleen. Hyödynnä olemassa olevia parhaita käytäntöjä ja työkaluja. Tässä muutamia tärkeimpiä:

- **Well Architected Framework tai Cloud Architecture Framework** ovat pilvipalvelualustakohtaisia kokoavia ohjeistuksia, joilla pääsee hyvin alkuun. Ne kuvaavat kaikki näkökulmat tietoturvasta kulujen optimointiin juuri siinä pilvipalvelussa.
- **Pilvipalvelun oma ohjeistus** kuvaa suositellut tavat käyttää kutakin palvelua.
- Center for Internet Security, CIS benchmarks ovat valmiita ohjeita ja konfiguraatioita satojen eri palvelujen tietoturvan parantamiseksi. CIS standardeja on kaksi: taso 1 parantaa tietoturvaa ilman merkittävää haittaa muuhun toimintaan ja taso 2 on vielä tiukempi taso niihin erityistarpeisiin, jossa kustannuksia ja suorituskykyä ollaan valmiita uhraamaan tiukemman tietoturvan vuoksi.
- Open Web Application Security Project (OWASP) ylläpitää resursseja, joiden avulla yritykset voivat varmistua suunnittelemiensa ja toteuttamiensa web-palveluiden olevan tietoturvallisia. Tunnetuimmat materiaalit ovat OWASP Top 10, kymmenen yleisintä tietoturvaongelmaa ja miten ne estetään sekä Application Security Verification Standard (ASVS), joka on suunnittelun ja testauksen kriteeristönä käytettävä lista tietoturvavaatimuksista.
- Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) soveltuu pilvipalveluiden turvallisuuden arviointiin erityisesti silloin kun käsitellään viranomaisten salassa pidettävää tai turvallisuusluokiteltua tietoa.

**Tekninen toteutus**
Pilvipalveluiden turvallinen käyttö ei tapahdu vain suunnittelupöydällä, vaan turvallisuus on huomioitava koko palvelun elinkaaren ajan. Tästä syystä pilvipalvelukohtaista ja tietoturvaan liittyvää osaamista tarvitaan myös toteutus- ja ylläpitovaiheessa.

Pilvipalveluissa vaadittu osaaminen eroaa konesaliosaamisesta. Tämä täytyy huomioida rekrytoinnissa tai kumppanien hyödyntämisessä.

Alan hyvät käytännöt kannattaa ottaa haltuun. DevOps, DevSecOps ja Site Reliability Engineering -käytännöt auttavat rakentamaan laadukkaita palveluita tehokkaasti, riskien todennäköisyyttä ja vaikutusta pienentäen.

**Pilvipalveluiden valvonta ja hälytysmekanismit**
Valvonta mahdollistaa pilvipalveluiden ja pilvipalvelualustojen päälle rakennettujen palveluiden toiminnan seuraamisen sekä poikkeamien tunnistamisen. Hälytykset taas mahdollistavat poikkeamiin reagoinnin.

Kaikissa ICT-ratkaisuissa valvonta- ja hälytysratkaisut ovat osa laadukasta jatkuvuudenhallintaa. Pilvipalvelut eivät poikkea tästä. Pilvipalveluiden omat valvontatyökalut ovat usein laadukkaita ja integroituvat hyvin suosittuihin yrityksesi jo mahdollisesti käyttämiin ratkaisuihin. Mikään näistä ei kuitenkaan synny ilman osaavaa työtä.

**Laadukas ulkoistus**

Pilvipalveluiden käyttö tarkoittaa, että yritys ulkoistaa osan työstä ja vastuusta palveluntarjoajalle. Moni yritys myös käyttää kumppaneita pilvipalveluiden ylläpitoon. Molemmissa tapauksissa, aivan kuten kaikissa muissakin ICT-ulkoistuksissa, täytyy varmistua valitun palveluntarjoajan ja kumppanin pystyvän toimimaan sovitulla tavalla. Alla on hyvin tiivis lista keskeisiä asioita, joita yrityksen kannattaa kysyä itseltään ennen päätöksentekoa pilvipalveluiden käyttöönotosta.

1. **Vastuunjako**
   - Mikä on vastuunjako tilaajan ja palveluntarjoajan tai kumppanin välillä? Miten se on kuvattu palvelusopimuksissa? Mitä sopimusten rikkomisesta seuraa?
2. **Jatkuvuus**
   - Onko palveluntarjoaja tai kumppani riittävän vakavarainen yritys? Onko heidän jatkuvuudessansa riskiä? Entä jos he supistavat tai jopa lopettavat toimintansa?
3. **Tietoturvakäytännöt**
   - Millaisia teknisiä ja hallinnollisia tietoturvatoimenpiteitä palveluntarjoaja tai kumppani on toteuttanut? Millainen osaaminen ja resurssit heillä on tietoturvan ylläpitämiseen ja kehittämiseen?
   - Jos kumppanin tietojärjestelmiin tai tietokoneille murtaudutaan, voiko sitä kautta saada pääsyn tietojärjestelmiinne?
4. **Osaamisen hallinta**
   - Jos kumppani nojaa yksittäisten asiantuntijoiden osaamiseen, miten varmistetaan korvaavan asiantuntijan saanti esimerkiksi henkilöstön vaihtuessa tai loma-aikoina? Miten kumppanin työntekijöiden hallussa oleva tieto saadaan siirrettyä tarvittaessa myös yritykselle? Mihin tärkeät tiedot on dokumentoitu?
5. **Tiedon tallennus ja pääsynhallinta**
   - Millainen pääsy kumppanilla on yrityksen tietojärjestelmiin, tietoon ja toimitiloihin?
   - Miten luvattomalta pääsyltä ja käytöltä on suojauduttu ja miten sitä valvotaan?
6. **Maa, josta kumppani operoi**
   - Mikäli kumppani toimii eri maassa, sopimuksissa kannattaa määrittää, minkä maan lainsäädäntöä noudatetaan ristiriitatilanteissa.
   - Se mistä maasta kumppanin työntekijät operoivat, voi vaikuttaa mm. henkilötiedon käsittelyyn.

Huomaa, että rekisterinpitäjä vastaa aina palvelusta, vaikka sillä olisi alikäsittelijä. On rekisterinpitäjän vastuulla huolehtia, että alikäsittelijä on hoitanut vastuunsa sovitun mukaisesti. Sopimukset ja säännölliset läpikäynnit ovat hyviä tapoja huolehtia tästä vastuusta. Sopimuksissa on myös hyvä selvyyden vuoksi todeta tämä vastuu, vaikka se tulee jo laista.

# Jatkuvuudenhallinta kriittisissä toiminnoissa

Jatkuvuudenhallinnan tavoitteet ja se, millaisiin poikkeamiin ja uhkaskenaarioihin kannattaa varautua, riippuvat paljolti yrityksen toimialasta ja millaisia sen kriittisen toiminnot ovat. Tässä luvussa esitellään malli toimintojen kriittisyyden tunnistamiselle ja kuvataan miten pilvipalveluiden käyttö voi vaikuttaa erilaisiin jatkuvuutta uhkaavien skenaarioiden todennäköisyyteen tai vaikutuksiin. Lisäksi tässä luvussa esitellään, miten pilvipalveluita voi käyttää jatkuvuudenhallinnan välineenä ja miten lainsäädäntö voi vaikuttaa pilvipalveluihin.

## Mikä on kriittinen toiminto?

Aloita pohtimalla kaikkein kriittisimpiä toimintoja, joiden häiriöillä olisi vakavia vaikutuksia yrityksen kykyyn toimia, ylläpitää huoltovarmuutta tai täyttää viranomaisvelvoitteita. Muista tunnistaa myös riippuvuudet – useat eri toiminnot voivat olla riippuvaisia tietyistä keskitetyistä toiminnoista tai järjestelmistä, jolloin ne ovat välillisesti kriittisiä.

## Onko jatkuvuudenhallinta mitoitettu toiminnon kriittisyyden mukaan?

Jatkuvuudenhallinnassa “yksi koko sopii kaikille” -ajattelu ei ole järkevää. Mitä kriittisempi toiminto, sitä tiukemmat jatkuvuusvaatimukset siihen kohdistuvat. Tällä on suoria vaikutuksia prosesseihin ja teknisiin ratkaisuihin, joilla on taas vaikutuksia kustannuksiin.

Mitä tiukemmat jatkuvuusvaatimukset, sitä enemmän kustannuksia jatkuvuudenhallinta vaatii. Tästä syystä on välttämätöntä luokitella yrityksen toiminnot kriittisyyden mukaan ja mitoittaa jatkuvuudenhallinta kriittisyyteen sopivaksi.

### Mikä on jatkuvuudenhallinnan tavoite kriittisille toiminnoille?

Esimerkiksi kaksi toimintoa voivat olla yhtä liiketoimintakriittisiä, mutta niiden jatkuvuudenhallinta voi olla hyvin erilaista. Ensimmäisen toiminnon kohdalla tärkeintä voi olla, että tieto on saatavilla. Tällöin jatkuvuudenhallinta keskittyy saatavuuteen. Toisen toiminnon kohdalla tärkeintä voi olla tiedon eheys, jolloin saatavuusongelmat eivät välttämättä olekaan kriittisiä, mutta tiedon tahallinen tai tahaton muuttuminen on.

Aloita **tarpeen ymmärtämisestä**, eli mikä on toiminnon kriittisyys ja minkä jatkuvuutta toiminnossa täytyy turvata. Se auttaa seuraavaan askeleeseen, eli varmista **oikein mitoitettu jatkuvuusratkaisu**, jonka suorat ja välilliset kustannukset ovat linjassa kriittisyyden kanssa.

Tämän oppaan kortit “Tunnista kriittiset toiminnot”, “Tunnista kriittiset tiedot”, “Tunnista kriittisten toimintojen uhkat ja riskit” ja “Kirkasta jatkuvuuden tavoitteet ja harjoittele käytännöt” auttavat tässä tehtävässä.

## Mikä liiketoimintaa uhkaa? Hallittuja päätöksiä riskien hallintaan

Liiketoimintaa haittaavat uhkat voivat olla hyvin erilaisia yrityksestä ja organisaatiosta riippuen. Jotkin uhkaskenaariot, esimerkiksi tietoliikenneverkkojen laajamittaiset häiriöt tai kiristyshaittaohjelmat kurittavat yrityksiä miltei toimialasta riippumatta. Sen sijaan jotkin uhkat liittyvät vahvasti yrityksen toimialaan, toiminnan luonteeseen tai alalle tyypillisiin ohjelmistoihin.

Liiketoimintariskejä kartoittaessasi huomioi myös asiakkaidesi toimiala, tarjottavien palveluiden kriittisyys ja mahdollinen huoltovarmuusnäkökulma. Esimerkiksi, jos yrityksesi toimittaa tuotannonohjausjärjestelmän valvontapalvelua kemianteollisuuden tehtaalle, yrityksesi tai sen tietty toiminto voi olla tämän asiakkuuden takia huoltovarmuuskriittinen ja vaatia tiukempaa lähestymistä jatkuvuudenhallintaan ja riskien hallintaan.

Lue lisää jatkuvuudenhallinnan kehittämisestä, johtamisesta ja parhaista käytännöistä VAHTI 2/2016-ohjeesta Toiminnan jatkuvuuden hallinta. Ohjeessa on kuvattu muun muassa, miten toimintojen kriittisyyttä voi arvioida toiminnan vaikutusanalyysillä (Business Impact Analysis, BIA) ja priorisoida määrittämällä toiminnoille palvelutasot ja alimman hyväksyttävän palvelutason. Ulkoistuksissa on tärkeää kommunikoiden ja sopimuksin varmistaa kumppanien ja alihankkijoiden myös ymmärtävän palveluiden kriittisyys.

Vaikka uhkakuvat koskisivat kaikkia suomalaisia yrityksiä, yrityksesi kannattaa arvioida riskit itse. Etenkin tietoon ja kyberturvallisuuteen liittyvissä riskeissä puntaroi, onko tärkeintä tiedon luottamuksellisuus, eheys vai saatavuus. Pitääkö yrityksesi tuotannon jatkua taukoamatta vai onko tärkeintä se, että mitään tietoa ei häviä? Tämä vaikuttaa yrityksesi suunnitelmiin suojautua tunnistetuilta riskeiltä. **Riskien arvioinnissa kannattaa käyttää yrityksessäsi jo käytössä olevaa riskienarviointimenetelmää ja riskimatriisia,** jotta riskiarviot ovat yhteismitallisia.

Joskus mainehaitta satuttaa liiketoimintaa enemmän kuin itse häiriö. Viive ja epämääräisyys vähäistäkin tietoturvapoikkeamaa koskevassa viestinnässä voivat heikentää luottamusta asiakkaidesi ja suuren yleisön silmissä. Puutteellisesti täytetyt lupaukset esimerkiksi palvelun saatavuudesta tai tiedonkäsittelystä voivat aiheuttaa mainehaitan. Esimerkiksi jos yrityksesi on luvannut asiakkailleen tallentaa tiedot aina Suomeen, lupaus rajaa teknologisia ratkaisuja. Jos haluatte myöhemmin siirtyä käyttämään pilvipalvelua, jossa tiedot tallennetaan eurooppalaiseen konesaliin vähintään yhtä turvallisesti, asiakkaiden silmissä muutos näyttää silti huonolta.

Mikäli yrityksessä ei ole riskienhallintamenetelmää tai se vaikuttaa liian suppealta tähän tarkoitukseen, neuvoja saa mm. VAHTI-ohjeesta 22/2017 Ohje riskienhallintaan.

## Miten pilvipalveluiden käyttö vaikuttaa uhkiin varautumiseen?

Liiketoiminnan jatkuvuudenhallinnan kannalta kannattaa arvioida esimerkiksi seuraavissa taulukoissa esitettyjen uhkien todennäköisyyttä ja vaikutuksia omassa yrityksessä ja kriittisissä toiminnoissa.

Tähän osioon valitut skenaariot perustuvat mm. Sisäministeriön julkaisemaan Kansalliseen riskiarvioon 2018 ja Kyberturvallisuuskeskuksen Tietototurvan vuosi 2021-raporttiin. Omalle yritykselle ja toimialalle relevantteja kyberuhkia ja trendejä voi löytyä myös Kyberturvallisuuskeskuksen Kybersää-tiedotteista.

### Pilvipalvelu on toisinaan huolettomampi

Pilvipalveluiden käyttö vaikuttaa joissain tapauksissa merkittävästi siihen, miten uhkaskenaarioihin tarvitsee varautua. Tällaisia uhkia on esitetty seuraavassa taulukossa.

| Uhkaskenaario | Konesali vai pilvipalvelu? | Pohdittavaa yrityksellesi |
|---|---|---|
| **Tietoliikenneyhteyksien ja viestintäverkkojen laajamittaiset häiriöt**<br>Myrskyt, sähkönjakelun häiriintyminen, kaivinkoneet, laiterikot ja konfiguraatiovirheet voivat aiheuttaa häiriöitä tietoliikenneyhteyksien ja viestintäverkkojen toiminnassa. Tällöin myös maksuliikenne voi häiriintyä.<br>Esimerkiksi vuonna 2019 talvimyrsky Aapelin aiheuttamat sähkökatkot aiheuttivat matkapuhelinverkkojen ja laajakaistayhteyksien häiriöitä useassa maakunnassa kaikilla teleoperaattoreilla. Kesällä 2021 kaivinkone kauhaisi poikki valokuitukaapeleita, minkä seurauksena useiden valtionhallinnon työntekijöiden sähköpostit ja videoneuvottelut lakkasivat toimimasta ja myös kansalaisille suunnatut palvelut, kuten Suomi.fi, olivat alhaalla. Pääyhteys ja varayhteys kulkivat samassa kaapelikourussa, joten molemmat yhteydet katkesivat samalla kertaa. | Pilvipalvelu on useissa tapauksissa huolettomampi, mutta silti on syytä varautua ainakin lyhytaikaisiin tietoliikennekatkoksiin.<br>Tietoliikenneyhteyksien katkeaminen on usein paikallinen ongelma, jolloin se vaikuttaa vain palvelun käyttöön, ei varsinaiseen toimintaan.<br>On epätodennäköisempää, että kansainväliset tietoliikenneyhteydet katkeaisivat, sillä tarvittaisiin useita samanaikaisia poikkeamia, kuin että yhteydet katkeaisivat kokonaan. Tämä ei ole kuitenkaan mahdotonta ja yritysten täytyy miettiä riskin todennäköisyys ja vaikutus. | Onko palvelu rakennettu sietämään datakeskuksen tietoliikennehäiriöitä? Vaihtoehtoja ovat esimerkiksi alueellinen hajautus, jonopalvelut, välimuistin käyttö ja sisällönjakeluverkot (CDN).<br>Onko datakeskuksella, palvelinsalilla tai yrityksellä varainternetyhteys? Miten se on eriytetty pääyhteydestä?<br>Onko palvelu rakennettu sietämään käyttäjien tietoliikennehäiriöitä? Sivustosta voi olla esimerkiksi kevytversio häiriötilanteiden varalle.<br>Miten alueelliset tietoliikennekatkot vaikuttavat kriittisten palveluidesi toimintaan?<br>Miten kansainvälisten tietoliikenneyhteyksien katkeaminen vaikuttaa yrityksesi toimintaan? |

| Uhkaskenaario | Konesali vai pilvipalvelu? | Pohdittavaa yrityksellesi |
|---|---|---|
| **Kyberhyökkäykset ja haavoittuvuudet**<br>Miltei jokainen yritys voi joutua kyberhyökkäyksen kohteeksi. Kiristyshaittaohjelmia levitetään myös opportunistisesti ja yritys saattaa joutua kohteeksi sen vuoksi, että sen käyttämistä järjestelmistä löytyy paikkaamaton haavoittuvuus. Lisäksi huoltovarmuuskriittisiin organisaatioihin tai sen alihankkijoihin voi kohdistua kyberhyökkäyksiä joko kiinnostavan tiedon vuoksi tai organisaation lamauttamiseksi. Kyberhyökkäysten motiivina voi olla myös julkisuuden tavoittelu tai kiusanteko.<br>Esimerkiksi lokakuussa 2021 Yle Areena -palveluun kohdistui palvelunestohyökkäys. | Palvelunestotilanteelta suojautuminen voi olla helpompaa pilvipalvelussa. Pilvipalvelut oikein rakennettuna skaalautuvat liikenteen mukaan, jolloin kevyempi palvelunestohyökkäys ei välttämättä näy käyttäjille lainkaan. Julkisilla pilvipalveluntarjoajilla, etenkin suuremmilla, on myös erilaisia palvelunestohyökkäysten suojauspalveluita tarjolla.<br>Myös tunnettujen haavoittuvuuksien hyväksikäytöltä suojautuminen voi pilvipalveluissa olla helpompaa, jos käytetään hallittuja palveluita (managed services). Hallituissa palveluissa palveluntarjoaja huolehtii osasta tai kaikista tietoturvapäivityksistä. | Millaisia motiiveja kyberrikollisilla voisi olla hyökätä sinun yritystäsi vastaan?<br>Miten kriittisten tietojärjestelmiesi haavoittuvuuksien tunnistaminen ja korjaaminen on hoidettu?<br>Onko yrityksellä suunnitelma tietoturvapoikkeamatilanteessa toimiseksi?<br>Ovatko yrityksesi varmuuskopio- ja palautuskäytännöt toimivia, testattuja ja harjoiteltuja? |
| **Datakeskusten häiriöt**<br>Myös pilvipalveluntarjoajien palvelinsalit voivat vikaantua. Esimerkiksi maaliskuussa 2021 pilvipalveluntarjoaja OVH:n datakeskus Strasbourgissa tuhoutui tulipalossa.<br>Myös sähkönjakelun tai tietoliikenteen häiriöt, erilaiset tekniset viat ja esimerkiksi inhimilliset virheet konfiguraatiomuutoksissa voivat aiheuttaa alueellisia saatavuusongelmia pilvipalveluissa. | Pilvipalvelu on oikein rakennettuna huolettomampi.<br>Julkisilla pilvialustoilla skaalautuminen useille saatavuusalueille jopa oman maan ulkopuolelle on helpompaa, jolloin yhden palvelinsalin tai datakeskuksen häiriö ei häiritse palvelun toimintaa. | Onko palvelu rakennettu kestämään yksittäisen datakeskuksen väliaikaista tai pysyvää ongelmaa?<br>Onko yrityksellenne tärkeämpää, ettei yksittäisen datakeskuksen häiriö edes näy palvelun käyttäjille vai se, että palvelu voidaan tarvittaessa palauttaa vian satuttua?<br>Onko varmuuskopiot hajautettu siten, että yksittäisen datakeskuksen tai maantieteellisen alueen ongelmat eivät väliaikaisesti tai pysyvästi estä palautumismahdollisuutta? |
| **Luonnonmullistukset**<br>Myrskytuulten aiheuttamien sähkö- ja tietoliikennevikojen lisäksi tulvat ja tulipalot voivat aiheuttaa ongelmia. Myös Suomessa on tulvariskialueita, joilla vesistöjen pinnan nousu voi aiheuttaa vahinkoja kiinteistöille tai tieverkostolle. Tulipalon alku voi keskeyttää työt hetkeksi tai pahimmillaan tuhota kokonaisen liikekiinteistön. | Pilvipalveluissa varautuminen on helpompaa.<br>Yksittäisen datakeskuksen menettäminen luonnonmullistuksessa on mahdollista. Sekä konesali- että pilvipalveluratkaisussa täytyy huolehtia, että toiminta ei vaarannu tai on palautettavissa tässäkin tapauksessa.<br>Julkipilvipalveluissa maantieteellinen hajauttaminen on usein hyvin yksinkertaista. | Millaiset luonnonmullistukset voivat uhata yrityksesi toimipaikkoja? Miten niihin on varauduttu?<br>Mikäli yrityksellä on toimintaa Suomen tai ulkopuolella, kannattaa tarkistaa alueelliset riskit, esimerkiksi maanjäristykset. |

### Tietyissä uhkissa toteutusteknologialla ei ole väliä

Joissain uhkaskenaarioissa ei ole erityistä väliä, onko palvelu toteutettu konesalissa vai julkisen pilvipalvelualustan päällä. Seuraaviin skenaarioihin tulee varautua toteutuksesta riippumatta.

| Uhkaskenaario | Konesali vai pilvipalvelu? | Pohdittavaa yrityksellesi |
|---|---|---|
| **Sähkönjakelun häiriintyminen**<br>Suomessa sähkökatkoja voi tulla syys- ja talvimyrskyjen aikaan. Aina silloin tällöin myös uutisoidaan työmaakaivurien poikki kauhaisemista kaapeleista.<br>Esimerkiksi vuonna 2018 uutisoitiin HUS:n sairaaloissa Meilahdessa sattuneesta noin tunnin mittaisesta laajasta sähkökatkosta, joka johtui voimakeskuksen kytkimien häiriöistä. Joidenkin kiinteistöjen varavoimalaitteet eivät kytkeytyneet päälle, mutta akkukäyttöiset lisävaravoimalaitteet toimivat eikä potilasturvallisuus vaarantunut. | Sähkökatkot ovat tyypillisesti alueellisia. Konesaleilla on lähes poikkeuksetta varavirtaratkaisu ja julkipilvipalveluntarjoajien konesalit ovat hyvin sähkökatkoilta turvattuja.<br>Pidempi sähkökatko voi aiheuttaa ongelmia. Jos palvelu on peilattu useaan konesaliin tai julkisessa pilvialustassa konfiguroitu useammalle saatavuusalueelle, palvelun toimivuus ei häiriinny.<br>Jos palvelun käyttäjä on sähkökatkon piirissä tai sähkökatko vaikuttaa tietoliikenneyhteyksiin, katko voi estää tai haitata palvelun käyttöä. | Kuinka kauan sinun yrityksesi pärjää ilman sähköjä? Kuinka kauan varavoimalaitteissa riittää virtaa?<br>Jos käytätte omia tai vuokrattuja konesaleja, tiedättekö miten pitkään ne selviävät sähkökatkosta?<br>Miten sähkökatko vaikuttaa laitteiden toimintaan? Tarvitseeko esimerkiksi laitteet sammuttaa ja käynnistää hallitusti? Tai käynnistyvätkö verkkolaitteet oikeaan tilaan sähkökatkon päätyttyä? |
| **Ohjelmistoviat ja virheet asetuksissa**<br>Ohjelmistovirhe voi häiritä kriittisen prosessin toimintaa virheellisillä tuloksilla tai prosessin keskeytymisellä. Lisäksi erilaiset näppäilyvirheet tai virheellisten asetusten lataaminen voivat aiheuttaa toimintahäiriön.<br>Esim. ylläpitäjä voi unohtaa uusia palvelun verkkotunnuksen aitoudesta kertovan varmenteen tai tehdä virheen palomuurisäännöissä. Näissä tilanteissa palvelun käyttö voi estyä täysin – ilman kyberrikollisen toimia. | Ohjelmistovirheitä ja viallisia asetuksia voi sattua yhtä lailla niin konesali- kuin pilviympäristössäkin.<br>Julkipilvialustoissa on usein tarjolla hallinnoituja palveluita, jotka voivat vähentää vikoja tai ainakin vianhallintaan liittyvää työtä.<br>Pilvipalveluissa on usein myös asetusten hallintaan liittyvää automaatiota.<br>Vastaavanlaisia toimintoja on mahdollista rakentaa konesaliinkin, mutta se voi vaatia enemmän työtä. | Onko yrityksessänne käytössä sellaiset ohjelmistokehitys- ja infrakäytänteet, joilla riskien todennäköisyyttä ja vaikutusta voidaan minimoida? Onko kriittisissä järjestelmissä muutostenhallintaprosessi?<br>Ovatko tuotantomuutokset laajoja ja/tai manuaalisia vai pieniä ja automaattisia? Jos virhe huomataan, onko edelliseen versioon palautus automatisoitu?<br>Testataanko uusia ohjelmistoversiota ja asetuksia erillisessä testiympäristössä? |
| **Pandemia**<br>Koronapandemia tuli yllätyksenä. Se häiritsi toimitusketjuja, aiheutti työvoimapulaa ja pakotti tehtaita sulkemaan ovensa kokonaan. Myös kassavirta pieneni ja pakotti yrityksiä leikkauksiin. Korona pakotti osan yrityksistä digiloikkaan ja vähintään etätyökäytännöt piti laittaa useissa firmoissa uusiksi | Pandemian vaikutukset ovat pitkälti samanlaiset toteutusympäristöstä riippumatta. Toisaalta etäyhteyksien järjestäminen voi olla helpompaa julkiseen pilvipalveluun. | Mikäli uusi pandemia tulee, miten se vaikuttaa yrityksesi toimintaan? Onko esim. VPN-yhteyksiä riittävästi etätyöhön siirryttäessä? |
| **Avainhenkilöiden saatavuus estyy**<br>Avainhenkilöiden saatavuus voi estyä muistakin syistä kuin pandemiasta. Onnettomuudet, loukkaantumiset tai kuormitustekijät voivat viedä pitkälle sairaslomalle. Avainhenkilöt voivat myös siirtyä eläkkeelle tai toisen työnantajan palkkalistoille. | Avainhenkilöiden puuttumisen vaikutukset ovat melko samanlaiset toteutusympäristöstä riippumatta, joskin teknologiavalinta voi vaikuttaa saatavilla olevien korvaavien osaajien määrään. | Ketkä ovat avainhenkilöitä yrityksessäsi tai kumppaneillasi? Onko teillä yksittäisiä henkilöitä, joilla on ainoana osaamista johonkin vähemmän tunnettuun järjestelmään?<br>Miten yrityksessäsi on varmistettu, että oleellinen tieto, osaaminen ja muut resurssit ovat tarvittaessa toisten työntekijöiden saatavilla? Entä miten osaamista hankitaan rekrytoimalla tai kumppanien kautta lisää tarvittaessa? |

| Uhkaskenaario | Konesali vai pilvipalvelu? | Pohdittavaa yrityksellesi |
|---|---|---|
| **Ulkoistuksen ja alihankintaketjun häiriöt**<br>Ulkoistuskumppanin tai heidän alihankkijansa henkilöstöpula voi aiheuttaa toimitusviiveitä. Pahimmillaan kumppanisi voi mennä konkurssiin. Jos heillä on pääsy tietojärjestelmiisi, kiristyshaittaohjelma tai muu kyberhyökkäys voi tulla myös tätä kautta. | Ulkoistuksen ja alihankintaketjujen häiriöiden vaikutukset ovat melko samanlaiset sekä konesali- että pilvipalvelutoteutuksissa. | Mitä vaikutuksia on yrityksesi kumppanien toimitusten tai työpanoksen menetyksellä?<br>Millainen pääsy kumppaneilla ja heidän alihankkijoillansa on yritystesi tiloihin tai tietojärjestelmiin?<br>Miten olet varmistunut siitä, että kumppanisi ja heidän alihankkijansa käsittelevät tietojasi turvallisesti? Entä miten varmistatte sovitun palvelutason sekä saatavuuden, luottamuksellisuuden ja eheyden vaatimukset? |
| **Informaatiovaikuttaminen**<br>Informaatiovaikuttamisen yritykset voivat kohdistua erityisesti media-alan toimijoihin, jolloin niiden toimintaa voidaan pyrkiä estämään esimerkiksi palvelunestohyökkäyksillä. Viestintäpalveluihin voidaan myös koettaa tehdä tietomurtoja, joiden tarkoituksena on pyrkiä levittämään niiden kautta haitallista tietoa. | Informaatiovaikuttaminen ei riipu toteutustekniikasta. | Voiko yrityksesi olla informaatiovaikuttamisen kohteena ja miten?<br>Osaatko tunnistaa informaatiovaikuttamisen ja vastata siihen?<br>Onko yrityksessänne sosiaalisen median käytännöt sovittu? Entä kriisiviestinnän ratkaisut etukäteen mietittyinä? |
| **Logistiikan häiriöt**<br>Logistiikan häiriöt voivat johtua useista syistä. Esimerkiksi työvoimapula ja lakot voivat jumittaa satamia. Maaliskuussa 2021 Suezin kanavaan juuttunut Ever Given -konttialus vaikutti laajalti ja pitkään.<br>Joillekin yrityksille logistiikan häiriöt tarkoittavat vain pidempää odotusaikaa uudelle läppärille, mutta toisille puuttuva varaosa tarkoittaa pidentynyttä tuotannon käyttökatkoa, mikäli tärkeä osa vikaantuu. | Logistiikan häiriöillä on todennäköisesti melko samanlaiset vaikutukset sekä konesali- että pilvipalvelutoteutuksiin. | Millaiset logistiikkahäiriöt voivat vaikuttaa yrityksesi toimintaan?<br>Miten nopeasti häiriö vaikuttaa? |
| **Teknologiakentän tai lainsäädännön muuttuminen**<br>Vanhat teknologiat poistuvat käytöstä uusien tieltä, joskus nopeastikin. Esimerkiksi palveluntarjoaja voi poistaa on-premise-ratkaisut valikoimistaan ja siirtää kaikki asiakkaat pilvipalvelunsa käyttäjiksi.<br>On myös periaatteessa mahdollista, että lainsäädännöllisistä epäselvyyksistä, kilpailullisista tai jopa poliittisista syistä johtuen tietyn pilvipalvelualustan käyttö kielletään esimerkiksi tietyllä toimialalla. | Teknologian ja ohjelmistojen vanhentuminen on epätodennäköisempää pilvipalveluissa, palveluntarjoajan hoitaessa osan tai kaikki päivitykset. Sen sijaan pilvipalveluiden käyttöön vaikuttava lainsäädäntö elää ja muuttuu jatkuvasti. Esimerkiksi Privacy Shield, jonka tarkoitus oli helpottaa henkilötietojen siirtämistä EU:n ja Yhdysvaltojen välillä, otettiin käyttöön 2016 ja lakkautettiin jo 2020. | |

# “Tunnista ja turvaa” -korttipakka

Onko yrityksemme huolehtinut liiketoimintakriittisten toimintojen jatkuvuudesta riittävän hyvin? Voiko huoltovarmuuskriittistä tietoa tai kriittistä prosessia tukevan tietojärjestelmän siirtää pilvipalveluun ja mitä silloin pitää ottaa huomioon? Onko konesali Suomessa meille tarpeeksi hyvä ratkaisu, jos tulee tietoliikenneongelmia tai sähkökatkoja?

Jos pohdit mm. näitä kysymyksiä, tämä “Tunnista ja turvaa” -korttipakka on sinulle.

Kortit auttavat sinua ja yritystäsi muun muassa:

- Tunnistamaan, mikä liiketoiminnassasi on liiketoiminta-, huoltovarmuus-, ja regulaatiokriittistä
- Kartoittamaan yrityksen nykyisen jatkuvuudenhallinnan tilan
- Ymmärtämään tärkeimmät tehtävät pilvipalveluun siirtymisessä tai muissa tietojärjestelmämuutoksissa. Vaikka korttipakasta löytyy paljon pilvipalveluesimerkkejä, korttipakkaa voi käyttää riippumatta mihin lopputulokseen päädytään
- Huomioimaan muutostilanteissa jatkuvuudenhallinnan, huoltovarmuuden, tietoturvan ja tietosuojan
- Tekemään tietoon ja riskiarvioon perustuvia harkittuja päätöksiä

Korttipakan käyttö on tiimityötä. Jokaisessa kortissa on määritetty, millaista osaamista tehtävien tekemiseen vaaditaan. Korttien tehtävät kannattaa käydä läpi ryhmässä ja jakaa työt osaamisen mukaan.

Jokaisessa kortissa on case-esimerkkejä. Läpi ohjeen esiintyvät seuraavat kuvitteelliset yritykset:

**1. Cirrocumulus Logistics Ltd, logistiikka-alan palveluorganisaatio**
Yritys on palvelu- ja konsultointitalo, joka tuottaa ja ylläpitää huoltovarmuuskriittisen organisaation logistiikkapalvelua. Yritys tarjoaa lisäksi vastaavia palveluita yksityisyrityksille. Yritys on laajentunut vuosien varrella työskentelemään useissa eri maissa. Käytännön kokemuksien perusteella yritys on linjannut, että pilvipalveluita pyritään käyttämään aina kun mahdollista, jotta voidaan taata skaalautuvuus ja riittävän hyvä saatavuus kustannustehokkaasti. Yritys on myös ylpeä siitä, että se on modernin digitalisoinnin edelläkävijä logistiikka-alalla ja haluaa tarjota paikkariippumatonta työtä työntekijöilleen. Päätöksiin on vaikuttanut varmasti myös se, ettei talossa ole työntekijöitä, joilla olisi kokemusta oman konesalin palveluiden pyörittämisestä vaan suurin osa kehitys- ja ylläpitotiimistä on jonkun pilvipalvelun osaaja.

**2. Laastari Oy, terveydenhuoltoalan yksityisyritys**
Yritys toimii terveydenhuoltoalalla ja tuottaa ostopalveluita julkiselle sektorille. Yritys käsittelee asiakkaidensa terveystietoa. Historiallisista syistä yrityksellä on oma konesali, jossa pyöriviä järjestelmiä operoi ulkoistuskumppani.

**3. Moniala Oy, iso monialakonserni**
Moniala Oy on laajentunut yritysostojen ja fuusioiden myötä useille toimialoille. Yritys tarjoaa palveluita ja toimittaa laitteita useille huoltovarmuuskriittisille toimijoille. Yritysostojen ja osittain myös yrityskulttuurin myötä yrityksen eri liiketoimintayksiköillä on varsin erilaiset prosessit, toimintatavat ja tietojärjestelmät.

## Milloin kortteja käytetään?

Korttipakka jakautuu kahteen osaan: perustuskortteihin ja muutoskortteihin. Perustuskorttien avulla kartoitat nykytilanteen ja ne kannattaa käydä läpi ainakin kerran ennen muutoskortteihin siirtymistä.

Muutoskortit kannattaa käydä läpi silloin, kun on tunnistettu tarve esimerkiksi uuden tietojärjestelmän hankinnalle, nykyisen tietojärjestelmän modernisoinnille tai osittain päällekkäisten toimintojen yhdistämiselle. Esimerkki tällaisesta korttipakan käytöstä on kaaviossa 1.

**Kaavio 1: Esimerkkikaavio korttipakan käytöstä. Tietojärjestelmäuudistusta aikova yritys tunnistaa ensin olemassa olevat tietonsa, riskinsä ja lainsäädännön vaatimukset ennen kuin lähtee tarkemmin suunnittelemaan muutoksen toteutusmahdollisuuksia.**

Huoltovarmuuskriittinen yritys haluaa tutkia palveluiden siirtämistä pilveen ja se päättää käyttää apuna korttipakkaa.

Yritys päättää kartoittaa kriittiset toimintonsa, tietonsa ja niihin liittyvät uhkat ja riskit ennen muutosta, koska ei ole ennen tehnyt sitä systemaattisesti ja yhteneväisesti.

Kriittiset tiedot ja toiminnot selvitetään yhdessä työpajassa.

Tämän jälkeen uhkat ja riskit selvitetään toisessa työpajassa.

Yrityksen juristilla on ollut tähänkin mennessä hyvä näkemys yritystä koskevista laeista ja sopimuksista. Liiketoimintajohto on puolestaan ollut perillä toimialavaatimuksista. Nyt yritys päättää käydä asian läpi vielä yhdessä ja dokumentoida kaiken yhteen paikkaan.

Yrityksellä on ennestään ollut jatkuvuussuunnitelmia, mutta he käyvät ne läpi tämän korttipakan kysymysten avulla. Joitain puutteita löytyy mm. sopimuksista ja harjoittelukäytännöistä.

Kun perustuskortit on käyty läpi, yrityksellä on lista erilaisista asioista, joita olisi syytä parantaa. He aloittavat muutos-korttien läpikäynnin sillä ajatuksella, että ajatellun pilvi-palveluihin siirtymisen pitäisi auttaa myös näissä kehityskohteissa.

Muutoksen kohteena olevan tiedon tunnistaminen on nyt nopeaa, koska kaikki kriittiset tiedot ja toiminnot on jo aiemmin lueteltu. Yritys päättää tässä kohtaa keskittyä yhteen kriittiseen toimintoon ja sen uudistamiseen.

Muutoksessa tarvittavan osaamisen ja resurssien tunnistaminen ja toteutusmahdollisuuksien tunnistaminen etenevät osittain rinnakkain, sillä eri toteutusteknologiat vaativat omanlaistaan osaamista.

Lopulta yritys valitsee lupaavimman vaihtoehdon ja saa kartoitettua tarvittavan osaamisen ja resurssit.

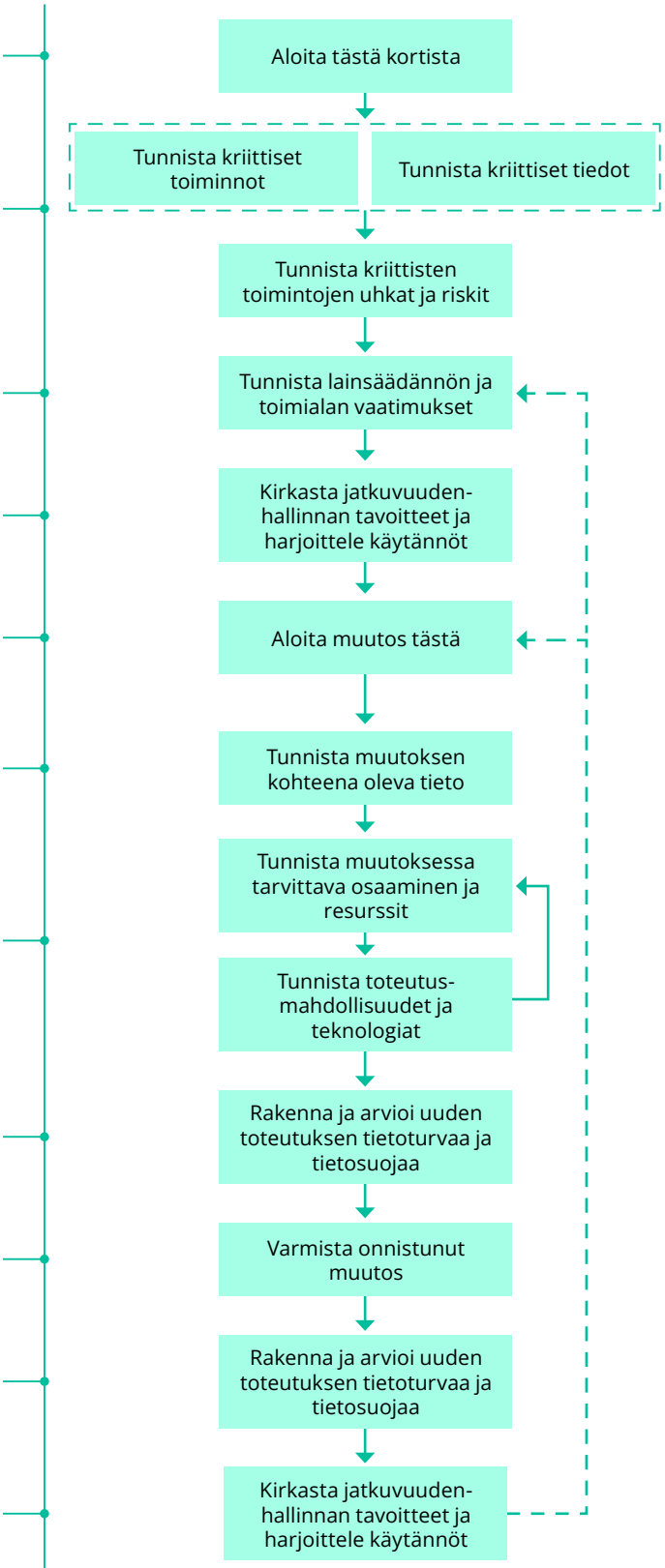
Uuden pilvitoteutuksen tietoturvaa ja tietosuojaa lähdettiin rakentamaan jo toteutusvaiheessa asettamalla tietoturvavaatimuksia ja katselmoimalla toteutusta.

Yritys seurasi muutosprojektin suuntaa säännöllisesti. Projektin aikana kartoitettiin, millä tavalla osa sisäisistä prosesseista ja vastuunjaosta tulee muuttumaan, että ne osataan ohjeistaa ja kouluttaa henkilöstölle ennen uuden tietojärjestelmän käyttöönottoa.

Yritys arvioi lopuksi lähes valmiin toteutuksen uhkat. Lisäksi järjestelmä tietoturvatestattiin ja tehtiin tietosuojaa koskeva vaikutustenarviointi.

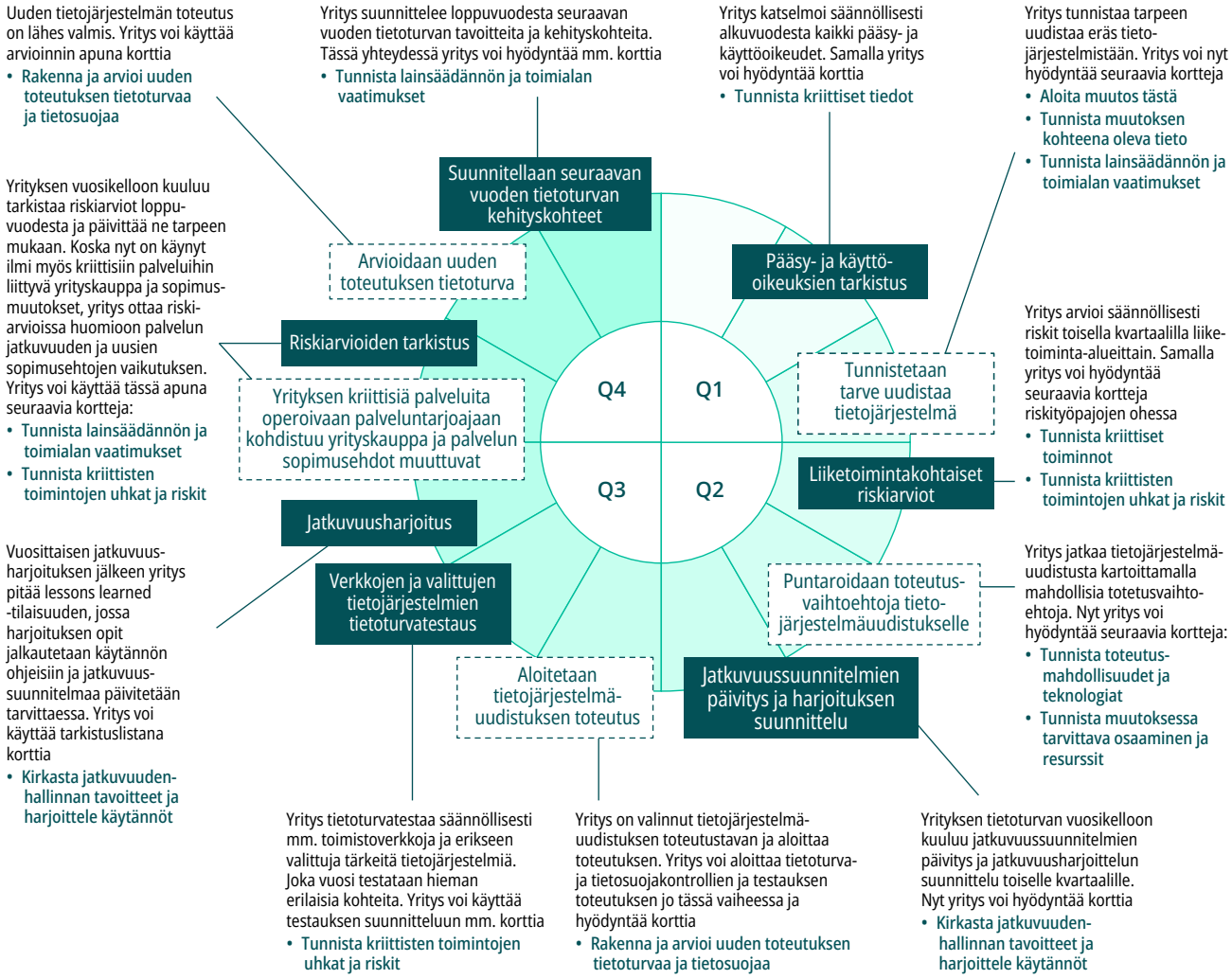
Yritys päätti vielä lopuksi palata uudestaan jatkuvuuden-hallintaa ja harjoittelua ohjeistavaan korttiin, koska he huomasivat siinä olevan paljon kehitettävää.

Yritys voi palata tarpeen mukaan muihin kortteihin, esimerkiksi uuden tietojärjestelmämuutoksen yhteydessä korttiin Aloita muutos tästä tai lainsäädännön tai uhkien muuttuessa näistä kertoviin kortteihin.



Kortit voi ottaa myös käyttöön yrityksen tietoturvan vuosikellon tueksi. Lisäksi erilaiset muutokset yrityksen toimintaympäristössä voivat vaatia korttien läpikäyntiä uudelleen, jotta muutosten aiheuttamat uudenlaiset riskit, toimintojen erilainen kriittisyysluokitus tai uudet reunaehdot esimerkiksi laeista tulevat huomioiduksi. Tällainen käyttötapa on esitetty kaaviossa 2.

**Kaavio 2. Korttipakka tietoturvan vuosikellon tukena ja muutostilanteissa.**



## Korttien lukuohje

### Symbolit

**Ohjeistus**
Aloita tästä kortista. Sisältää tärkeitä ohjeita.

**Perustus**
Tämä kortti kannattaa käydä läpi ainakin kerran nykytilan ymmärtämiseksi.

**Muutos**
Tämä kortti kannattaa käydä läpi silloin, kun on tunnistettu tarve esimerkiksi uuden tietojärjestelmän hankinnalle, nykyisen tietojärjestelmän modernisoinnille tai kun yrityksen toimintaympäristö muuttuu.

**Jatkuva prosessi**
Kortissa määritellyt tehtävät ovat toistuvia. Esimerkiksi jatkuvuussuunnitelman päivittäminen.

### Edeltävät vaiheet ja esiehdot

Tässä kohdassa lueteltujen korttien tehtävät on suositeltavaa käydä läpi ennen tätä korttia, sillä niissä selvitetään jotain tämän kortin tehtävien kannalta oleellista etukäteistietoa.

### Osaamis- tai vastuualue

Näiden roolien tai asiantuntijoiden osaamista tarvitaan kortin keskeisten tehtävien toteuttamiseksi. Asiantuntemus voi olla yrityksen omaa tai ulkoistettua.

| Osaamis- tai vastuualue | Kuvaus ja tyypillinen tehtävänimike |
|---|---|
| **Osaaminen ja koulutus** | Henkilöstön osaamisesta ja koulutustarpeista vastaavat henkilöt. Tyypillisiä osallistujia ovat henkilöstöhallinto, esihenkilöt ja tiiminvetäjät. |
| **Järjestelmä-arkkitehtuuri** | Järjestelmäarkkitehtuurin asiantuntija osaa arvioida tietojärjestelmien ja sovellusten muodostamaa kokonaisuutta ja niiden välisiä rajapintoja. Monimutkaisen järjestelmän arkkitehtuuri voi vaatia tarkastelua esimerkiksi, teknologioiden yhteensopivuuden ja tietokantojen, integraatioiden, sovellusten, pilvialustan tai tietoturvan kannalta. |
| **Jatkuvuuden-hallinta** | Yrityksen jatkuvuudenhallinnasta vastaava henkilö. Yrityksestä riippuen tehtävänimi voi olla esimerkiksi Chief Information Security Officer (CISO), Business Continuity Manager, tietoturvapäällikkö, turvallisuuspäällikkö tai jatkuvuuspäällikkö. |
| **Lainsäädäntö** | Yritystä koskevaa yleislainsäädäntöä ja toimialan lainsäädäntöä tunteva ja ymmärtävä henkilö. Tällaisen roolin tehtävänimike voi olla esimerkiksi juristi, Legal Counsel tai General Counsel. |
| **Kriittisen toiminnon toiminta ja kehitys** | Kriittisen toiminnon tai prosessin toiminnasta ja kehittämisestä vastaava henkilö. Tällaisen roolin tehtävänimike voi olla esimerkiksi Business Owner, Service Owner tai Product Owner (tuoteomistaja). |
| **Kriittisen järjestelmän toiminta** | Järjestelmän toiminnan ja käytön tunteva henkilö, esimerkiksi järjestelmän pääkäyttäjä, järjestelmäasiantuntija tai tuoteomistaja. |

| Osaamis- tai vastuualue | Kuvaus ja tyypillinen tehtävänimike |
|---|---|
| **Liiketoiminta** | Tietyn liiketoiminta-alueen kehittämisestä vastaava henkilö. Yrityksestä riippuen tehtävänimike voi olla esimerkiksi Business Manager, liiketoimintapäällikkö tai liiketoiminta-asiantuntija. |
| **Riskienhallinta** | Yrityksen riskienhallinnasta vastaava henkilö. Yrityksestä riippuen tehtävänimike voi olla esimerkiksi riskienhallintapäällikkö, tietoturvapäällikkö tai CISO. |
| **Tietojärjestelmät** | Yrityksen tietojärjestelmäkokonaisuudesta tai kriittisistä järjestelmistä ja niiden kehittämisestä vastaava henkilö tai henkilöitä. Yrityksestä riippuen tehtävänimike voi olla esimerkiksi tietohallintopäällikkö, Head of IT tai Chief Information Officer (CIO). |
| **Tietosuoja** | Tietosuojavaatimusten käytännön toteuttamista ymmärtävä henkilö. Yrityksestä riippuen tehtävänimike voi olla esimerkiksi juristi, Legal Counsel, tietosuojakonsultti tai tietosuojavastaava. |
| **Hallinnollinen tietoturva** | Yrityksen hallinnollisesta tietoturvasta, kuten tietoturvapolitiikoista, tietoturvaan liittyvistä prosesseista ja kouluttamisesta, jne. vastaava henkilö. Yrityksestä riippuen tehtävänimike voi olla esimerkiksi tietoturvapäällikkö tai CISO, tai hallinnollisen tietoturvan asiantuntija, esimerkiksi tietoturvakonsultti. |
| **Tekninen tietoturva** | Teknisestä tietoturvasta, kuten tietoturvatestauksesta, verkon tietoturvasta, identiteetin- ja pääsynhallinnasta tai tietoturvan valvonnasta vastaava henkilö tai asiantuntija. |
| **Teknologia-asiantuntemus** | Kyseessä olevaa teknologiaa, sen mahdollisuuksia ja rajoitteita tunteva henkilö. |
| **Toimialatuntemus** | Kyseessä olevaa toimialaa, esimerkiksi logistiikkaa tai energia-alaa, ja sen erikoispiirteitä ja asiakaskuntaa tunteva henkilö. |
| **Viestintä** | Yrityksen sisäisestä ja tarvittaessa myös ulkoisesta viestinnästä vastaava henkilö. Yrityksestä riippuen tehtävänimike voi olla esimerkiksi viestintäpäällikkö, Communications Manager tai Communications Specialist. |
| **Yrityksen tukitoiminnot** | Liiketoimintaa mahdollistavat toiminnot yrityksessä, esimerkiksi IT, markkinointi, henkilöstöhallinto ja viestintä. |
| **Yritysjohto** | Ylintä päätäntävaltaa käyttävät ja vastuuta kantavat henkilöt, esimerkiksi toimitusjohtaja tai johtoryhmä. |

# 1. Aloita tästä kortista

**Aloita tästä kortista. Kortin avulla saat nopeasti selville mitkä ovat vaadittavat esitehtävät ja -tiedot tämän korttipakan käyttöön. Tämän kortin avulla varmistat, että yrityksesi saa korttipakasta eniten tuloksia irti ja toisaalta pääsette mahdollisesti laajassa ja monimutkaisessa työssä selkeästi jollain kulmalla alkuun.**

## Vinkki!

Urakkaa helpottaaksesi ei kannata käydä jokaisen kortin jokaista tehtävää jokaista yrityksen kriittistä toimintoa vasten kerralla, vaan jakaa työ pienempiin kokonaisuuksiin. Esimerkiksi keskittymällä vain yhteen toimintoon kerrallaan tai tärkeimpiin kortteihin / tehtäviin ja vasta sitten laajentamalla toisiin toimintoihin / kortteihin / tehtäviin.

**Edeltävät vaiheet ja esiehdot:**
-

**Osaamis- tai vastuualueet:**
-

**Esimerkki: Moniala Oy**

Yritys pohtii voivatko he hyödyntää julkisia pilvipalveluita kriittisissä toiminnoissaan. Aihe on todella laaja ja moniulotteinen ja yksiselitteistä vastausta on mahdotonta saada. Yritys päättää hyödyntää tätä opasta ja korttipakkaa päätöksenteon tukena. Rajatakseen työmäärää he käyvät ensin pienellä ydinporukalla läpi kaikki kortit pintapuolisesti. Sen jälkeen he valitsevat kriittisistä toiminnoista vähiten kriittisen, jonka pilveen siirtämistä he suunnittelevat proof-of-concept-tyyppisesti.

Ydintiimi käy läpi kaikki muutoskortit valittuun toimintoon peilaten. He tekevät roadmapin löytyneistä huomioista ja päättävät ratkaista kaikkein kriittisimmät ensiksi. Tiimi tunnistaa, että päätöksenteko vaatii yrityksen riskienhallintakäytäntöjen parantamista, juristin apua tulkitsemaan heidän alansa regulaatiota sekä pilviasiantuntijaa, joka auttaa siirtymään pilvipalveluun turvallisesti ja oikealla tavalla. Yrityksellä ei ole omaa juristia, joten he pyytävät apua lakiasiaintoimistosta. Heillä ei ole myöskään varsinaista riskienhallintapäällikköä, mutta yrityksen finanssitiimistä löytyy riskienhallintaosaamista.

Yritys pystyy tekemään päätöksen proof-of-concept-vaiheesta, jossa pilvipalveluun siirretään yksi osa yrityksen yhdestä toiminnosta ja käytetään ulkopuolista auditoijaa varmistamaan ratkaisun täyttävän alan regulaation. Vihreää valoa saatuaan yritys tietää pilvisiirtymän olevan mahdollista tietyillä reuna-ehdoilla ja etenee päätöksentekoprosessin kanssa siirtyen kartoittamaan kriittisempien toimintojen siirtämistä.

# 1. Aloita tästä kortista

## Keskeiset tehtävät korttipakan käyttöön

1. Tutustukaa korttipakkaan.
   - Tämän oppaan luku “Milloin kortteja käytetään” kertoo miten ja missä tilanteissa kortteja käytetään.
   - Selatkaa ensin kaikki perustus- ja muutoskortit läpi saadaksenne kokonaiskuvan mitä vaiheita korttipakka sisältää, millaisia rooleja tarvitaan mukaan ja mitä esitehtäviä kuhunkin korttiin liittyy.
2. Kirkastakaa mitä halutaan saavuttaa korttipakan avulla.
   - Nykytilan analyysi ja perustusten vahvistaminen tai jos käytät korttipakkaa ensimmäisen kerran: valitkaa perustuskortit.
   - Muutosvaiheen suunnittelu tai läpivienti: valitkaa muutoskortit.
3. Selvittäkää aiemmin tuntemattomat termit.
   - Tutustukaa tämän oppaan määritelmäliitteeseen. Se käy läpi oppaassa keskeisesti käytetyt termit (esim. regulaatiokriittisyys, tietoturva, huoltovarmuus) ja avaa moniulotteisia termejä (esim. pilvipalvelut).
4. Kerätkää osallistujat korttipakan hyödyntämiseen.
   - Kerätkää pieni ydintiimi, jonka vastuulla on kertaluonteisesti tai jatkuvasti käydä läpi korttipakan vaiheet. Ydintiimi etsii korteissa mainitut osaajat kuhunkin vaiheeseen.
   - Katsokaa valitsemistanne korteista, millaista osaamista tarvitaan. Löytyvätkö osaajat yrityksestä vai tarvitaanko apua talon ulkopuolelta?
   - Kuka voi päättää? Keneltä tarvitsee kysyä neuvoa?
   - Jakakaa tietoa tavoitteista ja tästä ohjeesta osallistujille.
5. Sopikaa, minne havainnot, avoimet kysymykset, parannusehdotukset ja korttien tehtävien tulokset kirjataan yhteisesti.
   - Dokumentaatio voi olla esimerkiksi sisäisessä wikissä, jaetussa kansiossa tai vaikkapa laskentataulukossa.
   - Hyödyntäkää yrityksen olemassa olevia työkaluja, esim. riskienhallinnassa.
6. Ottakaa selvää, mitä on päätetty tai linjattu jo aiemmin yrityksessä.
   - Onko yrityksellänne pilvistrategia tai kyberstrategia? Onko yrityksen yleisessä strategiassa määritetty jotain jatkuvuudenhallinnasta? Mitä on IT:n suunnitelmissa?
7. Priorisoikaa korttipakan avulla nousevat muutostarpeet ja korjaukset.
   - Kirjatkaa korttipakan avulla nousevat puutteet ja muutostarpeet. Priorisoikaa ja aikatauluttakaa muutokset.
   - Priorisoikaa korkealle ne muutokset, jotka eniten parantavat mahdollisuutta tietoon perustuvaan päätöksentekoon, esim. puutteellisen riskienhallintaprosessin parantaminen.
8. Hyödyntäkää muuta olemassa olevaa materiaalia.
   - Käykää läpi tämän oppaan linkkilista. Sinne on kerätty materiaalia, jota päätöksenteossa ja mahdollisessa pilvisiirtymässä kannattaa hyödyntää.

# 2. Tunnista kriittiset toiminnot

**Tunnista yrityksesi ne kriittiset toiminnot ja prosessit, joilla on vaikutusta omaan ja asiakkaan liiketoiminnan jatkuvuuteen ja huoltovarmuuteen. Luokittele toiminnot niiden kriittisyysasteen mukaan. Tämä auttaa varmistamaan, että kaikista tärkeimpien toimintojen jatkuvuudesta on huolehdittu ja että kaikki niihin liittyvät tietojärjestelmät on tunnistettu. Kriittisyyslista auttaa myös mahdollisten löydösten korjaamisen priorisoinnissa.**

## Vinkki!

Kriittisten toimintojen tunnistamisen voi jakaa yksiköittäin tai liiketoiminta-alueittain. Mikäli toimintoja vaikuttaa olevan paljon, voi aluksi keskittyä oman liiketoiminnan kannalta oleellisimpiin toimintoihin ja suurimpiin asiakkaisiin.

Kriittisten toimintojen tunnistamiseen on olemassa työkaluja, esimerkiksi sote-tietojärjestelmien luokitteluun neliportainen malli tai VAHTI-ohje Kriittisten kohteiden luokittelu.

**Edeltävät vaiheet ja esiehdot:**
-

**Osaamis- tai vastuualueet:**
Liiketoiminta, Yrityksen tukitoiminnot, Yritysjohto, Jatkuvuudenhallinta

**Esimerkki: Cirrocumulus Logistics Ltd**

Yritys on jo aiemmin tehnyt liiketoimintariskiarvionteja. He ovat tunnistaneet, että logistiikkasovelluskokonaisuuden toiminta on kriittistä, koska ilman sitä he eivät voi palvella asiakkaitaan. Yritysellä on tärkeä huoltovarmuuskriittinen asiakas, joka tuottaa komponentteja. Oman liiketoiminnan kannalta myös tuntikirjanpito- ja laskutusjärjestelmä on tunnistettu kriittiseksi, koska vaikkei laskutus ja investoinnit ole yrityksen ydinliiketoimintaa, häiriöt niissä estävät tai vakavasti haittaavat liiketoimintaa.

Kun yritys käy kortin tehtäviä läpi yhdessä liiketoimintajohtajien ja tietohallinnon kanssa, he hoksaavat myös dokumentinhallintajärjestelmän olevan liiketoimintakriittinen järjestelmä. Syynä järjestelmässä säilytettävät asiakasympäristöjen operointiin tarvittavia tiedot ja ylläpito-ohjeet.

# 2. Tunnista kriittiset toiminnot

## Keskeiset tehtävät

1. Tutustukaa yrityksen mahdolliseen jatkuvuussuunnitelmaan.
   - Onko kriittiset toiminnot tunnistettu? Voiko tuloksia hyödyntää sellaisenaan vai onko tilanne jo muuttunut? Yli 1–2 vuotta vanha lista kannattaa päivittää.
2. Listatkaa toiminnot ja prosessit, joiden keskeytyminen tai häiriintyminen vaikuttaa liiketoiminnan jatkuvuuteen (*liiketoimintakriittisyys*), huoltovarmuuteen (*huoltovarmuuskriittisyys*) tai viranomaisvelvoitteiden toteuttamisen (*regulaatiokriittisyys*).
   - Miten nämä toiminnot palvelevat yrityksen ydintoimintoja ja strategiaa?
   - Jatkuvuudenhallintasuunnitelmat ja liiketoimintariskiarviot voivat auttaa vastaamaan näihin kysymyksiin.
3. Listatkaa, mitä tietoja, tietojärjestelmiä, sovelluksia tai laitteita toimintoihin tarvitaan. Myös jotkin tukitoiminnot voivat olla kriittisiä.
4. Listatkaa, millaisia seurauksia toimintojen tai prosessien häiriintymisellä on.
   - Esimerkki: *Laskutusjärjestelmän ongelman takia yritys ei voi lähettää laskuja. Pidentynyt katkos aiheuttaa yritykselle kriittisen kassavajeen.*
5. Selvittäkää, millaisia riippuvuuksia tarvittaviin tietoihin tai tietojärjestelmiin liittyy.
   - Esimerkki: *Tuotannonohjausjärjestelmään kirjaudutaan kertakirjautumisjärjestelmällä. Tämä tekee myös siitä järjestelmästä kriittisen.*
6. Selvittäkää, miten kauan voidaan toimia ilman tunnistettuja toimintoja tai järjestelmiä. Millaiset palautumisvaatimukset järjestelmillä on? Onko vaihtoehtoisia tapoja toimia?
7. Priorisoikaa järjestelmät aiempien tietojen perusteella. Mikä toiminnoista on kaikkein kriittisin yrityksen toiminnan ja olemassaolon kannalta?

### Esimerkki: Laastari Oy

Yritys on jo aiemmin tunnistanut kriittisiä toimintojaan. He ovat käyttäneet tunnistamiseen ja dokumentointiin vapaamuotoista dokumenttia. Yrityksellä on vuosikello, joka määrää kerran vuodessa päivittämään kriittisten toimintojen listaa.

Yritys päättää tällä kertaa käyttää sote-alalle luotua neliportaista luokittelumallia. Toimintojen läpikäynnissä ei löydy suuria yllätyksiä, mutta uusi luokittelumalli auttaa heitä paremmin erottamaan toisistaan operatiivisesti kriittiset, operatiivista toimintaa tukevat, tukijärjestelmät sekä tutkimusjärjestelmät.

### Esimerkki: Moniala Oy

Yritys ei ole ennen tehnyt määrämuotoisesti kriittisten toimintojen tunnistamista. Yrityksellä on jatkuvuudenhallintasuunnitelma, mutta sitä ei ole räätälöity eri kriittisyysasteille sopivaksi, vaan se on ns. “yksi koko sopii kaikille”. Yritys tunnistaa tämän kortin avulla välillisesti kriittiset toiminnot sekä ne toiminnot, jotka eivät ole liiketoimintakriittisiä mutta ovat esimerkiksi regulaatio- tai huoltovarmuuskriittisiä. Yritys päivittää jatkuvuudenhallintasuunnitelmaansa siten, että kriittisille toiminnoille on eri tavoitteet kuin tukitoiminnoille.

# 3. Tunnista kriittiset tiedot

**On hankalaa suojata tietoa, ellet tiedä mitä tietoa omistat ja mihin se on tallennettu! Tunnista mitä tietoa käsitellään kriittisissä toiminnoissa ja prosesseissa ja miten tärkeää tieto on liiketoiminnalle ja huoltovarmuudelle. Kortti auttaa myös kartoittamaan, mitkä ovat vaatimukset tiedon luottamuksellisuudelle, eheydelle ja saatavuudelle ja sille missä ja miten tietoa voi käsitellä. Kortin avulla parannat yrityksesi jatkuvuudenhallintaa.**

**Edeltävät vaiheet ja esiehdot:**
Tunnista kriittiset toiminnot

**Osaamis- tai vastuualueet:**
Liiketoiminta, Hallinnollinen tietoturva, Tietojärjestelmät, Kriittisen järjestelmän toiminta

**Esimerkki: Cirrocumulus Logistics Ltd**

Yritys analysoi asiantuntijoidensa kanssa sekä asiakkaalle tuotettavaa logistiikkapalvelua ja sen tietojärjestelmiä, omaa dokumentinhallintapalveluaan ja tuntikirjanpito- ja laskutusjärjestelmäänsä. He tunnistavat mm. seuraavia kriittisiä tietoja:

- Logistiikkasovellusten lähdekoodi
- Reittioptimointialgoritmi ja sen parametrit
- Asiakaskohtaiset järjestelmäasetukset
- Asiakaskohtaiset nouto- ja vientipisteet, kuljetuskapasiteetti, kuljettajien ja ajoneuvojen tunnisteet ja saatavuustieto, viimeisimmät lasketut reitit
- Asiakkaan yhteystiedot
- Ylläpito-ohjeet järjestelmäpäivityksiin ja muihin tyypillisiin tilanteisiin
- Tietoturvapoikkeamienhallinnan prosessit ja toimintaohjeet
- Jatkuvuussuunnitelma
- Järjestelmien palautumissuunnitelmat
- Laskutusjärjestelmän toimittajan yhteystiedot tukipyyntötilanteissaTunnista kriittiset tiedot

# 3. Tunnista kriittiset tiedot

## Keskeiset tehtävät

1. Listatkaa ja luokitelkaa ne tiedot, joita kriittisissä toiminnoissa tarvitaan.
   - Millaista tietoa on kyseessä?
   - Mikä on tiedon vaikutus liiketoiminnan jatkuvuuteen tai huoltovarmuuteen? Onko tieto välttämätöntä vai vain avuksi?
   - Miten kauan voidaan toimia ilman tätä tietoa?
   - Ovatko tiedon luottamuksellisuuden, eheys ja saatavuus yhtä tärkeitä? Esimerkiksi osa tiedosta on sellaista, jonka täytyy olla aina saatavilla, arkistotiedon kohdalla eheys on väliaikaista saatavuutta tärkeämpää
2. Tarkistakaa seuraavat asiat kaikkien kohdassa 1 tunnistettujen tietojen osalta
   - Tarkistakaa, mitä velvoitteita tai rajoitteita näiden tietojen käsittelyyn on.
     - Onko tiedon käsittelyyn ja säilytykseen erityisiä velvoitteita esimerkiksi lainsäädännöstä? Käytä tarvittaessa korttia *Tunnista lainsäädännön ja toimialan vaatimukset*
     - Esimerkki: *Viranomainen on turvaluokitellut tiedon TLIV-tasoiseksi.*
   - Tarkistakaa, että kriittisen tiedon jatkuvuudesta on huolehdittu.
     - Onko tiedolle määritetty palautumissuunnitelma ja onko esimerkiksi varmuuskopioiden olemassaolo ja palautuksen toimivuus testattu? Käytä tarvittaessa korttia *Kirkasta jatkuvuuden-hallinnan tavoitteet ja harjoittele*
3. Jos tunnistatte tiedon tai sen tallennuspaikkojen perusteella uusia kriittisiä toimintoja, palaa korttiin *Tunnista kriittiset toiminnot.*
   - Esimerkki: *Kriittinen järjestelmä tarvitsee toimiakseen ei-kriittiseksi luokitellun tietovaraston tietoja. Tämä tekee kyseisestä tietovarastosta välillisesti kriittisen.*

### Esimerkki: Laastari Oy

Yritys harjoittaa leikkaussalitoimintaa. Heillä on potilaista muun potilasdatan lisäksi erillinen tietojoukko, jota tarvitaan leikkauksissa. Yritys tunnistaa tämän tietojoukon olevan erittäin kriittistä yrityksen jatkuvuudelle ja sen puute estää tai vaarantaa leikkaukset. Tiedon luottamuksellisuus, eheys ja saatavuus ovat kaikki tärkeitä. Yritys käy tasaisin väliajoin läpi, että tiedonhallinnan toteutustapa noudattaa vaatimuksia. He myös harjoittelevat palautuskäytännöt kumppaniensa kanssa.

### Esimerkki: Moniala Oy

Yrityksen tienhuoltoyksikön automaattinen työvuorosuunnittelujärjestelmä käyttää julkisen sääpalvelun lumisade-ennusteita. Jos lumisade-ennusteiden puuttuminen rampauttaa työvuorosuunnittelun, myös ennustedata ja sitä tarjoava palvelu ovat kriittisiä.

# 4. Tunnista kriittisten toimintojen uhkat ja riskit

**Tunnista uhkaskenaariot, jotka voivat häiritä kriittisiä toimintoja. Arvioi uhkiin liittyvät riskit ja riskien todennäköisyys huomioiden olemassa olevat suojakeinot. Riskiarvion perusteella voit suunnitella ja priorisoida kriittisten toimintojen jatkuvuuden suojaamista parantavat lisätoimet. Täten voit varautua uhkiin jo ennalta ja pienentää niiden todennäköisyyttä tai vaikutusta.**

## Vinkki!

Uhka, riski vai haavoittuvuus – mitä eroa termeillä on? Nämä termit menevät usein sekaisin, joten löydät termien määritelmät liitteestä 2.

## Vinkki!

Uhkien tunnistamisesta ja riskien arvioinnista on kerrottu laajemmin luvussa Esimerkkejä uhkaskenaarioista ja riskien arvioinnista. Uhkamallinnus (threat modeling) on yleinen tapa uhkaskenaarioiden läpikäyntiin.

**Edeltävät vaiheet ja esiehdot:**
Tunnista kriittiset toiminnot, Tunnista kriittiset tiedot

**Osaamis- tai vastuualueet:**
Liiketoiminta, Kriittisen prosessin toiminta ja kehitys, Riskienhallinta, Hallinnollinen tietoturva, Riskienhalllinta, Tietosuoja, Jatkuvuudenhallinta

**Esimerkki: Cirrocumulus Logistics Ltd**

Yritys on jo aiemmin tunnistanut seuraavat uhkat asiakkaalle tuotettavassa palvelussa. Yritys on arvioinut kullekin uhkalle riskin suuruuden. He käyttivät siihen samaa työkalua kuten kaikessa riskienhallinnassaan, jotta riskit olisivat yhteismitallisia läpi yrityksen. Työkaluna riskin suuruuden määrittelyssä ke käyttävät “todennäköisyys asteikolla 1–5 kertaa vaikutus asteikolla 1–5”, jolloin kertolaskun tulos antaa riskin suuruuden.

- Palvelussa on yli tunnin käyttökatko. Todennäköisyys: mahdollinen (3). Vaikutus: vakava (4). Riskin suuruus: merkittävä riski (12).
- Asiakkaan kuljetusreittien vuotaminen vahingossa. Todennäköisyys: mahdollinen (3). Vaikutus: kohtalainen (3). Riskin suuruus: kohtalainen riski (9).
- Asiakastietojen pysyvä menetys. Todennäköisyys: erittäin epätodennäköinen (1). Vaikutus: katastrofaalinen (5). Riskin suuruus: kohtalainen riski (5).

Yritys priorisoi seuraavat jatkuvuutta parantavat toimenpiteet:

- Käynnistetään projekti yrityksen palvelun saatavuuden parantamiseksi sekä teknisen toteutuksen että palautustilanteiden harjoittelun kannalta.
- Asiakastieto on hajautettu kahteen eri konesaliin, mutta ne ovat maantieteellisesti vierekkäin lisäten luonnonkatastrofien riskiä. Tiedot päätetään hajauttaa isommalle maantieteelliselle alueelle.

# 4. Tunnista kriittisten toimintojen uhkat ja riskit

## Keskeiset tehtävät

1. Listatkaa kriittisten toimintojen häiriintymiseen tai estymiseen liittyvät uhkaskenaariot. Mieti uhkaskenaarioita liiketoiminnan, tietoturvan ja tietosuojan kannalta. Myös osaavan henkilökunnan puuttuminen voi olla uhka. Apuna kannattaa käyttää uhkamallinnusta.
   - Esimerkki: Kertakirjautumisjärjestelmä vikaantuu estäen sisäänkirjautumisen.
   - Esimerkki: Järjestelmään tehdään tietomurto tunnetun haavoittuvuuden avulla. Korjaustoimenpiteiden ja selvitystyön aikana järjestelmä on pois käytöstä.
   - Esimerkki: Yrityksellä on vain yksi mainframe-osaaja.
2. Verratkaa tunnistettuja uhkia yrityksen yleiseen riskiarvioon. Jos riskiarviota ei ole aiemmin tehty, uhkaskenaarioita kannattaa tässä vaiheessa miettiä laajemmin,
3. Arvioikaa jokaiseen uhkaskenaarioon liittyvä todennäköisyys ja vaikutukset ja muodostakaa niistä riskin suuruus.
4. Listatkaa nykyiset suojakeinot, jotka pienentävät uhkaskenaarion vaikutusta tai toteutumismahdollisuutta. Suojakeinot voivat olla teknisiä, prosesseja tai ihmisten toimintaan liittyviä.
   - Esimerkki: Järjestelmä skannataan tunnettujen haavoittuvuuksien varalta automaattisesti (tekninen suojaus). Havaitut haavoittuvuudet korjataan niiden vakavuusasteen mukaisesti (prosessi). Tämä pienentää riskin todennäköisyyttä.
   - Esimerkki: Varmuuskopioiden palauttamista harjoitellaan säännöllisesti (ihmisten toiminta). Tämä pienentää riskin vaikutusta.
5. Jos nykyiset suojakeinot eivät merkittävästi pudota riskin todennäköisyyttä tai vaikutusta, priorisoikaa uusien suojakeinojen kehitystä
   - Esimerkki: Järjestelmä määritetään toimimaan useilla saatavuusalueilla (availability zone), jolloin yhden datakeskuksen vikaantuminen ei haittaa järjestelmän toimintaa. Tämä pienentää merkittävästi riskin todennäköisyyttä.
6. Päivittäkää jatkuvuussuunnitelmaa siten, että se vastaa korkeimman riskin skenaarioihin
   - Esimerkki: Erästä järjestelmää ylläpitää vain yksi henkilö. Mikäli järjestelmästä ja sen tietokannasta täytyy palauttaa varmuuskopio tietomurron takia eikä ylläpitäjä ole käytettävissä, palautus voi epäonnistua puuttuvien ohjeiden takia. Ohjeet järjestelmän palauttamiseen dokumentoidaan.

### Esimerkki: Laastari Oy

Yritys järjestää aihepiirikohtaisia uhkatyöpajoja tietoturvakonsultin avulla kriittisten toimintojen uhkien tunnistamiseksi. He tunnistavat mm. seuraavia uhkia:

- Potilaiden hoitaminen ei onnistu ja joku voi jopa kuolla, jos kriittiset riskitiedot eivät ole saatavilla hätätilanteessa.
- Arkaluontoisia terveystietoja vuotaa tietojärjestelmän haavoittuvuuden seurauksena. Asiasta seuraa haittaa yksityishenkilöille ja selvitystyö vie resursseja henkilöstöltä.
- Tietovuoto voi aiheuttaa hyvin negatiivista julkisuutta ja kustannuksia yritykselle. Ainakin tietosuojasakot ovat mahdollisia. Työpajan osallistujat toteavat, että heillä ei ole tarpeeksi hyvää tietämystä lainsäädännöstä ja mahdollisesta lain rikkomisen seuraamuksista, joten he aikovat järjestää vielä palaverin yrityksen juristin kanssa.

# 5. Tunnista lainsäädännön ja toimialan vaatimukset

**Tunnista, mitkä lait, asetukset tai toimialan erityisvaatimukset koskevat yritystäsi ja sen kriittisiä toimintoja. Lainsäädäntö, viranomaisohjeistukset ja toimialan standardit voivat asettaa oleellisia reunaehtoja esimerkiksi sille, miten tietoa saa käsitellä ja miten nopeasti poikkeamista tulee toipua. Huomaathan, että asiakkaidesi toimialaan liittyvä lainsäädäntö ja vaatimukset voivat vaikuttaa sinun yrityksesi toimintaan.**

## Vinkki!

Huoltovarmuuskeskuksen toimialakohtaisilla sivuilla on lueteltu huoltovarmuuskriittisten toimialojen lainsäädäntöä. Erittäin hyvä konkreettinen kooste sellaisesta lainsäädännöstä, joka voi vaikuttaa pilvipalveluiden käyttöönottoon, löytyy Sote-tietojärjestelmät pilvipalveluina soveltamisohjeesta. Vaikka ohje on tarkoitettu sote-sektorille, se on hyödynnettävissä isoin osin myös muilla toimialoilla.

## Vinkki!

Lakeihin, säädöksiin ja asetuksiin liittyy paljon myyttejä, etenkin kun puhutaan voiko pilvipalveluita hyödyntää. Oppaan kohdassa “Pilvipalveluiden käyttö kriittisissä toiminnoissa” on lisää tietoa aiheesta.

**Edeltävät vaiheet ja esiehdot:**
Tunnista kriittiset toiminnot, Tunnista kriittiset tiedot

**Osaamis- tai vastuualueet:**
Kriittisen prosessin toiminta ja kehitys, Lainsäädäntö, Tietosuoja, Toimialatuntemus

**Esimerkki: Moniala Oy**

Yrityksen eräässä toiminnossa prosessoidaan henkilötietoja, joten heidän täytyy noudattaa henkilötietojen käsittelyssä EU:n tietosuoja-asetusta GDPR:ää. Yritys on juuri siirtämässä teknistä toteutusta konesalistaan kansainväliseen pilvipalvelualustaan ja käyttää kumppaniaan apuna tutkiakseen onko ratkaisu sallittu. Pilvipalvelusta on käytetty EU/ETA-alueella olevaa datakeskusta, mutta koska palvelun sovelluslokeja käsitellään yhdysvaltalaisessa palvelussa ja palvelun ylläpitokumppani on Intiassa, tiedonsiirto EU/ETA-alueen ulkopuolelle on turvattava esimerkiksi EU-komission hyväksymillä vakiolausekkeilla (Standard Contractual Clauses). Samalla kun yritys teki tiedonsiirron vaikutusten arviointia (Transfer Impact Assessment, TIA) ja tarkisti tiedonsiirrron turvallisuutta, he huomasivat, että palvelun sovelluslokitusta täytyy korjata, sillä lokeihin vahingossa tallentuu tarpeettoman paljon henkilötietoa. Näillä toimenpiteillä pilvipalvelun käyttöönotolle ei ole GDPR:n suhteen estettä.

# 5. Tunnista lainsäädännön ja toimialan vaatimukset

## Keskeiset tehtävät

1. Tunnistakaa, miten **kansallinen** lainsäädäntö ja yleislainsäädäntö koskee teitä. Mitä vaatimuksia tai reunaehtoja niistä seuraa? Huomioikaa seuraavat näkökulmat:
   - **Yrityksen** oma **toiminta** ja **toimiala**
     - Esimerkki: *Yritys on osakeyhtiö ja listautunut pörssiin.*
   - **Asiakkaiden** toiminta ja toimiala
     - Esimerkki: *Asiakas on energia-alan toimija.*
   - Yrityksen omat ja asiakkaiden **kriittiset toiminnot**
     - Esimerkki: *Yritys tuottaa sähkön vähittäismyyntiin liittyvää palvelua.*
   - Yrityksen ja asiakkaan kriittinen tieto, johon liittyy lainsäädäntöä
2. Tunnistakaa, miten **toimialakohtainen** lainsäädäntö tai suositukset koskevat teitä.
   - Huomioikaa samat näkökulmat kuin kohdassa 1.
   - Esimerkki: *Laissa sosiaalihuollon asiakasasiakirjoista määritellään asiakirjojen säilytysaikoja.*
   - Esimerkki: *Laki sähköisen viestinnän palveluista velvoittaa teleyrityksiä huolehtimaan, että niiden toiminta jatkuu mahdollisimman häiriöttömänä.*
3. Tunnistakaa, miten **EU-lainsäädäntö** ja muu kansainvälinen lainsäädäntö koskee teitä. Huomioikaa samat näkökulmat kuin kohdassa 1.
   - Esimerkki: *Yleinen tietosuoja-asetus, GDPR.*
   - Esimerkki: *Datahallintosäädös (Digital Governance Act, DGA).*
   - Esimerkki: *Lähivuosina voimaan tulossa olevat digipalvelusäädös Digital Services Act, DSA) ja digimarkkinasäädös (Digital Markets Act, DMA).*
4. Tunnistakaa, mitä toimialan standardeja ja suosituksia yrityksen tulee noudattaa.
   - Huomioikaa samat näkökulmat kuin kohdassa 1.
   - Esimerkki: *Yrityksen vapaaehtoisesti hankkima ISO 27001 -sertifiointi.*
   - Esimerkki: *Verkkokaupan luottokorttimaksun käsittelyn tulee noudattaa PCI DSS -standardia.*
5. Millaisia vaatimuksia tulee asiakkaiden ja yhteistyökumppanien kanssa tehdyistä sopimuksista? Esimerkiksi asiakasta koskevan lainsäädännön vaatimukset voivat tulla sopimuksen kautta yritykselle.
   - Huomioikaa samat näkökulmat kuin kohdassa 1.
   - Esimerkki: *Yritys tuottaa valtion virastolle palvelua, jossa käsitellään turvaluokiteltua tietoa. Yrityksen tulee noudattaa palvelussa Valtioneuvoston asetusta asiakirjojen turvallisuusluokittelusta valtionhallinnossa.*

### Esimerkki: Laastari Oy

Laastari Oy on yksityinen terveydenhuoltoalan yritys. Sen tulee tietojärjestelmähankkeissaan huomioida muun muassa *laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista, laki sosiaali- ja terveystietojen toissijaisesta käytöstä, terveydenhuoltolaki, potilaslaki ja GDPR.*

# 6. Kirkasta jatkuvuuden tavoitteet ja harjoittele käytännöt

**Kirkasta jatkuvuuden tavoitteet kriittisten toimintojen osalta. Samat tavoitteet eivät sovellu jokaiselle toiminnolle, vaan ne kannattaa mitoittaa toimintojen kriittisyyden ja tyypin mukaan. Käy läpi suunnitelmat ja vastuut. Tarkista, mitä aiheesta on sovittu asiakkaiden ja palveluntarjoajien kanssa ja suunnittele toistuvat jatkuvuudenhallinnan käytäntöjen harjoittelut. Paraskaan suunnitelma ei auta, jos eri osapuolet eivät osaa toimia tehokkaasti yhdessä hätätilanteessa.**

## Vinkki!

Jatkuvuudenhallinnan suunnittelua on ohjeistettu kattavasti VAHTI-ohjeessa 2/2016 *Toiminnan jatkuvuuden hallinta*. Muista harjoitella yhdessä myös palveluntarjoajien, yhteistyökumppanien tai asiakkaiden kanssa, koska kriisitilanteessa et ole koskaan yksin.

**Edeltävät vaiheet ja esiehdot:**
Tunnista kriittisten toimintojen uhkat ja riskit

**Osaamis- tai vastuualueet:**
Jatkuvuudenhallinta, Kriittisen prosessin toiminta ja kehitys, Riskienhallinta

### Esimerkki: Cirrocumulus Logistics Ltd

Cirrocumulus Logistics Ltd ei ole aiemmin harjoitellut jatkuvuudenhallintaa muuta kuin testaamalla varmuuskopioiden palautusta. Nyt he päättävät tutustua aiheeseen enemmän lukemalla Kyberturvallisuuskeskuksen Kyberharjoitusoppaan. Oppaan ja Kyberturvallisuuskeskuksen skenaariopankin avulla he järjestävät omin voimin lyhyen työpöytäharjoitukseen, jossa tarkistetaan sisäisten ohjeiden ja suunnitelmien käyttökelpoisuus tilanteessa, jossa palvelussa käytetty avoimen lähdekoodin kirjasto huomataan saastuneeksi. Harjoitus osoittaa, että tilanteen johtamisen ja viestinnän vastuissa on jonkin verran puutteita. Yritys päättää päivittää jatkuvuus- ja kriisiviestintäsuunnitelmiaan harjoituksen perusteella ja pyytää tarjouksia toiminnallisen kyberharjoituksen järjestämisestä tietoturvakonsulttiyhtiöiltä.

### Esimerkki: Laastari Oy

Terveydenhuoltoalan yrityksenä Laastari Oy on panostanut jatkuvuudenhallintaan. Heillä on eri kriittisyysasteen palveluille eri jatkuvuustavoitteet. Esimerkiksi arkistodatan suhteen tiedon eheys on tärkeintä, kun taas leikkauksissa käytettävä data on oltava saatavilla tilanteesta riippumatta. He järjestävät toistuvia harjoituksia, jossa testaavat eri osapuolten toimintaa ja poikkeusoloissa toimimista.

# 6. Kirkasta jatkuvuuden tavoitteet ja harjoittele käytännöt

## Keskeiset tehtävät

1. Millaisia jatkuvuuteen liittyviä riskejä on tunnistettu kriittisistä toiminnoista?
   Katso kortti *Tunnista kriittisten toimintojen uhkat ja riskit.*

2. Miten jatkuvuuteen liittyviin riskeihin on varauduttu itse?
   - Esimerkki: *Yritys on sopinut kriisitiimin, jolla on soittorinki. Kriisitiimillä on kopio jatkuvuussuunnitelmista ja kriisiviestintäohjeesta läppärillä ja puhelimessa.*

3. Mikä on yrityksen oma rooli ja vastuu kriittisten toimintojen jatkuvuudenhallinnassa? Liittyykö vastuu jatkuvuudenhallinnan koordinointiin ja viestintään vai myös teknisiin jatkuvuuden ylläpitoon ja palauttamiseen liittyviin toimiin?
   - Esimerkki: *Yritys on hankkinut dokumentinhallintapalvelun SaaS-palveluna. SaaS-palvelun toimittaja vastaa palvelun jatkuvuudesta. Yrityksen on itse suunniteltava mahdollinen varamenettely ja tiedotus tilanteissa, joissa dokumentinhallintajärjestelmä ei toimikaan.*

4. Miten jatkuvuudenhallinnan vastuut jakautuvat yrityksen sisällä?
   - Esimerkki: *Yrityksen CISO vastaa jatkuvuudenhallinnasta ja suunnittelusta koko yrityksen tasolla. Jatkuvien palveluiden liiketoimintajohtaja vastaa, että asiakkaiden palveluiden osalta on tehty jatkuvuussuunnitelma ja sitä harjoitellaan säännöllisesti. Suunnitelmaan kuuluvat säännölliset testit tekee ylläpitotiimi.*

5. Miten mahdollinen ulkoistuskumppani tai palveluntarjoaja on varautunut jatkuvuuteen? Selvitä esimerkiksi:
   - Onko varautumisesta sovittu kumppanin kanssa?
   - Miten kumppanin jatkuvuussuunnitelma on varmistettu toimivaksi?

6. Onko jatkuvuudenhallinnasta sovittu asiakkaiden kanssa ja miten asia on dokumentoitu?

7. Mitkä ovat jatkuvuuden tavoitteet? Tavoite voi liittyä esimerkiksi:
   - Mahdollisimman nopeaan toipumiseen häiriötilanteesta, joka on melko todennäköinen (esimerkiksi tietoliikennehäiriö tai kyberhyökkäys)
   - Varautumiseen ennalta ääritilanteisiin, esimerkiksi sodan tai terrorismin uhkaan, maantieteellisen saarekkeen muodostamiseen, konesalista pilveen siirtymiseen tai irtautumiseen kokonaan jostain järjestelmästä.

8. Suunnitelkaa, miten jatkuvuudenhallintaa harjoitellaan säännöllisesti ja miten jatkuvuus- ja palautumissuunnitelmia kehitetään harjoitusten havaintojen pohjalta. Esimerkkejä:
   - Jatkuvuussuunnitelman tai palautumissuunnitelman säännöllinen katselmointi.
   - Työpöytäharjoitus, jossa harjoitellaan jatkuvuussuunnitelman käyttöä ja toimintaa etukäteen suunnitellun skenaarion ja syötteiden perusteella.
   - Vuosittainen laajempi jatkuvuusharjoitus palveluntarjoajien kanssa. Harjoitellaan päätöksentekotilanteita ja viestintää simuloidussa poikkeustilanteessa.
   - Varmuuskopioiden sekä koko palvelun tai sen osan palautuksen testaaminen.
   - Järjestelmän hallittu alasajo ja varajärjestelmien käynnistymisen varmistus.
   - Sähköjen tai tietoliikenneyhteyksien katkaisu ja tarkistus, että varavirta tai varayhteys käynnistyy odotetusti.

# 7. Aloita muutos tästä

**Kiteytä liiketoiminnan tarve ja ajurit muutokselle. Miksi muutos, esimerkiksi tietojärjestelmän hankinta, pilvipalveluun siirtyminen tai toisen konesalin käyttöönotto, halutaan tehdä ja mitä muutoksella halutaan saavuttaa? Kartoita myös, mitkä ovat odotettavat hyödyt ja mitä vaaditaan, että oletetut hyödyt toteutuvat. Mieti myös millaisiin riskeihin tai kustannuksiin yrityksesi on valmis sitoutumaan.**

## Vinkki!

Business Model Canvas voi auttaa tunnistamaan ja sanoittamaan muun muassa, millaisia hyötyjä liiketoiminta voi saada ja millaisia kustannuksia syntyy.

**Edeltävät vaiheet ja esiehdot:**
Aloita tästä kortista, Tunnista kriittiset toiminnot, Tunnista kriittisten toimintojen uhkat ja riskit

**Osaamis- tai vastuualueet:**
Liiketoiminta, Hallinnollinen tietoturva, Tietojärjestelmät, Yritysjohto

### Esimerkki: Cirrocumulus Logistics Ltd

Yritys on aikanaan hankkinut erillisiä tietojärjestelmiä tuntikirjaukseen ja laskutukseen, asiakkuuksien hallintaan ja projektinhallintaan. Käyttäjiltä on tullut palautetta ja kehitysehdotuksia näihin työkaluihin, jotta järjestelmät saataisiin sovitettua yksiköiden prosesseihin paremmin. Kyseiset tietojärjestelmät ovat kaikki eri toimittajilta ja aikanaan yrityksen silloisiin tarpeisiin räätälöity. Yritys kartoitti vaihtoehtoja ja kävi läpi nykyisten tietojärjestelmän vuosikustannuksia. Selvisi, että on saatavilla järjestelmiä, joissa kaikki halutut toiminnot löytyvät yhdestä järjestelmästä. Tämä toisi kustannussäästöjä ja vähentäisi järjestelmien välisten integraatioiden rakentamistarpeita, mutta myös kasvattaisi yhteen toimittajaan ja tietojärjestelmään liittyvää riskiä. Yritys puntaroi liiketoimintahyötyjen ja riskiprofiilin muutoksen suhdetta tehdessään päätöstä siirtyykö uusiin järjestelmiin.

### Esimerkki: Laastari Oy

Yrityksellä on tietovarastossa potilasdataa. Tietovarasto on rakennettu tuotteen päälle, josta on asennettu yrityksen konesaliin viimeisin versio. Tuotteen toimittaja ilmoittaa, että itse asennettavia versioita tuotteesta ei enää tule, vaan tulevaisuudessa kaikki versiot ovat pilvipohjaisia SaaS-palveluita. Tuki ja tietoturvapäivitykset itseasennettuun versioon päättyvät kahden vuoden kuluttua. Yritys ymmärtää, että muutos on väistämätön ja aloittaa projektin selvittääkseen voivatko he käyttää pilvipohjaista versiota tuotteesta ja millä reunaehdoilla.

# 7. Aloita muutos tästä

## Keskeiset tehtävät

1. Miksi muutos halutaan tehdä? Onko muutos yrityksen strategian mukainen?
   - Esimerkki: *Finanssialan organisaatio kokee olevansa kilpailijoita jäljessä digitalisoitumisessa.*
   - Esimerkki: *Teollisuusyritys haluaa tehostaa tuotannon prosesseja automatisoinnilla. Samalla vähennetään työvoiman tarvetta.*
   - Esimerkki: *Tietojärjestelmätuotteen toimittaja lopettaa konesaliin asennettavien versioiden tuen ja tarjoaa tulevaisuudessa vain pilvipohjaisia SaaS-tuotteita.*
2. Mitä konkreettisia hyötyjä muutoksesta aiheutuu omalle liiketoiminnalle tai asiakkaille?
   - Esimerkki: *Kustannussäästöt.*
   - Esimerkki: *Asiakkaalle tuotettavan palvelun saatavuustaso paranee.*
   - Esimerkki: *Henkilöstön päivittäisen työn tehokkuus paranee.*
   - Esimerkki: *Ei suoria hyötyjä, mutta ilman muutosta voi seurata vakavia haittoja.*
3. Millaisia haittoja ja riskejä omalle liiketoiminnalle muutoksesta voi seurata? Millaisiin riskeihin yritys on valmis sitoutumaan?
   - Esimerkki: *Teollisuusalan yritys harkitsee tuotannonohjauksen siirtämistä pilveen. Muutosprojekti on mittava ja sen aikataulu ja kustannukset voivat venyä.*
   - Esimerkki: *Yritys päättää siirtää palveluita konesalistaan pilvipalveluihin. Yrityksellä ei ole omia pilvipalveluasiantuntijoita, vaan osaamista tarvitaan ulkoa.*
4. Onko muutokselle jotain rajoituksia tai vaatimuksia? Rajoitukset voivat liittyä esimerkiksi kustannuksiin, teknologioihin tai lainsäädäntöön.
   - Esimerkki: *Yritys yhdistää lukuisia tietovarantojaan, joissa on luokiteltua tietoa. Tästä syntyy kasautumisvaikutus, joka nostaa tiedon turvallisuusluokkaa.*
   - Esimerkki: *Terveydenhuoltoalan yritys harkitsee siirtymistä pilvipalveluun, jota tuotetaan Suomen ulkopuolelta. Yrityksen tulee huomioida mm. määräys sosiaali- ja terveydenhuoltojärjestelmien olennaisista ja toiminnallisista ja tietoturvavaatimuksista.*
5. Mihin kriittisiin toimintoihin muutos kohdistuu?
   - Esimerkki: *Muutos kohdistuu yrityksen verkkokauppaan.*
   - Esimerkki: *Muutos kohdistuu viranomaisille tuotettavaan raportointiin.*

### Esimerkki: Moniala Oy

Yritys, jonka tarjoamilla palveluilla on korkeat saatavuusvaatimukset, tuottaa palveluitaan omasta konesalistaan, koska kansainvälisten tietoliikenneyhteyksien katkaiseminen ei saa häiritä toimintaa. Sovelluskehitys on kuitenkin hitaampaa ja kalliimpaa konesalissa kuin mitä se olisi pilvipalveluissa. Yritys selvittää, onko mahdollista pitää tuotantoympäristö konesalissa, mutta tehdä sovelluskehitystä ja testausta pilvipalvelualustaa hyödyntäen. Tälle mallille ei ole estettä, kunhan yritys varmistaa tuotantodatan pysyvän vain konesalissa ja pilvipalveluissa käytetään turvallista testidataa.

# 8. Tunnista muutoksen kohteena oleva tieto

**Kartoita käsitelläänkö muutoksen seurauksena jotain uutta tietoa, poistuuko jotain tietoa vai syntyykö jotain uudenlaista tietoa. Tämän ymmärtäminen on tärkeää, jotta tarvittavat tietoturva- ja tietosuojavaatimukset sekä lain ja sopimusten aiheuttamat rajoitteet osataan täyttää.**

## Vinkki!

Tietojärjestelmäuudistuksessa muutoksen kohteena oleva tieto ei välttämättä rajoitu pelkästään kyseiseen tietojärjestelmään, vaan lisäksi kannattaa tutkia, mitä tietoa käsitellään siihen integroiduissa tietojärjestelmissä.

**Edeltävät vaiheet ja esiehdot:**
Tunnista kriittiset toiminnot, Tunnista kriittiset tiedot, Tunnista lainsäädännön ja toimialan vaatimukset

**Osaamis- tai vastuualueet:**
Liiketoiminta, Kriittisen prosessin toiminta ja kehitys, Hallinnollinen tietoturva, Tietojärjestelmät

**Esimerkki: Cirrocumulus Logistics Oy**

Yritys haluaa vaihtaa aiemmat erilliset tietojärjestelmänsä yhteen tietojärjestelmään. Käsiteltäviä tietoja ovat mm:

- Henkilöstön nimi, sähköposti, tehtävänimike, tiimi, osaamisalueet
- Henkilöstön tuntikirjaukset projekteille ja poissaolomerkinnät kommentteineen
- Asiakkaiden nimet ja asiakkaan yhteyshenkilöiden yhteystiedot
- Projektien nimi, kesto, laskutusperuste, projektin hinta, projektissa työskentelevät henkilöt ja projektipäällikkö
- Projektin laskutusaste ja lähetetyt laskut.

Mitään uudenlaista tietoa ei muodostu mutta tieto kootaan yhteen paikkaan. Aiempiin järjestelmiin kohdistuneet asiakasvaatimukset ja lainsäädäntö kohdistuu myös tähän järjestelmään. Päättyneitä projekteja ja edellisen vuoden tuntikirjauksia ei tulla siirtämään uuteen järjestelmään, joten nämä tiedot arkistoidaan erikseen siltä varalta, että tietoihin tulee tarpeen palata. Tunnista muutoksen kohteena oleva tieto

# 8. Tunnista muutoksen kohteena oleva tieto

## Keskeiset tehtävät

1. Tarkistakaa tiedot, joita muuttuvassa toiminnossa tai tietojärjestelmässä käsitellään nykyisellään. Katso kortti *Tunnista kriittiset tiedot.*
2. Muodostuuko tai käsitelläänkö tässä muutoksessa jotain uudenlaista tietoa?
   - Millaista tieto on ja miten kriittistä se on?
   - Onko tiedon käsittelyyn jotain velvoitteita tai rajoitteita?
   - Mitkä ovat nykyiset tietovarastot ja miten ne on suojattu?
3. Poistuuko jokin aiempi tieto käytöstä tässä muutoksessa?
4. Käsitelläänkö muutoksen vuoksi tietoa eri tavalla kuin ennen?
   - Tekninen muutos – esimerkiksi uusi tietojärjestelmä tallentaa sovelluslokeihin yksityiskohtaisempaa tietoa kuin ennen
   - Prosessimuutos – esimerkiksi ylläpitokumppanin vaihtuminen tai SaaS-malliin siirtyessä vastuun jakautuminen

### Esimerkki: Laastari Oy

Tietojärjestelmäuudistuksen kohteena on potilasjärjestelmä, jossa tallennetaan potilaiden perushenkilötiedot sekä sairaus- ja hoitohistoria. Näistä tiedoista kriittisiä ovat aiemmin tunnistetut potilaan kriittiset riskitiedot. Uudenlaisia tietoa ei muodostu. Muutoksen yhteydessä tunnistetaan, että asiakkaista kerätään sellaisia tietoja, jotka eivät ole yrityksen nykyprosesseilla enää välttämättömiä. Näiden tietojen keräämisestä päätetään luopua ja olemassa oleva tiedot tuhota.

### Esimerkki: Moniala Oy

Yritys tarjoaa asiakkailleen valvontakamerapalvelua, jota tuotetaan yrityksen omasta konesalista. Palvelussa käsiteltävä henkilötieto sisältää pääkäyttäjien yhteystietojen lisäksi videokuvaa. Moniala Oy käyttää tällä hetkellä suomalaista kumppania palvelun jatkokehitykseen ja ylläpitoon. Palvelun operointi- ja kehityskustannukset ovat kuitenkin suuret, joten yritys päättää siirtää palvelun pilvipalvelualustalle, uudistaa samalla teknistä järjestelmää ja kilpailuttaa ylläpitokumppanin.

Kun järjestelmä siirretään pilvialustalle ja käsiteltävät tiedot ovat periaatteessa samat sekä vanhassa ja uudessa järjestelmässä, muutoksia voi silti aiheutua. Palvelun käyttämät datakeskukset sijaitsevat Euroopassa, mutta uudella ylläpitokumppanilla on vianselvitystä tekeviä työntekijöitä Yhdysvalloissa ja Intiassa. Vianselvitys voi vaatia videotallenteiden tarkistamista ja muiden henkilötietojen käsittelyä, jolloin henkilötietojen käsittelyn turvallisuus GDPR:n vaatimalla tavalla on varmistettava.

# 9. Tunnista muutoksessa tarvittava osaaminen ja resurssit

**Tunnista millaista osaamista ja resursseja vaaditaan sekä muutoksen läpiviemiseksi että muutosprosessin jälkeisten hyötyjen kotiuttamiseksi. Tämä kortti auttaa tunnistamaan tarpeita osaamisen hankkimisen (koulutus, rekrytointi, jne.) ja työn ulkoistamisen suhteen.**

## Vinkki!

Tarvittava osaaminen voi olla hyvin hienojakoista. Esimerkiksi pilvisiirtymä voi vaatia osaamista valitusta pilvestä, migraatioprojektien läpiviennistä, pilven hallintamallista, alanne erityispiirteistä, regulaatiosta ja lainsäädännöstä, pilviarkkitehtuurista, sovelluskehityksestä sekä ylläpidosta. Nämä osaajat ovat harvoin yksi ja sama ihminen, ja jatkuvuusriskin takia kutakin osaamisaluetta olisi hyvä löytyä useammalta kuin yhdeltä henkilöltä. Kumppani- ja toimittajaverkostoa kannattaa ehdottomasti hyödyntää, jos yrityksen strategiassa ei ole rekrytoida tarvittavia osaajia itse. Pilvialustoja tarjotaan myös “avaimet käteen” eli Managed Service Provider (MSP) -mallilla, jossa toimittaja vastaa pilven hallinnasta ja ylläpidosta.

**Edeltävät vaiheet ja esiehdot:**
Aloita muutos tästä, Tunnista muutoksen kohteena oleva tieto

**Osaamis- tai vastuualueet:,** Osaaminen ja koulutus

**Esimerkki: Cirrocumulus Logistics Oy**

Yrityksen tietojärjestelmäuudistus halutaan toteuttaa projektina ja projektille tarvitaan kokenut projektipäällikkö. Lisäksi projektiin halutaan mukaan mieluiten aiempien tietojärjestelmien pääkäyttäjät tai ainakin henkilöt, joilla on vastaavaa käytännön kokemusta laskutusprosesseista, henkilöstöhallinnon prosesseista ja yrityksen osaamisen hallinnan ja projektinhallinnan prosesseista. Lisäksi yritys tunnistaa, että yrityksen juristi ja tietoturvapäällikkö kannattaa ottaa mukaan alusta alkaen auttamaan lainsäädäntöön, tietosuojaan ja tietoturvaan liittyvissä kysymyksissä. Projektin kartoitustyöhön varataan aikaa puoli vuotta, minkä jälkeen varsinainen toteutustyö arvioidaan erikseen.

# 9. Tunnista muutoksessa tarvittava osaaminen ja resurssit

## Keskeiset tehtävät

1. Miettikää, millaista osaamista tarvitaan, että muutoksen liiketoimintahyödyt saadaan lunastettua. Osaaminen voi liittyä esimerkiksi muutosjohtamiseen, projektinhallintaan, tietoturvaan, tietosuojaan, lainsäädäntöön, toimialaan tai tiettyihin teknologioihin.
   - Esimerkki: *Muutos tulee näkymään myös asiakkaille, joten tarvitaan toimialatuntemusta ja vahvaa viestintäosaamista, jotta asiakkaat saadaan vakuutettua heille koituvista hyödyistä.*
   - Esimerkki: *Pilvipalvelualustojen tarjoamat kustannus-, skaalaus- ja ketteryyshyödyt toteutuvat, jos pilvipalveluja käytetään oikein. Jos toimitaan konesalista opituilla tavoilla, kustannukset voivat jopa kasvaa.*
2. Onko osaamisen tarve lyhytaikaista vai pitkäaikaista? Jos tarvittavaa osaamista ei saada, aiheutuuko siitä riskejä toiminnan jatkuvuudelle?
3. Mistä tätä osaamista voidaan saada?
   - Onko talossa omaa osaamista aihepiirissä?
   - Onko mahdollista lisäkouluttautua ja miten kauan se veisi aikaa?
   - Mitä vaihtoehtoja on ulkopuolisen osaamisen saantiin esimerkiksi alihankinnalla tai konsultointisopimuksilla?
4. Tarvitseeko projektia varten tehdä erityisiä hankintoja tai varata toimitiloja?
   - Esimerkki: *Muutosprojektia varten varataan oma projektityöhuone yrityksen tiloista puoleksi vuodeksi.*
   - Esimerkki: *Projektihenkilöstölle hankitaan erilliset työasemat viranomaisen turvaluokitteleman tiedon käsittelyä varten.*
   - Esimerkki: *Yritys siirtyy käyttämään pilvipalvelualustaa. Yritys käynnistää projektin, jossa pilvipalveluun luodaan tarvittava pohja. Asiat kuten pilven hallintamalli, tilirakenne, keskeisin vastuunjako ja tietoturvallisen käytön pohjatyöt asetetaan kuntoon, ennen kuin itse sovellusten kehittäminen aloitetaan.*
5. Millaisia kustannuksia muutoksen vaatimista resursseista ja osaamisen hankkimisesta syntyy? Miten kustannukset budjetoidaan?

### Esimerkki: Moniala Oy

Moniala Oy jatkokehittää konesalista tarjottavia liiketoiminnalle tärkeitä palveluita. Yritys on tunnistanut, että pilvipalvelualustalle siirtyminen tehostaisi sekä kehitystyötä että mahdollistaisi alemmat operointikustannukset. Koska yrityksellä ei itsellään ole pilvipalveluosaamista, he käyttävät kumppanin apua migraatiovaiheessa. Yrityksen omat konesaliosaajat uudelleenkouluttautuvat kyseisen pilvialustan osaajiksi. Onnistuneen migraation jälkeen yritys käyttää vain omaa työvoimaa. Vuoden päästä kuitenkin huomataan, että pilvisiirtymän suunnitellut hyödyt, kuten nopeampi ja iteratiivinen kehityssykli, eivät toteudu. Vaikka migraatioprojekti onnistui, yritys ei onnistunut muuttamaan merkittävästi toimintatapojaan eikä uusia pilvialustan ominaisuuksia otettu käyttöön. Yritys päättää, että kertaluontoisen panostuksen lisäksi tarvitaan jatkuvaa työtä sen eteen, että toimintatavat ja kulttuuri muuttuvat ketterämmäksi.

# 10. Tunnista toteutusmahdollisuudet ja teknologiat

**Kartoita, mitä toteutusmahdollisuuksia muutokselle on teknologia-, yhteensopivuus- ja kustannusmielessä. Vertaile, mitkä ovat toteutusvaihtojen edut ja haitat. Toteutusmahdollisuuksien selvittämisen aikana voi olla tarpeen palata vaiheeseen Tunnista muutoksessa tarvittava osaaminen ja resurssit.**

### Edeltävät vaiheet ja esiehdot:

Tunnista kriittisten toimintojen uhkat ja riskit, Tunnista lainsäädännön ja toimialan vaatimukset, Tunnista muutosprojektissa tarvittava tieto, Tunnista muutoksessa tarvittava osaaminen ja resurssit

### Osaamis- tai vastuualueet:

Järjestelmäarkkitehtuuri, Teknologia-asiantuntemus, Liiketoiminta, Lainsäädäntö

### Esimerkki: Laastari Oy

Yrityksellä on konesalissaan elinkaaren lopussa oleva tietojärjestelmä, jossa on komponentteja, joihin ei enää saa tietoturvapäivityksiä. Yritys käy läpi vaihtoehtoja tietojärjestelmän uusimiselle:

1. Ostetaan SaaS-palveluna toiminnoiltaan vastaava järjestelmä:
   - Haasteena on, ettei SaaS-palvelu tue integraatiota yrityksen muihin järjestelmiin ja SaaS-toimittaja ei halua tehdä custom-toteutusta vain yhdelle asiakkaalle.
2. Järjestelmä modernisoidaan teknisesti ja toiminnallisesti vastaamaan nykytarpeita ja se toteutetaan AWS-pilvipalvelualustalle:
   - Toteutustapana kustannustehokas pilvinatiivi vai tarvittaessa toiselle pilvialustalle tai takaisin konesaliin siirron mahdollistava alustariippumaton malli?
   - Miten rakennetaan yhteys pilvestä konesaliin integraatioita varten?
   - Mitä uudenlaista osaamista toteutus ja sen jatkokehitys sekä ylläpito vaatii?
   - Millaiseksi kustannukset muodostuvat ja voidaanko ne ennustaa tarpeeksi hyvin?
   - Vanhan järjestelmän yhden komponentin tietoturvapäivitykset päättyvät pian. Entä jos projektin aikataulu venyy ja komponentista löytyy haavoittuvuus?
3. Vanhentunut teknologiakomponentti korvataan vastaavalla avoimen lähdekoodin toteutuksella. Epäyhteensopivat toiminnot toteutetaan uudestaan. Toteutus pidetään edelleen konesalissa. Tässä vaihtoehdossa on mm. seuraavia etuja:
   - Ennustettavissa oleva työmäärä, sillä nykyinen palveluntarjoaja on toteuttamassa vastaavanlaista projektia toiselle asiakkaalle.
   - Palvelun operointikustannukset pysyvät muutoksen jälkeen ja aikana ennallaan.
   - Yrityksen ei tarvitse etsiä uutta osaamista talon ulkopuolelta.
   - Valittu tapa ei estä pilvisiirtymää myöhemmin tulevaisuudessa

Kustannuksista, aikataulusta ja osaamistarpeista johtuen yritys päätyy pitämään ratkaisun konesali-toteutuksena. Vanhentunut komponentti korvataan uudella välttäen isompia muutoksia.

# 10. Tunnista toteutusmahdollisuudet ja teknologiat

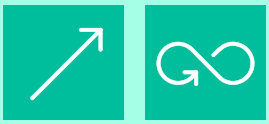
## Keskeiset tehtävät

1. Kartoita ja vertaile erilaisia toteutusmahdollisuuksia, esimerkiksi seuraavilla aspekteilla:
   - Millainen toteutustapa on kyseessä?
     - Julkinen pilvipalvelu, hybridipilvi, yksityinen pilvi vai oma konesali?
     - Pilvipalvelun hallintamallin kannalta: IaaS, PaaS, FaaS, SaaS, BPaaS
     - Voiko ratkaisun toteuttaa alustariippumattomasti vai riippuuko ratkaisu tietystä palvelun-tarjoajasta tai teknologiasta?
   - Onko toteutus yhteensopiva olemassa olevien palveluiden kanssa?
     - Ovatko tiedot siirrettävissä muuhun järjestelmään tarvittaessa?
     - Mikä on ratkaisun elinkaari? Käyttääkö se esimerkiksi jotain vanhentuvaa teknologiaa tai jonka ylläpito vaatii erityisosaamista?
     - Miten ratkaisu integroituu nykyisiin järjestelmiin?
     - Miten ratkaisu sopii yhteen mahdollisten muiden lähitulevaisuuden teknologiamuutosten kanssa?
   - Mitkä toteutusmahdollisuudet sopivat parhaiten yrityksen strategiaan?
     - Esimerkki: *Yrityksen strategian keskiössä on tiedolla johtaminen. Yritys välttää niitä teknologia-ratkaisuja, joista tietoja ei voi kerätä ja hyödyntää.*
     - Esimerkki: *Yritys keskittyy vahvasti ydinosaamiseensa ja suosii “avaimet käteen” -toteutus-malleja, jotka eivät vaadi heiltä erikoisosaamista.*
   - Millainen kustannus/investointi ratkaisu on lyhyellä ja pidemmällä aikavälillä?
   - Miten hyvin ratkaisut vastaavat aiemmin tunnistettuihin vaatimuksiin ja reunaehtoihin, kuten lakien tai toimialastandardien vaatimuksiin?
2. Miten kriittisten toimintojen uhkat ja riskit muuttuvat eri toteutusteknologioissa?
   - Esimerkki: E*lintarvikealan tuotantoyritys käyttää tuotannonohjausjärjestelmää, jota ylläpidetään konesalissa. Järjestelmään pääsee vain tehtaalta ja toimistoilta VPN:llä, joten kyberhyökkäykset vaativat fyysisten suojauksien ohittamista. Kun järjestelmä vaihdetaan SaaS-pohjaiseksi ja liike-toiminnan pyynnöstä sen käyttö mahdollistetaan myös mobiililaitteilta, riski hyökkäyksille ja luvattomalle pääsylle tietoon kasvaa, vaikka palvelun skaalautuvuus ja saatavuus paraneekin.*

### Esimerkki: Cirrocumulus Logistics Ltd

Yrityksen linjauksen mukaisesti Cirrocumulus Logistics harkitsee ainoastaan SaaS-palveluja, koska he eivät haluaa ylläpitää järjestelmää itse. Vaihtoehtoisia SaaS-tuotteita on aluksi kolme, mutta vain kaksi niistä tukee heidän kertakirjautumisjärjestelmäänsä. Molemmat näistä palveluntarjoajista mahdollistavat tiedon säilytyksen ja käsittelyn rajaamisen EU/ETA-alueelle. Ensimmäisellä palveluntarjoajalla on ISO 27001 - ja SOC 2 -sertifioinnit, mutta toisenkin palveluntarjoajan tietoturvakuvaus ja tietoturva-testauksen raportti antavat melko positiviisen kuvan. Jälkimmäisen palvelun kustannukset ovat alhai-semmat ja lisäksi käytettävyys ja räätälöintimahdollisuudet ovat paremmat. Yritys päättää arvioida molempien ratkaisujen tietoturvaa tarkemmin ja kokeilla ratkaisua proof of concept -kokeilujaksolla ennen varsinaista päätöstä, vaikka alustavasti jälkimmäinen palveluntarjoaja vaikuttaakin houkuttelevammalta.

# 11. Rakenna ja arvioi uuden toteutuksen tietoturvaa ja tietosuojaa



**Tietojärjestelmää tai pilvipalvelua hankittaessa sen tietoturva ja tietosuoja kannattaa arvioida monelta kannalta erikoisasiantuntijoiden avulla, jotta vaatimusten täyttyminen voidaan tarkistaa ja tarvittaessa toteuttaa lisätoimenpiteitä tietoturvaongelmilta suojautumiseksi. Kannattaa myös miettiä, muuttuvatko tietoturvariskit aiempaan verrattuna: esimerkiksi uusi toteutus voi pienentää tiettyjä aiemman ratkaisun tietoturvariskejä, mutta tuoda mukanaan uusia. Tietoturvan ja tietosuojan jäännösriskit ja vastuut tulee ymmärtää ja hyväksyä tai siirtää. Arviointi on joskus järkevää tehdä esimerkiksi muutamalle varteenotettavalle toteutusvaihtoehdolle, jolloin lopullinen valinta voidaan tehdä riskipohjaisesti.**

**Mikäli yritys on mukana uuden ratkaisun kehittämisessä alusta alkaen, tietoturvaa kannattaa alkaa rakentaa järjestelmään alusta alkaen DevSecOps-mallilla.**

**Edeltävät vaiheet ja esiehdot:**
Tunnista kriittisten toimintojen uhkat ja riskit, Tunnista lainsäädännön ja toimialan vaatimukset, Tunnista toteutusmahdollisuudet ja teknologiat

**Osaamis- tai vastuualueet:**
Liiketoiminta, Kriittisen prosessin toiminta ja kehitys, Järjestelmäarkkitehtuuri, Teknologia-asiantuntemus, Hallinnollinen tietoturva, Tekninen tietoturva, Tietosuoja , Lainsäädäntö

**Esimerkki: Cirrocumulus Logistics Ltd**

SaaS-palveluiden teknistä ja fyysistä tietoturvaa ei voida testata, mutta Cirrocumulus Logistics pyytää tietoturvakonsultointifirmalta apua palvelun tietoturvan arvioimiseen. Molemmilta varteenotettavilta palveluntarjoajilta pyydetään palvelun tietoturva- ja tietosuojakuvaukset, lisätietoa tietoturvaan liittyvistä sertifioinneista ja tietoturva-auditointien ja teknisten testauksien raporteista. Konsulttifirman avulla yritys lähettää myös tarkentavia kysymyksiä tietoturvakäytännöistä palveluntarjoajille. Yrityksen juristi tarkistaa myös sopimusehdot molemmista palveluista.

Edullisemman ja käytettävyydeltään paremman ykkössuosikin sopimusehdot ovat juristin mielestä huonot, sillä palveluntarjoajan vastuu tietoturvaloukkaustilanteissa on vähäinen, eikä hän arvele niissä olevan juurikaan neuvottelun varaa. Lisäksi konsulttiyrityksen mielestä palveluntarjoajan kuvaus haavoittuvuuksienhallinnasta ja tietoturvapoikkeamien valvontakyvystä ei herätä luottamusta. Yritys päätyy valitsemaan toisen palveluntarjoajan, sillä sen kanssa jäännösriskit ovat pienemmät.

# 11. Rakenna ja arvioi uuden toteutuksen tietoturvaa ja tietosuojaa

## Keskeiset tehtävät

1. Valitkaa, mitä kriteerejä järjestelmän tietoturvan ja tietosuojan tulee täyttää. Käytä apuna korttia Tunnista lainsäädännön ja toimialan vaatimukset.
2. Mikäli olette kehittämässä tietojärjestelmää:
   - Suunnitelkaa, miten noudatatte tietoturvallisen ohjelmistokehityksen ja ylläpidon periaatteita. Lisätietoa on luvussa ”Miten käyttää pilvipalveluita turvallisesti?”
   - Esimerkki: Kehitystiimi on jakanut kehitystehtävät aihekokonaisuuksiksi ja niihin kuuluviksi tehtäviksi. Jokaiselle isommalle aihekokonaisuudelle, joita ovat esimerkiksi arkkitehtuurimuutos tai uusi tai muuttuva ominaisuus, tehdään uhkamallinnus. Mikäli aihekokonaisuuteen liittyy henkilötietojen käsittelyä, tarkistetaan myös tietosuojan vaikutustenarvioinnin ajantasaisuus.
3. Mikäli otatte käyttöön olemassa olevaa tietojärjestelmää tai palvelua:
   - Arvioikaa arkkitehtuuri kokonaisarkkitehtuurin ja tietoturvan kannalta järjestelmäarkkitehtuurin ja tietoturvan osaajien kanssa. Ottakaa huomioon erityisesti kriittisten toimintojen ja tietojen jatkuvuus suojaaminen.
   - Analysoikaa toteutuksen uhkat esimerkiksi uhkamallinnuksen avulla: mikä voi mennä pieleen? Mitä voimme tehdä asialle?
   - Järjestäkää tekninen tietoturvatestaus järjestelmälle. Toteutuksesta riippuen kannattaa huomioida seuraavia osa-alueita: asiakassovellukset, palvelinalusta, käyttöjärjestelmä, tietojenkäsittely-ympäristö, tietoliikenne ja hallintarajapinnat.
   - Tehkää tietosuojaa koskeva vaikutustenarviointi henkilötietoihin liittyvien riskien ymmärtämiseksi.
4. Arvioikaa lopuksi uhkamallinnuksen, testaustulosten ja tietosuojan vaikutustenarvioinnin perusteella riskin suuruus ja riskiä pienentävät toimenpiteet, jotka on syytä toteuttaa ennen ratkaisun käyttöönottoa. Arvioikaa jäännösriski ja onko se hyväksyttävällä tasolla.

### Esimerkki: Laastari Oy

Laastari Oy:n potilastietojärjestelmä on B-luokan sote-järjestelmä, joten siltä ei vaadita ulkopuolista tietoturvan arviointia. Nyt Laastari Oy haluaa kuitenkin teettää sellaisen. Tietoturvan arviointikriteerinä ovat sosiaali- ja terveydenhuoltojärjestelmien tietoturvan vähimmäisvaatimukset, jotka löytyvät Valviran verkkosivuilta. Lisäksi tietoturva-auditointifirman kanssa sovitaan, että he testaavat järjestelmää ja sen web-käyttöliittymää myös OWASP Application Security Verification Standardin tason 2 mukaisesti.

Aiemman järjestelmän arkkitehtuuri on arvioitu tietoturvan kannalta kymmenen vuotta sitten ja siitä on olemassa suppeahko raportti. Sieltä löytyneet havainnot huomioidaan, mutta arkkitehtuurin arviointi päätetään tehdä kokonaisuudessaan uudestaan eikä pelkästään muutoksiin keskittyen. Tällä kertaa kiinnitetään erityistä huomiota myös jatkuvuudenhallintaan.

# 12. Varmista onnistunut muutos

**Tunnista, mitä kaikki muuttuu esimerkiksi pilvisiirtymän tai tietojärjestelmä-uudistuksen jälkeen ja miten muutokset pitää huomioida esimerkiksi koulutuksessa, ohjeissa, prosesseissa tai jatkuvuudenhallintasuunnitelmissa.**

**Muutosprosessissa on jo tunnistettu suuret linjat, kuten liiketoimintahyödyt ja riskit sekä käyty läpi muutoksen kohteena oleva tieto ja osaamistarpeen muutokset. Toteutusvaihtoehtoja on rajattu ja tulevan toteutuksen tietoturva ja tietosuoja on varmistettu. Tämä kortti painottaa niitä asioita, joita muutoksesta seuraa ja jotka pitää huomioida jo muutosprosessin aikana. Muutos on myöskään harvoin päättyvä projekti, vaan se vaatii jatkuvaa huomiota.**

## Vinkki!

Tämä kortti kannattaa käydä läpi muutoksen alussa, muutoksen aikana sekä muutoksen jälkeen.

**Edeltävät vaiheet ja esiehdot:**
Kaikki muut muutosvaiheen kortit

**Osaamis- tai vastuualueet:**
Viestintä, Osaaminen ja koulutus, Hallinnollinen tietoturva

**Esimerkki: Cirrocumulus Logistics Ltd**

Cirrocumulus Logistics otti käyttöön uuden tietojärjestelmän, joka yhdistää aiempia tietojärjestelmiä. Uusi tietojärjestelmä päätettiin ottaa käyttöön vaiheittain eri tiimeille, jotta loppukäyttäjien koulutus voidaan järjestää porrastetusti - muutoksia oli nimittäin tulossa mm.

- tuntikirjausohjeisiin
- poissaolomerkintöjen hyväksymisprosessiin, sillä osa toiminnoista automatisoitiin
- tuntikirjausten tarkastamisprosessiin, ja
- projektinhallintaohjeisiin.

Lisäksi yritys tunnisti seuraavat tarvittavat muutostehtävät:

- Riskiarvion päivitys muuttuneiden tietojärjestelmien osalta.
- Jatkuvuussuunnitelman päivitys ja harjoittelun kehittäminen. Nyt yksittäisen tietojärjestelmän häiriö on erityisen kriittinen, joten jatkossa halutaan varmistaa palveluntarjoajan kyvykkyys toimintaan häiriö-tilanteissa yhteisillä jatkuvuusharjoituksilla
- Korostetut viestintätarpeet muutoksen aikana hälventääkseen muutosvastarintaa
- Varmista onnistunut muutos

# 12. Varmista onnistunut muutos

## Keskeiset tehtävät

1. Käykää läpi, miten muutos vaikuttaa yrityksenne toimintaan?
   - Vastuunjaon osalta
     - Esimerkki: *Kun järjestelmä oli omassa konesalissa, vastuu oli kokonaan itsellä. Uudessa toteutuksessa on monitoimittajamalli: pilvipalveluntarjoaja vastaa fyysisestä turvallisuudesta ja ajoalustan ja sen tarjoamien hallinnoitujen palvelujen turvallisuudesta. Kumppani operoi ja valvoo sovelluksia ja toteuttaa pienkehitystä. Lopullinen vastuu säilyy kuitenkin aina yrityksellä alihankintaketjusta riippumatta.*
   - Prosessien ja toimintamallien osalta
     - Esimerkki: *Koska uutta tietojärjestelmää ei enää ylläpidä oma IT, siihen liittyvät vikailmoitukset välitetään suoraan help desk -palvelusta suoraan palveluntarjoajalle.*
   - Ulkopuolisten tahojen, esim. sopimuskumppanien ja asiakkaiden osalta
     - Esimerkki: *Järjestelmämuutos mahdollistaa tekstiviestimuistutuksen asiakkaille. Puhelinnumeroja ei ole ennen kerätty asiakkailta.*

2. Käykää läpi, miten muutos vaikuttaa uhkiin ja niihin varautumiseen.
   - Muuttuvatko toimintoon tai koko yritykseen liittyvät uhkat tai riskit?
     - Esimerkki: *Kumppaniyrityksellä on laaja pääsy tietojärjestelmiin ja kumppanin alihankintaketju voi aiheuttaa tietoturvauhkia. Kumppanin liiketoiminnan haasteet vaikuttavat merkittävästi omaan toimintaan.*
   - Muuttuuko kriittisten tietojen ja toimintojen jatkuvuus? Tarvitseeko jatkuvuussuunnitelmia päivittää?
     - Esimerkki: *Jatkuvuussuunnitelmaa päivitetään ja harjoitellaan. Samalla luodaan palautumissuunnitelma, jos pilvipalvelusta joudutaan palaamaan myöhemmin takaisin konesaliin.*

3. Onko muita vaikutuksia?
   - Esimerkki: *Muutoksen jälkeen yrityksen kaikki merkittävät palvelut ovat samassa pilvipalvelussa. Yritys punnitsee hyötyjä ja haittoja pilviriippumattomassa toteutustavassa ja usean pilvipalvelun hyödyntämisessä yhden sijaan.*

4. Suunnitelkaa muutoksen läpivienti, seuranta ja mitä muutoksen jälkeen tapahtuu.
   - Esimerkki: *Muutoksen tarkoituksesta, etenemisestä ja vaikutuksista käydään säännöllisesti avointa keskustelua henkilöstön ja muiden osapuolien kanssa.*
   - Esimerkki: *Muutoksen läpivienti aikataulutetaan sprintteihin. Jokaisen sprintin lopuksi arvioidaan, miten muutosprojekti on sujunut tähän asti.*

### Esimerkki: Laastari Oy

Laastari Oy:n tietojärjestelmän modernisoinnin yhteydessä myös sovelluksen käyttöliittymää päivitetään selkeämmäksi. Henkilöstölle järjestetään uuden järjestelmän käyttökoulutus ja lisäksi jokaiseen työhuoneeseen printataan pikaohjeet. Lisäksi palveluntarjoaja päivittää tietojärjestelmän palautussuunnitelmaa vastaamaan uutta toteutusta.

# Liite 1: Termit ja määritelmät

**GDPR**
General Data Protection Regulation (GDPR) on eurooppalainen henkilötietojen käsittelyä koskeva laki, jota alettiin soveltaa vuonna 2018.

**Haavoittuvuus**
Haavoittuvuus on tietojärjestelmässä tai ympäristössä oleva heikkous, jota voidaan käyttää hyväksi. Esimerkiksi toimiston oven jättäminen lukitsematta illalla tai se, että palvelinta ei ole kahdennettu, ovat haavoittuvuuksia.

**HIPAA**
Health Insurance Portability and Accountability Act (HIPAA) on yhdysvaltalainen potilastietojen yksityisyyttä koskeva laki.

**Huoltovarmuus**
Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa. Huoltovarmuuden turvaaminen on määritetty laissa.

**Huoltovarmuuskriittinen organisaatio**
Huoltovarmuuskriittinen organisaatio on yritys tai muu organisaatio, joka on erityisen merkittävä yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta.

**Huoltovarmuuskriittinen toiminto**
Huoltovarmuuskriittisellä toiminnolla on vaikutusta Suomen huoltovarmuuteen, eli kykyyn ylläpitää yhteiskunnan perustoimintoja. Esimerkiksi teleoperaattorin matkapuhelinverkon ylläpito on huoltovarmuuskriittinen toiminto.

Mikäli yrityksesi tuottaa tai tukee toimintoja, jotka ovat huoltovarmuuskriittisiä, myös nämä toiminnot tulee käsitellä kuten liiketoimintakriittiset toiminnot.

**Häiriö**
Häiriöllä tarkoitetaan tässä ohjeessa tapahtumaa, joka vaarantaa yrityksen prosessien normaalitoiminnan.

**ISO/IEC 27001**
ISO/IEC 27001 tai usein lyhyesti ISO 27001 on tunnettu kansainvälinen standardi tietoturvan hallintajärjestelmälle.

**Jatkuvuudenhallinta**
Jatkuvuudenhallinta tarkoittaa prosessia, jossa tunnistetaan toimintaa koskevat uhkat, arvioidaan niiden vaikutukset sekä organisaatiolle että sen kumppaneille ja asiakkaille, ja luodaan tapa toimia häiriötilanteiden varalle.

Lue lisää jatkuvuudenhallinnasta.

**Jatkuvuussuunnitelma**
Jatkuvuussuunnitelmassa määritetään keinot, joilla yritys varautuu poikkeustilanteisiin ja joilla poikkeustilanteet hoidetaan.

**Konesali**
Kts. Pilvipalvelu ja konesali.

**Kriisi**
Kriisi on vakava poikkeustilanne, joka vaatii erityistoimenpiteitä.

**Kriittinen toiminto**
Tässä oppaassa keskitytään kolmenlaisiin yrityksen kriittisiin toimintoihin: liiketoimintakriittisiin toimintoihin, huoltovarmuuskriittisiin toimintoihin ja regulaatiokriittisiin toimintoihin. Niihin kaikkiin viitataan tässä oppaassa termillä kriittinen toiminto.

Sama toiminto voi olla kaikkea kolmea yhtä aikaa tai vain osaa näistä. Esimerkiksi on hyvin tyypillistä, että huoltovarmuuskriittinen toiminto tai regulaatiokriittinen toiminto ei ole välttämättä liiketoimintakriittinen. Yritys joutuu kuitenkin turvaamaan kyseisen toiminnon jatkuvuuden yhtä huolellisesti kuin liiketoimintakriittisen toiminnon.

**Kyberturvallisuusstrategia**
Kyberturvallisuusstrategia tai kyberstrategia on ylätason suunnitelma, joka määrittää organisaation kyberturvallisuuden kehittämisen tulevaisuudet tavoitteet lähitulevaisuudessa. Kyberstrategian määrittäminen lähtee organisaation uhkamaiseman ymmärtämisestä, kyberturvallisuuden tämänhetkisen kypsyystason kartoittamisesta, halutun kypsyystason, tavoitteiden ja mittareiden määrittämisestä. Kyberstrategiaa, kuten muitakin strategioita, tulee päivittää organisaation tai uhkien muuttuessa.

**Liiketoimintakriittinen toiminto**
Liiketoimintakriittinen toiminto on yrityksen jatkuvuudelle ja liiketoiminnalle välttämätön toiminto, jota ilman yritys ei voi toimia. Esimerkiksi pääasiassa verkkokauppaa tekevälle yritykselle verkkokaupan tilausjärjestelmä on liiketoimintakriittinen toiminto.

**PCI DSS**
Payment Card Industry Data Security Standard (PCI DSS) on kansainvälinen luottokorttimaksuja koskeva tietoturvastandardi. Kaikkien luottokorttimaksuja käsittelevien yritysten tulee noudattaa PCI DSS:ää.

**Pilvipalvelu ja konesali**
Pilvipalvelu tarkoittaa palvelumallia, jossa palveluntarjoaja tarjoaa tietojenkäsittelykapasiteettia tai -palvelua, jonka tuottamisessa hyödynnetään tyypillisesti jaettuja ja skaalautuvia resursseja. Usein pilvipalveluista maksetaan käytön mukaan ja niiden käyttöönotto tai käyttäminen voi olla osin automatisoitua. Pilvipalveluista löytyy erilaisia palvelu- ja toteutusmalleja. Oleellista pilvipalveluissa on vastuun jakautuminen tilaajan ja palveluntarjoajan välillä.

**Yleisimpiä palvelumalleja ovat**
- infrastruktuuri palveluna (Infrastructure as a Service, **IaaS**),
- ohjelmistoalusta palveluna (Platform as a Service, **PaaS)** ja
- ohjelmisto palveluna (Software as a Service, **SaaS**).

IaaS-mallissa palveluntarjoaja vastaa fyysisistä palvelimista ja tilaajan vastuulle jää käyttöjärjestelmän, sovellusten ja rajapintojen toteutus ja tietoturva. IaaS on teknologian kannalta lähimpänä konesaliratkaisua, mutta tarjoaa resurssien käytön joustavuutta ilman suuria etukäteisinvestointeja.

PaaS-mallissa hankitaan käyttövalmis alustaratkaisu, esimerkiksi tietokanta- tai sovellusalusta palveluna. Vain sovelluksen ylläpito ja konfiguraatio on tilaajan vastuulla.

SaaS-mallissa hankitaan koko palvelu käyttövalmiina ja palveluntarjoaja vastaa sen tuottamista ja ylläpitämisestä. Tässä mallissa tilaajalla itsellään on vähiten ylläpidettävää, mutta myös vähiten kontrollia palveluun.

Pilvipalveluiden **toteutusmalli** voi olla julkinen pilvi, yksityinen pilvi tai hybridipilvi. **Julkinen pilvi (public cloud)** tarkoittaa kenen tahansa hankittavissa olevaa ja julkisesti tarjolla olevaa pilvipalvelua. Yksityinen pilvi (private cloud) tarkoittaa palvelua, joka tuotetaan vain tilaajaorganisaatiolle joko palveluntarjoajan tai tilaajan omasta konesalista. **Hybridipilvi (hybrid cloud)** tarkoittaa palvelua, jossa yhdistetään oma konesali julkiseen pilvipalveluun, jolloin osa toteutuksista ja tiedoista voi olla konesalissa ja osa pilvipalveluissa ja tietoliikenne kulkee näiden välillä ennalta määrättyjen sääntöjen mukaisesti.

**Oma konesali (on-prem)** tarkoittaa, että organisaatiolla on oma palvelintila ja he itse tuottavat konesalipalvelua. Vaihtoehtoisesti yrityksen omaa konesalia operoi ulkoinen palveluntuottaja, organisaatio itse operoi palveluntuottajan konesalin heille varattua osaa tai palveluntuottajalta on vuokrattu sekä konesali että sen operointi.

"Sote-tietojärjestelmät pilvipalveluina" -ohjeistus selittää vielä kattavammin eri pilvipalveluiden ja konesalien tuotanto- ja palvelumallit.

**Pilvistrategia**
Pilvistrategia on ylätason suunnitelma siitä, miten organisaatio voi hyödyntää erilaisia pilvipalveluita pidemmällä tähtäimellä. Pilvistrategian määrittäminen lähtee liiketoiminnan tarpeiden ymmärtämisestä, käytettyjen teknologioiden nykytilan kartoituksesta, toimintaympäristön rajoitusten tunnistamisesta ja ideoinnista siitä, mitä hyötyjä pilvestä voisi olla.

**Regulaatiokriittinen toiminto**
Regulaatiokriittiseen toimintoon liittyy sellainen viranomaisvelvote, jota oletuksena täytyy noudattaa myös kriisin aikana. Esimerkiksi finanssialan viranomaisraportointivelvollisuus on regulaatiokriittinen toiminto.

**Riski**
Riski on potentiaali sille, että uhkan haitalliset seuraukset toteutuvat. Riski on mitattavissa ja sitä arvioidaan usein todennäköisyyden ja aiheutuneen vahingon suuruuden avulla.

**Saatavuusalue (availability zone)**
Saatavuusalue on erillinen datakeskus tietyllä maantieteellisellä alueella (region). Pilvipalveluilla on tyypillisesti useita saatavuusalueita maailmanlaajuisesti. Useamman saatavuusalueen käyttö mahdollistaa palvelun tuottamisen myös tilanteessa, että tietyllä maantieteellisellä alueella tai tietyssä datakeskuksessa on tietoliikennehäiriöitä, sähkökatkoja tai muita saatavuusongelmia.

**Tiedon suojaus (Digital Information Protection)**
Tiedon suojaus on kattotermi prosesseille, joissa tieto luokitellaan, merkitään luokittelun mukaisesti, määritetään säännöt ja teknisiä kontrolleja tiedon jakamiselle ja käyttöoikeuksille organisaation sisällä ja ulkopuolelle, ja joissa tiedon jakamista seurataan esimerkiksi automaattihälytyksillä tai raporteilla.

**Tietojen luokittelu**
Tietojen luokittelu tarkoittaa tiedon jakamista luokkiin tiedon omistajan määrittämien kriteerien mukaisesti. Usein tiedot luokitellaan niiden luottamuksellisuuden mukaan, esimerkiksi julkiseen, yrityksen sisäiseen, luottamukselliseen ja erittäin luottamukselliseen tietoon. Luokittelussa voidaan ottaa huomioon yrityksen omat liiketoimintatarpeet ja myös asiakkaan vaatimukset tiedon käsittelylle. Jokaiselle tiedon luokalle määritellään muun muassa, miten ja missä tietoa saa käsitellä ja tallentaa, keille sitä saa jakaa ja miten kauan tietoa saa tai pitää säilyttää.

Tietojen luokittelussa voidaan ottaa huomioon luottamuksellisuuden lisäksi myös eheys- ja saatavuustarpeet. Saatavuusluokittelu on tarpeellista jatkuvuudenhallinnan kannalta.

Valtionhallinnon viranomaisten asiakirjoissa käytetään turvallisuusluokkia I-IV. Turvallisuusluokan I (merkitään TLI tai "ERITTÄIN SALAINEN") asiakirjan oikeudeton paljastuminen tai käyttö voi aiheuttaa erityisen suurta vahinkoa, kun taas turvallisuusluokan IV (merkitään TLIV tai "KÄYTTÖ RAJOITETTU") tiedon paljastuminen aiheuttaa lievää vahinkoa. Turvallisuusluokittelu on määritelty Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa.

**Tietoturva**
Tietoturva on yhdistelmä teknisiä toimenpiteitä, prosesseja ja ihmisten toimintaa, joilla varmistetaan tiedon

- **luottamuksellisuus**, eli se että tietoon pääsevät vain ne henkilöt, joilla on siihen oikeus,
- **eheys**, eli että tietoa voivat muokata vain siihen oikeutetut henkilöt,
- **saatavuus**, eli tieto on saatavilla aina kun tietoon oikeutetut henkilöt sitä tarvitsevat, ja
- **jäljitettävyys**, eli että tiedon käytöstä ja tietoon pääsystä jää jälki.

**Tietosuoja**
Tietosuoja on perusoikeus, joka turvaa henkilöiden oikeuksien ja vapauksien toteutumisen, kun henkilötietoja käsitellään. Tällaisia oikeuksia ovat mm. se, että henkilötietojen käsittely perustuu aina lakiin, henkilötietoja käsitellään vain sen verran kuin on tarpeellista ja vain niiden henkilöiden toimesta, joiden on tarpeen käsitellä tietoja. Tietosuojan ja tietoturvan välinen ero on se, että tietoturva on yksi tapa toteuttaa tietosuojaa. Tietoturvatoimenpiteet koskevat myös muiden tietojen kuin henkilötietojen turvaamista.

**Toiminnan vaikutusanalyysi**
Toiminnan vaikutusanalyysi, eli Business Impact Analysis (BIA) on menetelmä, jolla selvitetään ja kuvataan häiriöiden ja muiden haitallisten tekijöiden vaikutuksia tarkasteltavalle toiminnolle. BIA on pohjana toimintojen priorisoinnille, toimintojen riippuvuuksien tunnistamiselle ja jatkuvuussuunnittelulle yhdessä riskiarvioinnin kanssa.

**Toipumissuunnitelma**
Toipumissuunnitelma on kokoelma ohjeita ja toimenpiteitä, joilla liiketoimintaprosessi palautetaan toimintaan. Tyypillisesti jokaisella tietojärjestelmällä on oma toipumissuunnitelma.

**Uhka**
Uhka on ei-toivottu tapahtuma, jolla on haitallisia seurauksia. Esimerkiksi tietojärjestelmän haavoittuvuuden väärinkäyttö tai että myrskytuuli kaataa puun ovat uhkia.

**Varautuminen**
Varautuminen on toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön toiminta muulloinkin kuin normaalitilanteessa. Varautumistoimenpiteitä ovat esimerkiksi riskien arviointi, jatkuvuussuunnittelu, valmiussuunnittelu, kriittisten resurssien varaukset ja muut etukäteisvalmistelut.

# Liite 2: Linkkejä ja olemassa oleva ohjeistus

Tähän liitteeseen on koottu kaikki oppaan linkit ja muut huoltovarmuuteen, pilvipalveluihin ja jatkuvuudenhallintaan liittyvät aiemmin kirjoitetut suomenkieliset ohjeistukset, jotka voivat olla yrityksellesi hyödyllisiä. Jokaisesta linkistä ja dokumentissa on pyritty kertomaan tiivistelmä ja kenelle dokumentti on hyödyllistä luettavaa.

**Asiakastietolain mukaiset sosiaali- ja terveydenhuollon tietojärjestelmät**
Valvira
https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat
Asiasanat: sosiaalihuolto, terveydenhuolto, tietojärjestelmät, tietoturvavaatimukset
Tiivistelmä: Artikkelissa selitetään, mitä ovat asiakastietolain mukaiset sosiaali- ja terveydenhuollon A- ja B-luokan tietojärjestelmät, mitkä ovat tietojärjestelmäpalvelun tuottajan velvollisuudet ja mitä ovat näiden tietojärjestelmien toiminnalliset, yhteentoimivuus-, ja tietoturva-, ja tietosuojavaatimuksiin. Artikkeli on hyödyllinen sote-järjestelmien hankinnan ja uudistamisen yhteydessä.
Kenelle: sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvasta vastaavat henkilöt, tietoturva-asiantuntijat

**Business Model Canvas**
Wikipedia, 2022.
https://en.wikipedia.org/wiki/Business_Model_Canvas
Asiasanat: liiketoimintamalli, ansaintalogiikka, strategia
Tiivistelmä: Business Model Canvas on liiketoimintamallin tai ansaintalogiikan suunnitteluun tai dokumentointiin käytettävä visuaalinen työkalu. Se voi olla hyödyllinen liiketoiminta-ajureiden ja hyötyjen sanallistamiseen esimerkiksi niin uutta liiketoimintaa tai palveluja suunnitellessa kuin tietojärjestelmäuudistustenkin yhteydessä
Kenelle: Liiketoimintajohto, palvelupäälliköt, digitaalisten palveluiden suunnittelijat

**CIS Benchmarks - Center of Internet Security**
Center of Internet Security
https://www.cisecurity.org/cis-benchmarks/
Asiasanat: tietoturva, tietoturvavaatimukset, sovellusten tietoturva, valmiit ratkaisut
Tiivistelmä: CIS Benchmarks ovat maksuton kokoelma sovelluskohtaisia parhaita tietoturvakäytäntöjä. Kukin benchmark kuvaa tietyn sovelluksen tai pilvipalvelun kohdalta, miten juuri siinä pitää konkreettisesti toimia saavuttaakseen paremman tietoturvan tason.
Kenelle: Järjestelmäarkkitehdit, tietoturva-asiantuntijat, sovelluskehittäjät, tuoteomistajat

**[Huoltovarmuuskriittiset] Toimialat**
Huoltovarmuuskeskus
https://www.huoltovarmuuskeskus.fi/toimialat
Asiasanat: huoltovarmuus, yhteiskunnan elintärkeät toiminnot
Tiivistelmä: Huoltovarmuuskeskuksen toimialasivuilla on esitelty kaikki huoltovarmuuskriittiset toimialat, niiden tehtävät ja tavoitteet, toimintaa ohjaavat lait ja yhteistyömahdollisuudet. Toimialasivut ovat hyödyllisiä huoltovarmuuskriittisillä aloilla tai niiden kanssa toimiville organisaatioille.
Kenelle: huoltovarmuudesta kiinnostuneet henkilöt, huoltovarmuuskriittisillä aloilla toimivat henkilöt tai niille palveluita tuottavat henkilöt

**Informaatiovaikuttamiseen vastaaminen: Opas viestijöille**
Valtioneuvoston kanslia, 2019
http://urn.fi/URN:ISBN:978-952-287-708-6
Asiasanat: Informaatiovaikuttaminen, hybridivaikuttaminen, varautuminen, viestintä
Tiivistelmä: Ohje auttaa tunnistamaan informaatiovaikuttamisen eri tapoja, rakentamaan tietoisuutta informaatiovaikuttamisesta ja vastaamaan informaatiovaikuttamiseen, joka kohdistuu omaan yritykseen.
Kenelle: Viestintäasiantuntijat, yritysjohto

**Julkisen hallinnon pilvipalvelulinjaukset**
Valtiovarainministeriö, 2018
https://vm.fi/julkaisu?pubid=29401
Asiasanat: julkisen hallinnon ICT, pilvipalvelut
Tiivistelmä: Dokumentissa on linjauksia siitä, miten julkisen hallinnon organisaation omistamaa tietoa voidaan käsitellä pilvipalveluissa.
Kenelle: Julkishallinnon tietojärjestelmien kehittämisestä ja hankkimisesta vastaavat henkilöt

**Kansallinen riskiarvio 2018**
Sisäministeriö, 2019
http://urn.fi/URN:ISBN:978-952-324-245-6
Asiasanat: Riskiarvio, riskienhallinta, uhkamalli, häiriötilanne, yhteiskunnan elintärkeät toiminnot, huoltovarmuus
Tiivistelmä: Kansallinen riskiarvio on kooste eri toimijoiden ja hallinnonalojen uhkamalleista ja häiriötilanteista, jotka vaikuttavat yhteiskunnan elintärkeisiin toimintoihin kansallisesti. Skenaarioista on arvioitu riski ja todennäköisyyden muutostrendi. Dokumentti voi olla hyödyllinen huoltovarmuuskriittisten alojen varautumista ja jatkuvuutta suunnitteleville henkilöille.
Kenelle: huoltovarmuuskriittisten yritysten yritysjohto, ja jatkuvuudenhallinnasta ja riskienhallinnasta vastaavat henkilöt

**Katakri - tietoturvallisuuden auditointityökalu viranomaisille**
Kansallinen turvallisuusviranomainen, 2020 (versio 2020)
https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille
Asiasanat: julkisen hallinnon ICT, turvallisuuden arviointi
Tiivistelmä: Katakria voidaan käyttää auditointityökaluna arvioitaessa yrityksen turvallisuusjärjestelyjä yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Se on hyödyllistä luettavaa viranomaisten käyttöön tarkoitettujen tietojärjestelmien suunnittelussa, kehityksessä ja tietoturvan arvioinnissa.
Kenelle: tietoturva-asiantuntijat, asiantuntijat, joiden tehtäviin kuuluu julkishallinnon sähköisten palveluiden suunnittelu, hankinta, toteuttaminen, kehittäminen ja ylläpito

**Kriittisten kohteiden luokittelu. VAHTI-hyvät käytännöt tukimateriaali**
Digi- ja väestötietovirasto, 2022
https://dvv.fi/documents/16079645/110183105/Kriittisten+kohteiden+luokittelun+menetelm%C3%A4kuvaus.pdf
Asiasanat: Kriittisyysluokittelu, vaikutusten arviointi
Tiivistelmä: Dokumentti auttaa tunnistamaan organisaation suojattavat kohteet ja arvioimaan niiden kriittisyyttä. Ohje on hyödyllistä luettavaa, kun on tarve luokitella yrityksen kriittisiä toimintoja ja tietoja.
Kenelle: Jatkuvuudenhallinnasta vastaavat henkilöt

**Kyberharjoituksen skenaariopankki**
Kyberturvallisuuskeskus (Traficom), 2020–2022
https://www.kyberturvallisuuskeskus.fi/fi/s/kyberharjoitusskenaariot/skenaariot
Asiasanat: Kyberturvallisuus, jatkuvuudenhallinta, kyberharjoitus, häiriönhallinta, tietoturvapoikkeamanhallinta
Tiivistelmä: Kyberharjoituksen skenaariopankki sisältää tosielämän tietoturvapoikkeamiin ja häiriöihin perustuvia tapauksia. Skenaariot ovat hyödyllistä luettavaa poikkeamanhallintaharjoitusten suunnittelijoille ja jatkuvuussuunnitelmien ja tietoturvapoikkeamien käsittelyohjeiden päivittämisen tueksi.
Kenelle: Tietoturva-asiantuntijat, jatkuvuudenhallinnasta vastaavat henkilöt

**Kyberharjoitusohje - Käsikirja harjoituksen järjestäjälle**
Kyberturvallisuuskeskus (Traficom), 2022
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/kyberharjoitusohje-kasikirja-harjoituksen-jarjestajalle
Asiasanat: Kyberturvallisuus, jatkuvuudenhallinta, kyberharjoitus, häiriönhallinta, tietoturvapoikkeamanhallinta
Tiivistelmä: Kyberharjoitusohjeessa esitellään erilaisia harjoitustyyppejä ja annetaan käytännönläheisiä ohjeita harjoituksen suunnitteluun ja järjestämiseen. Ohje on hyödyllistä luettavaa kyberharjoittelusta kiinnostuneille tai harjoituksia tilaaville henkilöille ja harjoitusten suunnittelijoille.
Kenelle: Tietoturva-asiantuntijat, jatkuvuudenhallinnasta vastaavat henkilöt, tietoturvapoikkeamien hallinnasta vastaavat henkilöt

**Kybersää**
Kyberturvallisuuskeskus (Traficom)
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa
Asiasanat: Kyberturvallisuus, tietoturva, tietoturvailmiö, tietoturvapoikkeama
Tiivistelmä: Kybersää on kuukausittain julkaistu yleistajuinen kooste kuluneen kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Kybersää antaa yleiskuvan tietoturvan tilasta ja tapahtumista ja auttaa suunnittelemaan mm. varautumista ja tietoturvatietoiskuja.
Kenelle: Tietoturvasta vastaavat henkilöt, yritysjohto, tietoturvasta kiinnostuneet henkilöt

**Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille**
Kyberturvallisuuskeskus (Traficom), 2019
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohjeita-pilvipalvelujen-turvallisuudesta-yksityishenkiloille-pien-yhteisoille-ja
Asiasanat: julkisen hallinnon ICT, turvallisuuden arviointi, pilvipalvelut
Tiivistelmä: Ohje käsittelee yleisimpiä tietoturvallisuusnäkökulmia, joita yksityishenkilöiden, pienyhteisöjen ja pienyritysten kannattaa huomioida pilvipalveluiden käyttöönottoa huomioidessa. Ohje on yksityiskohtaisempi kuin PiTuKri ja viittaa sen vaatimuksiin.
Kenelle: tietoturva-asiantuntijat, asiantuntijat, joiden tehtäviin kuuluu julkishallinnon sähköisten palveluiden suunnittelu, hankinta, toteuttaminen, kehittäminen ja ylläpito

**OWASP Top 10**
Open Web Application Security Project (OWASP)
https://owasp.org/www-project-top-ten/
Asiasanat: tietoturvatestaus, web-sovellusten tietoturva, tietoturvavaatimukset
Tiivistelmä: OWASP Top 10 listaa kymmenen suurinta sovelluksen tietoturvauhkaa ja miten ohjelmistoa tuottaessa niiltä voidaan välttyä. Lista on laajalti käytössä oleva ja sen täyttämistä jokaisessa ohjelmistoprojektissa pidetään minimivaatimuksena.
Kenelle: sovelluskehittäjät, tuoteomistajat, tietoturva-asiantuntijat, järjestelmäarkkitehdit

**Pilvipalveluiden juridinen selvitys**
FiCom, 2023. (Löydät Huoltovarmuuskeskuksen sivuilta.)
Asiasanat: pilvipalvelut, lainsäädäntö, sääntely, GDPR, henkilötietojen käsittely
Tiivistelmä: Juridinen selvitys ja tiivistelmä siitä miten kansalliset ja kansainväliset lait sekä tiettyjen alojen erityissääntely vaikuttaa pilvipalveluiden käyttämiseen.

**Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri),**
Kyberturvallisuuskeskus (Traficom), 2019 (versio 1.1)
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri
Asiasanat: pilven tietoturva, julkisen hallinnon ICT, pilvipalvelut, turvallisuuden arviointi
Tiivistelmä: Pilvipalveluiden turvallisuuden arviointikriteeristö toimii työkaluna pilvipalveluiden turvallisuuden arviointiin erityisesti, kun käsitellään viranomaisten salassa pidettävää tai turvallisuusluokiteltua tietoa. Kriteeristöä voidaan käyttää myös yritysten tarpeisiin. Ohjeessa selitetään myös kattavasti tietoturvan vastuunjako erilaisissa pilvipalveluiden palvelumalleissa.
Kenelle: tietoturva-asiantuntijat, asiantuntijat, joiden tehtäviin kuuluu julkishallinnon sähköisten palveluiden suunnittelu, hankinta, toteuttaminen, kehittäminen ja ylläpito

**Pilvipalvelujen soveltamisohje - Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille**
Valtiovarainministeriö, 2020
http://urn.fi/URN:ISBN:978-952-367-503-2
Asiasanat: Julkisen hallinnon ICT, pilvipalvelut, soveltamisohjeet, julkinen hallinto, elinkaari
Tiivistelmä: Dokumentti on jatko-osa "Tuottavuutta pilvipalveluilla" -dokumentille. Ohjeessa esitellään pilvipalveluiden elinkaaren eri vaiheet ja mitä keskeisiä tehtäviä niihin liittyy. Ohjeessa ja sen useissa liitteissä annetaan julkisen hallinnon organisaatioille ohjeita, malleja ja valmiita pohjia pilvipalveluiden turvalliseen käyttöön.
Kenelle: (julkisen hallinnon) päätöksentekijät, asiantuntijat, joiden tehtäviin kuuluu sähköisten palveluiden suunnittelu, hankinta, toteuttaminen, kehittäminen ja ylläpito

**Sote-tietojärjestelmät pilvipalveluina**
Kuntaliitto & Akusti-foorumi, 2022
https://www.kuntaliitto.fi/julkaisut/2022/2158-sote-tietojarjestelmat-pilvipalveluina
Asiasanat: terveydenhuolto, sosiaalihuolto, tietojärjestelmät, tietosuoja, pilvipalvelut
Tiivistelmä: Suositeltavaa luettavaa jokaiselle yritykselle toimialaan riippumatta, joka hyödyntää tai harkitsee hyödyntävänsä pilvipalveluita. Opas käy yksityiskohtaisesti läpi kaikki ne lait, määräykset ja puolet, joita pilvipalveluiden hyödyntämisessä pitää pohtia, etenkin kriittisten toimintojen osalta.
Kenelle: Tiedonhallinnan ja -käsittelyn asiantuntijat, organisaatioiden pilvilinjauksista päättävät, pilvipalveluiden ja teknologian hankinnasta vastaavat henkilöt

**The Ultimate Beginner's Guide to Threat Modeling**
Shostack + Associates
https://shostack.org/resources/threat-modeling
Asiasanat: uhkamallinnus, uhka-analyysi, threat modeling, threat analysis
Tiivistelmä: Artikkeli taustoittaa, mitä uhkamallinnus on, miten se eroaa riskienhallinnasta, millaisia uhkamallinnusmenetelmiä on olemassa ja missä tilanteissa uhkamallinnusta kannattaa käyttää. Artikkeli on hyödyllistä luettavaa tietojärjestelmien hankinnan, kehityksen ja uudistuksen yhteydessä.
Kenelle: tietoturva-asiantuntijat, tietoturvasta vastaavat henkilöt, tietohallinto, ohjelmistokehittäjät, ohjelmistotestaajat, tuoteomistajat

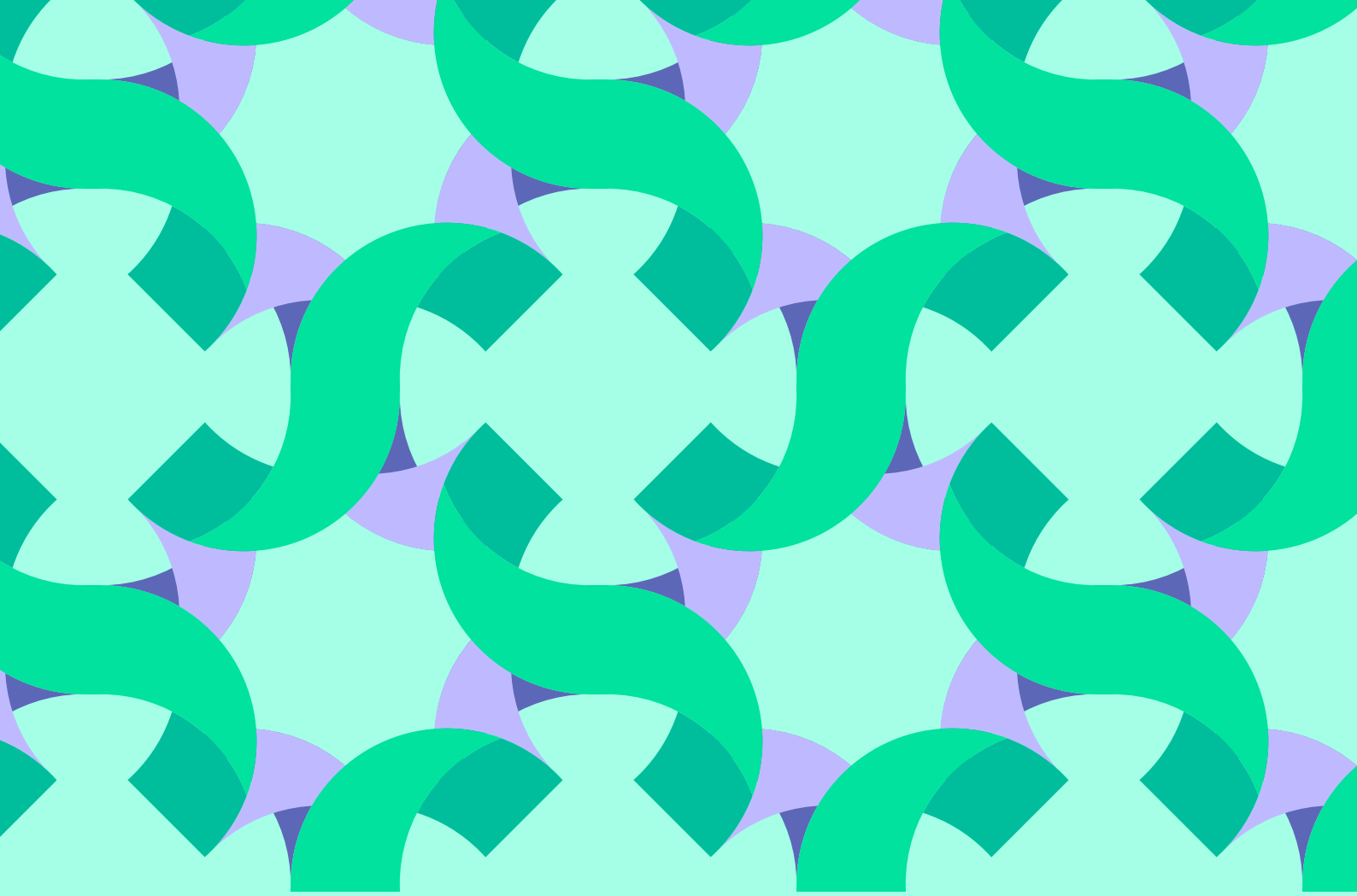
**Tietoturvan vuosi 2021. Kyberturvallisuus elää kasvun aikaa – torjumme häiriöitä ennakolta. Kyberturvallisuuskeskuksen vuosikatsaus.**
Kyberturvallisuuskeskus (Traficom), 2022.
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2021.pdf
Asiasanat: Kyberturvallisuus, tietoturva, Kyberturvallisuuskeskus
Tiivistelmä: Vuosikatsaus kertoo Kyberturvallisuuskeskuksen toiminnasta, summaa vuoden 2021 tärkeimmät tietoturvailmiöt ja tapahtumat ja ennustaa tietoturvan trendejä vuodelle 2021.
Kenelle: Tietoturvasta kiinnostuneet henkilöt

**Tuottavuutta pilvipalveluilla: Ohje julkisen hallinnon pilvipalvelujen hyödyntämiseen**
Valtionvarainministeriö, 2020
http://urn.fi/URN:ISBN:978-952-367-327-4
Asiasanat: julkisen hallinnon ICT, pilvipalvelut, soveltamisohjeet, julkinen hallinto
Tiivistelmä: Tässä ohjeessa kuvataan keskeisiä periaatteita julkisen pilven käyttöön ja edistämiseen valtionhallinnossa ja julkisella sektorilla. Lisäksi kuvataan seikkoja, joita tulee arvioida, kun suunnitellaan uusia pilvipalveluihin perustuvia ratkaisuja. Ohje on hyödyllistä luettavaa sekä julkishallinnossa että yritysmaailmassa toimiville henkilöille, jotka harkitsevat pilvipalveluiden käyttöönottoa.
Kenelle: (Julkisen hallinnon) ylin johto, tietohallintojohto, ICT-asiantuntijat, tietojärjestelmäarkkitehdit, hankinta-asiantuntijat

**Use of cloud-based service by the public sector. 2022 Coordinated Enforcement Action**
Euroopan Tietosuojaneuvosto, 2023.
https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf
Asiasanat: Tietosuoja, henkilötietojen käsittely, GDPR
Tiivistelmä: Lausunto käy läpi, miten julkishallinnossa pilvipalveluiden käyttöä henkilötietojen käsittelyssä ja mitä puutteita tässä toiminnassa on ollut. Lausunto avaa tarkemmin millä tavalla henkilötietoja pitäisi käsitellä GDPR:n ja EU:n vaateiden mukaisesti.
Kenelle: Tietosuoja-asiantuntijat

**VAHTI 2/2016 Toiminnan jatkuvuuden hallinta**
Valtiovarainministeriö, 2016.
https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22016-toiminnan-jatkuvuuden-hallinta
Asiasanat: Jatkuvuudenhallinta, jatkuvuussuunnittelu, varautuminen, toipumissuunnittelu, valmiussuunnittelu
Tiivistelmä: Ohje taustoittaa jatkuvuussuunnittelun peruskäsitteet ja miten jatkuvuudenhallintaa kehitetään. Ohje on hyödyllistä luettavaa sekä julkishallinnossa että yritysmaailmassa toimiville henkilöille, joiden tehtäviin kuuluu jatkuvuudenhallinnan suunnittelu ja häiriötilanteissa toimiminen tai viestiminen.
Kenelle: Jatkuvuudenhallinnasta vastaavat henkilöt, yritysjohto

**VAHTI 22/2017 Ohje riskienhallintaan**
Valtiovarainministeriö, 2017
https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-222017-ohje-riskienhallintaan
Asiasanat: Riskienhallinta
Tiivistelmä: Ohje antaa suosituksia varautumis-, jatkuvuus-, toipumis-, ja valmiussuunnitteluun.
Kenelle: Riskienhallinnasta vastaavat henkilöt



Huoltovarmuusorganisaatio