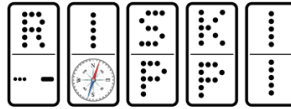




Vipuvoimaa
EU:lta
2014–2020



Vaasan yliopisto
UNIVERSITY OF VAASA

Hanke rahoitetaan Euroopan sosiaalirahaston REACT-EU tuella.
REACT-EU-hankkeet rahoitetaan osana Euroopan unionin COVID-19-pandemian johdosta toteuttamia toimia.

Moduuli 2: Riskienhallinta elinkaariajattelussa ja jatkuvuuden hallinnassa



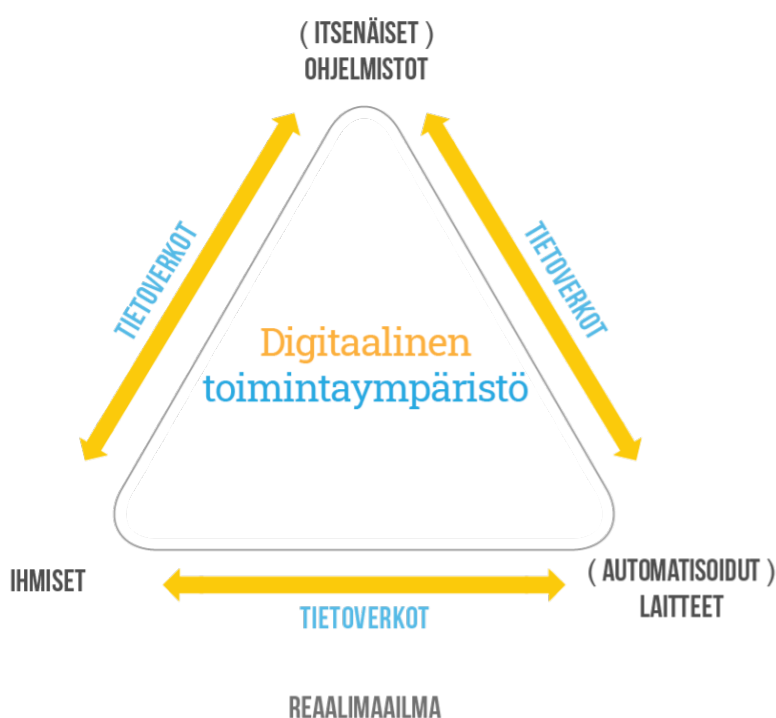
Johdanto: Digiturvallisuuden kokonaisuus

Oppimistavoite: Tässä kappaleessa opit viisi painopistettä, jotka ovat keskeisiä digiturvallisuuden toteutusalueita. Riskioppi-ympäristön kolme moduulia ovat oppimisaineistojen kokonaisuus, jonka avulla opitaan toteuttamaan digiturvallisuutta. Kappaleen lopussa vastaat ”yhdistä parit”-tehtävään liittyen digiturvallisuuden toteutusalueisiin ja niitä vastaaviin esimerkkitalanteisiin. Arvioitu ajankäyttö: 15 min.

Moduulissa 1 opit digiriskien hallinnan periaatteita. Riskienhallinta on ensimmäinen tärkeä askel, jotta voit saavuttaa toiminnan tavoitteesi digitaalisessa toimintaympäristössä. Moduuleissa 2 ja 3 opit, miten voit varmistaa toiminnan **digitaalisen turvallisuuden** kokonaisuutena.

VAHTI-riskienhallintasanaston määritelmän mukaan digiturvallisuus koskee muutakin kuin varsinaista digitaalista toiminta-aluetta. Se koskee myös reaali maailmaa sekä merkitysrakenteita, kuten luottamusta, politiikkaa ja vapaa-aikaa. Sanastossa digitaalinen turvallisuus eli digiturvallisuus määritellään kattokäsitteeksi, johon liittyvät kaikki sellaiset tekijät, jotka vaikuttavat digitaaliseen toimintaympäristön turvallisuuteen. Nämä eri tekijät voivat joko vahvistaa tai heikentää digitaalista turvallisuutta. Näiden digitaalisen toimintaympäristön turvallisuuteen vaikuttavien tekijöiden lisäksi digiturvallisuuteen liittyvät myös toisen suuntaiset vaikutukset eli kaikki ne tekijät, joihin digitaalinen toimintaympäristö voi vaikuttaa turvallisuuden näkökulmasta. (VAHTI s. 69)

Erityisesti jälkimmäinen näkökulma on tärkeä, sillä digitaalinen toimintaympäristö ei ole selkeästi rajattu, ja sen häiriöillä voi olla vaikutuksia myös fyysisessä maailmassa ja toisin päin. Tämä korostaa digiturvallisuuden kokonaisvaltaista merkitystä, sillä yksittäiset toimet digitaalisessa ympäristössä voivat vaikuttaa laajasti. Tätä asiaa on havainnollistettu alla Moduulista 1 tutulla kuvalla, jossa digiympäristö on määritelty.



Digitaalinen toimintaympäristö. Kuvan lisenssi: CC by KOMPASSI-hanke.

Asia voidaan ilmaista niin, että digitaalisen ympäristön riskit vaikuttavat myös fyysisessä maailmassa, jos ne toteutuvat. Digiympäristön kautta ohjataan usein laitteita ja järjestelmiä, jotka ovat osa fyysistä ympäristöämme, ja näiden laitteiden ja järjestelmien häiriöillä voi olla vakavia seurauksia ihmisten turvallisuuden tai ympäristön kannalta. Lisäksi digitaalisessa toimintaympäristössä toimiminen vaikuttaa ihmisten tietoon ja mielipiteisiin, ja tieto ja mielipiteet puolestaan vaikuttavat ihmisten toimintaan fyysisessä maailmassa. Disinformaatio eli väärä tieto, jolla pyritään tarkoituksella vaikuttamaan ihmisiin, voi olla uhka sekä digitaalisen toimintaympäristön että fyysisen maailman turvallisuudelle.

On tärkeää lähteä rakentamaan digiturvallisuutta kokonaisvaltaisesti. Tarvittavat taidot tähän saat Riskioppi-ympäristön moduuleista 1, 2 ja 3.

Digiturvallisuuden viisi toteutusalueetta

VAHTI-sanaston mukaan **digiturvallisuuden** keskeisiksi toteutusalueiksi on julkisen hallinnon ohjauksessa valittu **viisi painopistettä**. Nämä toteutusalueet muodostavat kokonaisuuden, joka yhdistää kaikki digiympäristön toimijat siten, että toimijat voivat yhdessä tuottaa toiminnallaan hallittua digiturvallisuutta. (VAHTI s. 69–70)

Kokonaisuus pohjautuu [Valtionvarainministeriön periaatepäätökseen digitaalisen turvallisuuden viitekehyksestä](#) (Valtiovarainministeriö 2020). Sen mukaan nämä viisi toteutusalueetta muodostavat välttämättömän kokonaisuuden, joka auttaa kohtaamaan erityyppisiä haasteita digiympäristössä (kts. VAHTI s. 70). Kattavuutensa ansiosta toteutusalueiden kokonaisuutta voidaan hyödyntää muuallakin julkisen hallinnon ulkopuolella.

Digiturvallisuuden toteutusalueet ovat seuraavat (VAHTI s. 70):

- **Johtaminen ja riskienhallinta**, joka kokoaa eri osa-alueet hallittavaksi kokonaisuudeksi.
- **Jatkuvuudenhallinta**, jolla varaudutaan ennakolta erilaisiin häiriöihin ja pyritään turvaamaan toiminnan jatkuvuus häiriöistä huolimatta.
- **Kyberturvallisuus**, jonka kautta tarkastellaan laajoja ilmiöitä verkottuneessa ympäristössä ja pyritään tunnistamaan häiriöiden monimutkaisia vaikutuksia digiympäristön ja fyysisen maailman välillä.
- **Tietoturvallisuus**, joka kohdistuu tietojen luottamuksellisuuteen, saatavuuteen ja eheyteen, sekä tiedon käyttövaltuuksien hallitsemiseen ja tiedon kiistämättömyyden todentamiseen.
- **Tietosuoja**, joka on omien ja toisten ihmisten yksityisyydensuojaa ja tietojen hallintaa.

Kokonaisuus on esitetty alla olevassa kuvassa. Kuten kuvasta ilmenee, on näillä viidellä toteutusalueella kaksi ulottuvuutta, digitaalinen toimintaympäristö ja muut toimintaympäristöt, joihin sisältyy myös fyysinen maailma.



Digiturvallisuuden viisi toteutusalueutta ja miten niitä käsitellään Riskioppi-ympäristön moduuleissa. Kuvaan on sovellettu lähdettä VAHTI s. 69.

Riskioppi-ympäristön aineiston rakenne noudattaa tätä digiturvallisuuden kokonaisuutta, johon kuuluu viisi painopistettä. Riskioppi-ympäristön Moduulissa 1 käytiin läpi ensimmäinen painopiste eli riskienhallinnan periaatteet digitaalisessa toimintaympäristössä. Käsillä olevat Moduulit 2 ja 3 tarjoavat oppimisaineistoa, joka täydentää digitaalisen turvallisuuden kokonaisuuden osaamista.

Moduulissa 2 käsittelemme riskienhallintaa jatkuvuudenhallinnan näkökulmasta.

Jatkuvuudenhallinnalla varaudutaan ennakolta häiriöihin ja toiminnan jatkuvuuden turvaamiseen ja rakennetaan näin digiturvallisuutta.

Moduulissa 2 käytetään konkreettisenä välineenä ISO 22301 -standardia. Moduulin 2 lopussa käydään läpi myös elinkaariajattelua sekä sen roolia digiriskien hallinnassa ja kokonaisturvallisuuden rakentamisessa.

Moduulissa 3 perehdytään siihen, miten digiturvallisuutta voidaan rakentaa käyttämällä kyberturvallisuutta, tietosuoja ja tietoturva riskienhallinnan tukena. Moduulissa käsitellään kyberturvallisuutta, tietosuoja ja tietoturva riskienhallinnan näkökulmasta. Kyberturvallisuus koskettaa jokaista, sillä jokaisen omalla toiminnalla on verkottuneessa digiympäristössä potentiaalisesti vaikutusta kaikkiin muihin toimijoihin. Tietosuoja ja tietoturva ovat tärkeitä, sillä jo laki edellyttää tietosuoja, ja tietoturva puolestaan luo pohjan toiminnalle digiympäristössä. Moduulissa käsitellään sitä, miten tällainen riskienhallinta täydentää digitaalista turvallisuutta. Konkreettiseksi välineeksi otetaan **ISO 27001** -standardin vaatimukset tietoturvalle ja **TARAJÄRJESTELMÄ**, jolla ennakoidaan uhkia digiympäristössä.

Moduulien 2 ja 3 aineistot esitetään rinnakkain tavalla, joka tukee niiden keskinäistä yhteyttä. Voit tutustua materiaaleihin kahdella tavalla: Ensimmäinen tapa on käydä läpi kummankin moduulin kappaleet peräkkäin niiden numeroiden mukaisessa järjestyksessä. Toinen tapa on opiskella kunkin moduulin vastaavien kappaleiden sisältöjä peräkkäin eli esimerkiksi tarkastella kappaleiden 2.1 ja 3.1 sisältöjä rinnakkain.

Intoa uuden oppimiseen digiturvallisuuden rakentamiseksi!



Alla vasemmalla näet listan digiturvallisuuden keskeisistä toteutusalueista. Alla oikealla on muutamia esimerkkitilanteita. **Yhdistä kukin toteutusalue sitä parhaiten kuvaavaan esimerkkitilanteeseen.**

Johtaminen ja riskienhallinta	Yrityksen asiakastietokantaan on päässyt murtautumaan ulkopuolinen henkilö.
Jatkuvuudenhallinta	Työntekijä on lähettänyt vahingossa sähköpostin, joka sisältää henkilötietoja asiakkaista.
Kyberturvallisuus	Yrityksen tärkeät asiakirjat ovat joutuneet väärin käsiin, ja ne sisältävät arkaluontoista tietoa.
Tietoturvallisuus	Yrityksen tietojärjestelmä on kaatunut, ja työntekijät eivät pääse käyttämään tietokonettaan.
Tietosuoja	Yrityksen verkkosivustolle on hyökätty ja sen kautta on jaettu haittaohjelmia asiakkaille.

Pohdi edellisen tehtävän esimerkkitalannetta ja yhdistä esimerkkitalanne oikeaan ratkaisuun.

Yrityksen tärkeät asiakirjat ovat joutuneet väärin käsiin, ja ne sisältävät arkaluontoista tietoa.	Yrityksen tietoturva-asiantuntijat tutkivat syitä ja tekevät muutoksia järjestelmiin, jotta hyökkäyksiltä vältytään tulevaisuudessa.
Yrityksen tietojärjestelmä on kaatunut, ja työntekijät eivät pääse käyttämään tietokonettaan.	Yrityksen johto laatii toimintasuunnitelman, jonka avulla varmistetaan, että vastaavanlaiset tietovuodot eivät toistu.
Yrityksen verkkosivustolle on hyökätty ja sen kautta on jaettu haittaohjelmia asiakkaille.	Yrityksen tietosuojavastaava selvittää mitä on tapahtunut ja miten, sekä ryhtyy toimenpiteisiin tietojen suojaamiseksi.
Yrityksen asiakastietokantaan on päässyt murtautumaan ulkopuolinen henkilö.	Yrityksen tietoturva-asiantuntijat selvittävät, miten tietokantaan on päästy murtautumaan, ja tekevät muutoksia järjestelmiin.
Työntekijä on lähettänyt vahingossa sähköpostin, joka sisältää henkilötietoja asiakkaista.	Yrityksellä on varasuunnitelma, jonka avulla se voi jatkaa toimintaansa myös tietojärjestelmän kaatumisen sattuessa.

2.1 Jatkuvuudenhallinta täydentää riskienhallintaa

Oppimistavoite: Tässä kappaleessa opit, miten täydennät toimintasi riskienhallintaa jatkuvuudenhallinnalla. Kappaleessa keskitytään jatkuvuudenhallintaan digiympäristössä. Konkreettisenä välineenä esitellään VAHTI 2/2016 -suunnitteluprosessi. Kappaleen lopussa vastaat valintatehtäviin liittyen jatkuvuudenhallinnan haasteisiin yrityksissä. Arvioitu ajankäyttö: 30 min.

Riski kuvaa epävarmojen ja ei-toivottujen tapahtumien vaikutusta toiminnan tavoitteisiin. Riskienhallinnan tavoitteena on tukea sitä, että organisaatio voi saavuttaa toimintansa tavoitteet. Jatkuvuudenhallinnan tarkoitus puolestaan on varautua hallitsemaan organisaation toimintaa häiritseviä tilanteita siten, että toiminta voi jatkua hyväksyttävällä tavalla häiriöistä huolimatta (JOHDA s. 219). Erityisesti liiketoiminnan jatkuvuuden hallintaan viitataan termillä **business continuity management (BCM)**.

Riski kuvaa epävarmuuden vaikutusta tavoitteisiin. Jatkuvuudenhallintaan liittyvä **jatkuvuussuunnittelu** tarkoittaa sellaisten toimenpiteiden laatimista, joilla pyritään

vähentämään toimintaa haittaavien epävarmojen tapahtumien vaikutusta tai lyhentämään tällaisten tapahtumien eli häiriöiden kestoja. Kun jatkuvuussuunnittelua tarkastellaan riskienhallinnan näkökulmasta, sillä siis pyritään minimoimaan riskienvaikutusta toiminnan tavoitteisiin.

Liiketoiminnan jatkuvuussuunnittelu on kokonaisvaltainen prosessi. Sen avulla voidaan tunnistaa niitä tekijöitä, jotka uhkaavat organisaatiota, ja ennakoida näiden tekijöiden seurauksia. Jatkuvuussuunnittelulla luodaan perusta organisaation toipumiskyvylle ja vastatoimenpiteille. Vastatoimet turvaavat organisaatiota itseään, sen mainetta, brändiä, sidosryhmiä ja lisäarvoa tuottavia toimintoja. ([Lähtäpöytä: Keskeytysriskit ja jatkuvuussuunnittelu](#))

Jatkuvuudenhallinnalla siis luodaan toimintatavat häiriötilanteita varten. Jatkuvuudenhallinta on yleensä omaehtoista toimintaa, mutta joillakin aloilla laki velvoittaa organisaatioita varmistamaan toimintansa jatkuvuuden erilaisissa olosuhteissa.

Sekä jatkuvuudenhallinnan että riskienhallinnan avulla siis käsitellään toimintaan vaikuttavia uhkia ja suunnitellaan etukäteen, miten niihin varaudutaan. Seuraavassa käydään läpi jatkuvuudenhallinnan toteuttamisen periaatteet ja aiheeseen liittyvät keskeiset käsitteet.

Häiriöt ja poikkeamat

Jatkuvuudenhallinnalla siis valmistaudutaan varmistamaan, että organisaation toiminta voi jatkua mahdollisten häiriöiden ja poikkeamien aikana.

Häiriö on odotettu tai odottamaton tilanne, joka aiheuttaa suunnittele mattoman **negatiivisen poikkeaman organisaation tavoitteiden mukaisessa toiminnassa** (ISO 22301).

Puhutaan myös **häiriötilanteesta**. Häiriötilanteita varten luodaan toimintaohjeet. Jotta toiminnan keskeyttävästä häiriöstä voidaan palautua tehokkaasti ja nopeasti, laaditaan erilaisia häiriötilanteita varten **toipumissuunnitelmia, jotka voivat olla yleisiä tai toimintokohtaisia**. Organisaatiossa on oltava vähintään **kriisi-, jatkuvuus- ja toipumissuunnitelmat**, jotta mahdollisiin häiriöihin voidaan varautua.

- Käsitteellä **major incident management (MIM)** tarkoitetaan vakavan häiriötilanteen hallintaprosessia. Tällainen vakava häiriö voi johtaa organisaation toimintakyvyn merkittävään alenemiseen tai jopa toiminnan täydelliseen keskeytymiseen.

Poikkeama on tapaus, jossa asiat eivät etene suunnitellusti tai odotetulla tavalla, ja se voi **johtaa kielteisiin seuraksiin**, jollaisia ovat esimerkiksi (JOHDA s. 222)

- henkilövahinko tai ammattitauti
- päästö ympäristöön
- tulipalo, liikennevahinko tai näihin liittyvä omaisuusvahinko
- tuotantomenetys esimerkiksi käyntihäiriön vuoksi.

Onnettomuustilanteissa keskeinen ohje on organisaation **pelastussuunnitelma**.

Häiriöitä ja poikkeamia voi ilmetä fyysisessä maailmassa, digiympäristössä tai molemmissa. Häiriö ja poikkeama voivat koskea organisaatiota itseään tai toimittajaverkostoa, johon se kuuluu. Lisäksi häiriö voi koskea koko organisaatiota ympäröivää yhteiskuntaa.

Poikkeamiin reagointi tapahtuu siten, että häiriötilanteessa aktivoidaan ja toimeenpannaan jatkuvuussuunnitelma.

Vaatimukset

Jatkuvuussuunnitteluun liittyy viranomaisvaatimuksia ja valvontaa, jotka koskevat pääosin etenkin poikkeusoloihin varautumista ja huoltovarmuutta. Monia huoltovarmuuskriittisten alojen yrityksiä velvoittaa valmiuslaki. Valmiuslaissa säädetään poikkeusoloihin varautumisesta. Valtakunnan huoltovarmuuden kehittämistä ja ylläpitoa varten toimii Huoltovarmuuskeskus.

Lisäksi finanssivalvonnassa on määräyksiä jatkuvuussuunnittelun järjestämisestä.

Jatkuvuudenhallintaprosessi

Jatkuvuudenhallintaan sisältyy kolme osaa: valmiussuunnittelu, varautuminen ja jatkuvuudenhallintaprosessi.

1) **Valmiussuunnittelu** on suunnittelua, jota tehdään normaaliolojen aikana häiriötilanteiden varalle.

2) **Varautuminen**, jolla varmistetaan, että häiriötilanteissa pystytään hoitamaan tehtävät ja suorittamaan mahdollisesti tarvittavat poikkeukselliset toimenpiteet.

- Varautuminen jakaantuu suunnitteluun, sen edellyttämiin käytännön valmistelutoimenpiteisiin sekä näiden valmistelutoimenpiteiden toteuttamiseen, harjoitteluun ja edelleen kehittämiseen.
- Varautumistoimenpiteitä ovat esimerkiksi riskien arviointi, jatkuvuus- ja valmiussuunnittelu, järjestelmien tekniset ja rakenteelliset valmistelut, henkilöstön koulutus ja harjoittelut, fyysisten tilojen valmistelut sekä kriittisten resurssien varaukset.

3) **Jatkuvuudenhallintaprosessi**, jonka aikana yritys, järjestö, julkinen toimija tai muu organisaatio (JOHDA s. 219)

- **tunnistaa toimintaansa kohdistuvat uhkat**, esimerkiksi häiriötilanteet ja toimintojen riippuvuudet, sekä riskit, kuten jatkuvuusriskit
- **ennakoi ja arvioi tunnistettujen uhkien vaikutukset** organisaatiolle ja sen toimijaverkostolle, erityisesti kriittisille kumppaneille
- **luo toimintatavan häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa** sekä varmistaa kriittisten kumppaneidensa kyvyn toimia häiriötilanteissa

- **suojaa** arvontuottamisen toimenpiteet, organisaation maineen ja brändin sekä sidosryhmien intressit.

Jatkuvuudenhallintaohjelma

Jatkuvuudenhallintaohjelma on ensinnäkin **prosessi**, jolla organisaatio varmistaa johdon tukemana, että jatkuvuudenhallinnan toimenpiteet voivat toteutua.

Lisäksi jatkuvuudenhallintaohjelma on **dokumentti**, johon toimenpiteet kirjataan.

Jatkuvuudenhallintaohjelmalla ylläpidetään organisaation jatkuvuussuunnitelmaa ja -strategiaa. (JOHDA s. 219)

Jatkuvuussuunnitelma on paitsi dokumentoitava ja osallisille jaettava suunnitelma, myös työväline ja testaustyökalu. **Jatkuvuusstrategia** on pidemmän aikavälin suunnitelma.

Jatkuvuudenhallintaohjelmalla varmistetaan, että organisaation toiminnot, tuotantoprosessit ja palvelut **testataan, koulutetaan** ja niitä **harjoitellaan** jatkuvuudenhallinnan näkökulmasta (JOHDA s. 219). Koulutuksella ja harjoittelulla saavutetaan organisaatiossa pätevyys jatkuvuudenhallinnalle.

Jatkuvuudenhallintaohjelmaan sisältyy myös seuranta siitä, että organisaatio on huolehtinut riittävästä **vakuutuksista** (JOHDA s. 219).

Jatkuvuussuunnittelu

Jatkuvuussuunnittelu on järjestelmällistä varautumista häiriöihin. Jatkuvuussuunnitteluun sisältyy suunnitteluprosessi, jossa kehitetään menettelytapoja häiriötilanteita varten. Näillä menettelytavoilla varmistetaan, että organisaatio pystyy jatkamaan toimintaansa ja rajoittamaan tappioita häiriötilanteissa. Jatkuvuussuunnittelulla varaudutaan näin liiketoiminnan mahdollisiin keskeytyksiin ja palauttamaan toiminta normaalille tasolle hallitusti häiriön jälkeen. (JOHDA s. 220)

Jatkuvuussuunnitteluun sisältyy myös organisaation kriittisten liiketoimintatoimintojen ja niitä tukevien resurssien tunnistaminen. Jatkuvuussuunnittelun avulla luodaan **toimintasuunnitelma** sellaisten tilanteiden varalta, jotka uhkaavat organisaation olemassaoloa.

Jatkuvuussuunnittelussa tunnistetaan erilaiset häiriötilanteet ja niiden vaikutukset organisaation toimintaan. Näiden tietojen perusteella laaditaan jatkuvuussuunnitelmat, joissa on ohjeet siihen, miten tärkeimpien toimien jatkuminen turvataan häiriötilanteessa. Jatkuvuussuunnitteluun kuuluu myös suunnitelmien testaus ja harjoittelu sekä tarvittavan koulutuksen järjestäminen henkilöstölle. (JOHDA s. 220)

VAHTI 2/2016 -ohjeistuksessa kuvataan jatkuvuussuunnittelun prosessi. Prosessi sisältää kahdeksan vaiheittain toteutettavaa osa-aluetta. Ohjeistuksessa esitellään myös alla oleva kuva, joka havainnollistaa tätä prosessia.



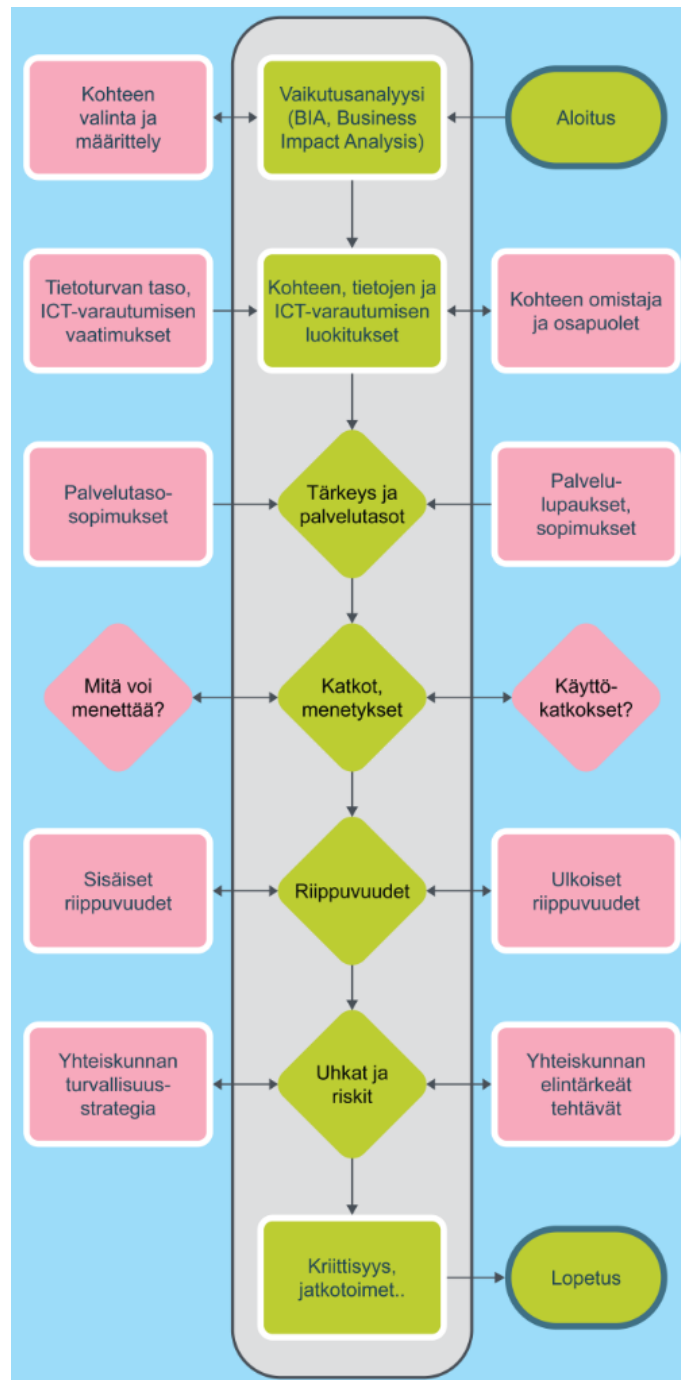
VAHTI 2/2016 -ohjeistuksen mukainen jatkuvuussuunnittelun prosessi käsittää kahdeksan vaiheittain toteutettavaa osaluuetta (Valtiovarainministeriö 2016 s. 41).

Vaiheiden keskeinen sisältö on seuraava:

1. Yleensä prosessi aloitetaan **toimintaympäristö- ja riskianalyysillä**.

2. Liiketoiminnan vaikutusanalyysillä (business impact analysis, BIA) selitetään ja kuvataan, miten ensimmäisessä vaiheessa tunnistetut mahdolliset häiriöt vaikuttavat organisaation liiketoimintaprosesseihin.

- Tämän analyysin avulla määritellään, missä järjestyksessä organisaation toiminnot palautetaan käyntiin häiriön päätyttyä.
- Lisäksi määritellään, mitä tarkistuksia jokaista toimintoa palautettaessa tulee tehdä ennen kuin voidaan siirtyä seuraavan toiminnon palauttamiseen.
- Vaikutusanalyysin prosessikaavio on esitetty alla.



Vaikutusanalyysin vaiheet. Analyysillä selvitetään palvelun tai järjestelmän tärkeys, toimintojen väliset riippuvuudet, toimintaa uhkaavat riskit sekä tarpeelliset jatkokehitystoimet. (VM 22/2017 s. 15)

3. Vaikutusanalyysi on tärkeä pohja **toimintojen priorisoinnissa**, toiminnan jatkuvuutta uhkaavien negatiivisten riskien arvioinnissa ja toimintojen välisen riippuvuuden tunnistamisessa.

4. Häiriön jälkeisten palautumistavoitteiden määrittelyssä käytetään käsitteitä RPO ja RTO:

- **Recovery point objective (RPO)** määrittelee tavoitellun toipumispisteen, johon toiminta, tiedot tai järjestelmät tulee palauttaa häiriön jälkeen. Toipumispisteen ei välttämättä tarvitse olla sama kuin häiriön alkamishetki. Palvelusopimuksessa (SLA) voidaan esimerkiksi määritellä, että varmuuskopio otetaan aina tunnin välein.

- **Recovery time objective (RTO)** taas määrittelee tavoitellun toipumisajan, jonka kuluessa kukin toiminto tulee saada palautettua takaisin toimintaan häiriötilanteen ilmettyä. Toiminnosta riippuen RTO voi olla sekunnin osia (esim. varavirran kytkeytyminen päälle), minuutteja, tunteja (esim. palvelimen datan palauttaminen varmuuskopiosta) tai päiviä (tuotantoprosessin uudelleenkäynnistäminen katkon jälkeen). RTO voidaan määritellä palvelusopimuksessa, kun ollaan joko palvelun asiakas tai palvelun tuottaja.

5. Kriittisten toimintojen jatkuvuussuunnittelu tulee määritellä tai päivittää.

6. Tehdään **palvelutasojen** tarkastus ja päätökset sen päivittämisestä.

- **Service level agreement (SLA)** on asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään hankituille palvelulle tietyt vaatimustasot ja mitataan erityyppisillä mittareilla, toteutuvatko palveluille asetetut vaatimukset. Jos palvelutaso alittuu, siitä seuraa sopimuksen mukainen sanktio.
- SLA sisältä tyypillisesti seuraavat kohdat:
 - i. Tavoitteiden määrittely
 - ii. Palvelun laajuus
 - iii. Palvelun tarjoajan vastuut
 - iv. Palvelun asiakkaan vastuut
 - v. Palvelun suorituskyky mittarit, kuten vasteaika ja häiriön ratkaisuaika
 - vi. Sanktiot sopimusrikkomuksesta; poissulkemiset

7. Dokumentoidaan **toipumissuunnitelmat**.

8. Toteutetaan **jatkuvuussuunnitelman auditointi, harjoittelu ja koulutus**.

Jonkin ajan päästä jatkuvuuden hallintaprosessia kehitetään päivittämällä toimintaympäristö- ja riskianalyysi sekä suorittamalla toiminnan vaikutusanalyysi ja muita vaiheita. Näiden vaiheiden läpikäyminen voidaan nähdä jatkuvana kehänä ja olennaisena osana jatkuvuudenhallintaa. Jatkuvuuden hallintaprosessi vaatii säännöllistä uudelleentarkastelua ja päivittämistä, jotta suunnitelmat ja menettelytavat voidaan pitää ajan tasalla. Eri vaiheita suunnitellaan toistuvien katselmointien tai havaittujen muutosten arvioinnin yhteydessä.

Koko liiketoiminnan kattava jatkuvuussuunnittelun standardi on *SFS-EN ISO 22301:2019 Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät*. Standardin vaatimukset liiketoiminnan jatkuvuudenhallinnalle käydään tarkasti läpi Riskioppi-ympäristön kappaleessa 2.3.

Jatkuvuussuunnitelma

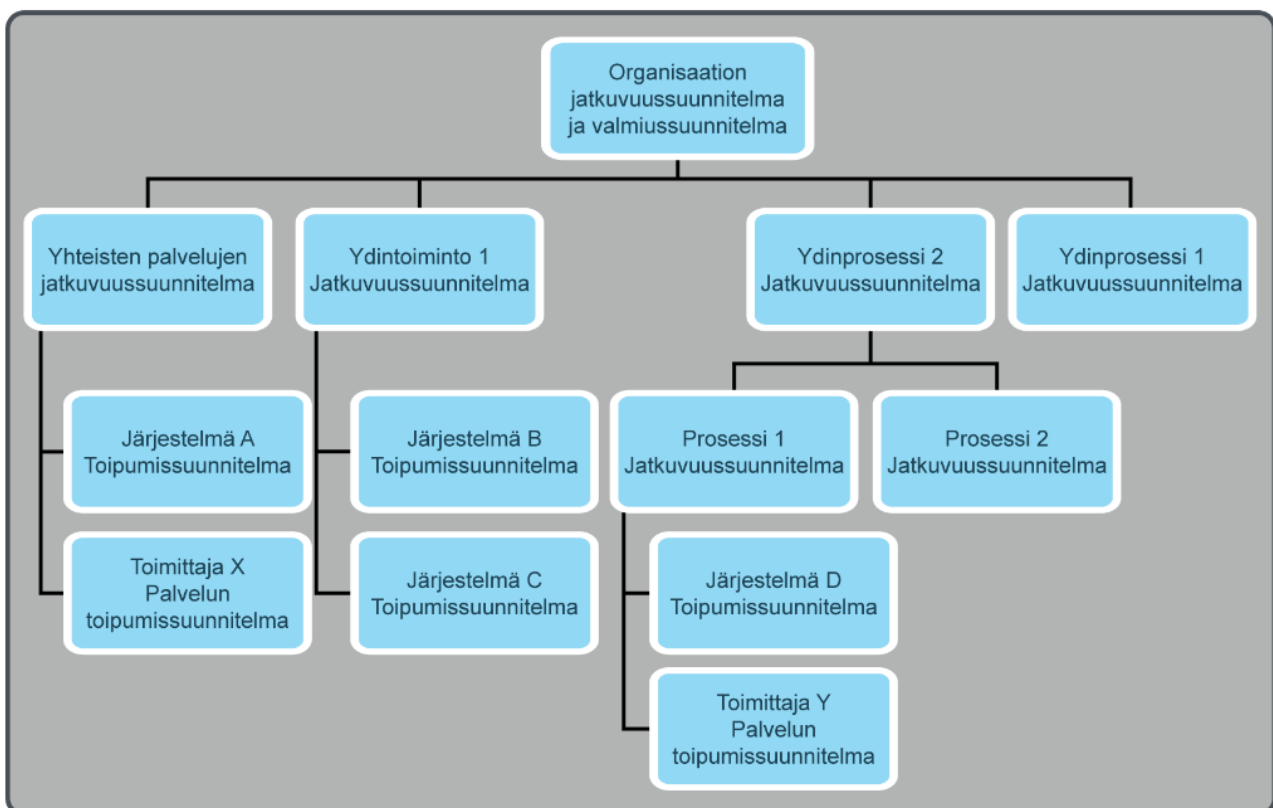
Jatkuvuussuunnittelussa tuotettu materiaali kootaan **(liiketoiminnan) jatkuvuussuunnitelmaksi**. Jatkuvuussuunnitelma sisältää kirjalliset määrittelyt vastuista ja toimenpiteistä häiriötilanteiden varalle.

Jatkuvuussuunnitelmassa kuvataan vähintään, miten häiriötilanteissa toimitaan, mitä toipumistoimenpiteitä tehdään ja miten sidosryhmien kanssa kommunikoidaan. Lisäksi suunnitelmassa määritellään, kuinka organisaation toimintaa johdetaan ja kenellä on vastuut häiriötilanteissa.

Organisaation jatkuvuussuunnitelma on yleensä kokonaisuus, joka koostuu useamman toiminnon ja prosessin jatkuvuussuunnitelmasta.

Organisaation eri kohteisiin liittyviä suunnitelmia voidaan tarkastella **hierarkkisissa suhteissa** toisiinsa. Alla kuvatun VAHTI 2/2016 -ohjeen mukaan ylimmällä tasolla ovat koko organisaation jatkuvuussuunnitelma ja valmiussuunnitelma.

- Koko organisaation jatkuvuussuunnitelma jakautuu yhteisten palvelujen jatkuvuussuunnitelmaan, organisaation ydintoimintojen jatkuvuussuunnitelmiin ja organisaation ydinprosessien jatkuvuussuunnitelmiin.
- Jokainen näistä jatkuvuussuunnitelmista sisältää toipumissuunnitelman. Toipumissuunnitelma koskee kuhunkin palveluun, toimintoon tai prosessiin liittyvää järjestelmää tai toimittajaa.

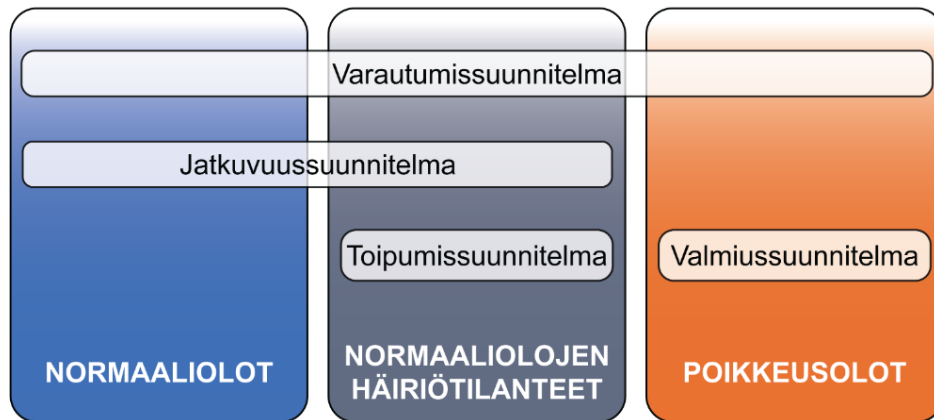


Kaaviossa esitetään VAHTI 2/2016 -ohjeen mukainen suunnitelmien välinen hierarkia (Valtiovarainministeriö 2016 s. 41).

Kaaviossa esitetty hierarkia auttaa, kun laaditaan suunnitelmia tai haetaan niitä ja jaetaan suunnitelmia IT-järjestelmään liittyvien yhteistyökumppaneiden kanssa.

Normaaliolot, häiriötilanteet ja poikkeusolot

Alla oleva kaavio esittää jatkuvuussuunnitteluun liittyviä käsitteitä. Tässä mallissa toiminnan olosuhteet on jaettu kolmeen eri tyyppiin: 1) normaaliolot; 2) normaaliolojen häiriötilanteet; 3) poikkeusolot.



Jatkuvuussuunnittelun käsitteiden ja määritelmien suhde toisiinsa. (Iivari & Laaksonen 2009 s. 19).

Tämän mallin mukaan varautumissuunnitelma kattaa toiminnan normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Jatkuvuussuunnitelma puolestaan kattaa ainoastaan normaaliolot ja normaaliolojen häiriötilanteet.

Normaaliolojen aikana toteutetaan jatkuvuussuunnitelmat, toipumissuunnitelmat ja valmiussuunnitelmat, sekä harjoitellaan niiden käyttöönottoa.

Normaaliolojen häiriötilanteista selvittää jatkuvuussuunnitelman ja toipumissuunnitelman avulla.

Poikkeusoloista selvittää valmiussuunnitelman ja varautumissuunnitelman avulla. Poikkeusolot määritellään kansainvälisestä tilanteesta tai suuronnettomuudesta johtuvaksi **vakavaksi vaaraksi** talouselämälle, oikeusjärjestykselle, väestön toimeentulolle, kansalaisten perusoikeuksille tai maan alueelliselle koskemattomuudelle (JOHDA s. 222).

- **Valmius on tila**, joka saavutetaan suunnittelun ja valmistelujen tuloksena ja jossa kyetään vastaamaan mahdollisiin tiedossa oleviin uhkiin (JOHDA s. 226).
- Valmiussuunnittelulla varaudutaan erilaisiin turvallisuustilanteisiin. Sen tuloksena syntyy **valmiussuunnitelma**. Valmiussuunnitelma on dokumentti, jossa kuvataan, miten toiminnan jatkuvuus turvataan ja mitä toimenpiteitä on suoritettava normaalioloihin palaamiseksi. (lähde: Sosiaalitoimen valmiussuunnitteluopas 2008)

Jatkuvuussuunnittelu parantaa **huoltovarmuutta** organisaatiossa ja siinä toimittajaverkostossa, johon se kuuluu.

Jatkuvuudenhallinta ja riskienhallinta

Riskienhallinnan konsulttiyrityksen Graniten mukaan liiketoiminnan **jatkuvuussuunnittelu** on laaja prosessi, jonka kautta organisaatio jatkuvasti tunnistaa ja arvioi toimintaansa vaarantavia riskejä. Riskien tunnistamisen jälkeen tehdään liiketoimintavaikutusten analyysi. Liiketoimintavaikutusten analyysin avulla arvioidaan, mitä riskien mahdollinen toteutuminen merkitsisi organisaatiolle. Samalla määritetään organisaation kriittiset, ylläpidettävät toiminnot. Seuraavaksi kehitetään toimintatapoja, joilla voidaan ennaltaehkäistä tunnistettuja uhkatilanteita, suojautua niiltä ja rajoittaa niiden vaikutuksia.

Yksi yleisimmistä haasteista jatkuvuudenhallinnassa on riskien tunnistaminen ja arvioiminen. Jatkuvuudenhallinnan kannalta on tärkeää tunnistaa riskit ja uhat, jotka voivat häiritä toimintaa. Tunnistaminen voi kuitenkin olla haastavaa, koska mahdolliset häiriöt voivat tulla useista lähteistä ja niillä voi olla erilaisia vaikutuksia. Ratkaisuna tähän haasteeseen Granite ehdottaa, että riskiarviointia tehdään säännöllisesti. Riskiarvioinnit auttavat tunnistamaan uusia uhkia ja päivittämään jatkuvuudenhallinnan suunnitelmia niiden pohjalta.

Jatkuvuussuunnittelussa on erityisen tärkeää tunnistaa **henkilöstöön kohdistuvat riskit ja uhat**. Jatkuvuudenhallintasuunnitelmassa onkin turvattava, että **avainhenkilöt ovat tavoitettavissa ja käytettävissä** häiriötilanteiden aikana. Tavoittamisen voi estää sairaus, loma tai jokin muu syy. Organisaatioiden tulee siksi varautua varamiesjärjestelyillä siihen, että avainhenkilöt eivät ole tavoitettavissa. Lisäksi avainhenkilöiden yhteystietojen on oltava ajan tasalla. (GRANITE)

Viestintä osana jatkuvuussuunnittelua

Jatkuvuussuunnitteluun kuuluu myös viestintäsuunnitelman kehittäminen. Viestintäsuunnitelmalla varmistetaan, että työntekijöitä, asiakkaita ja muita sidosryhmiä tiedotetaan oikealla hetkellä ja oikealla tavalla poikkeus- tai häiriötilanteessa.

Viestintä voi olla haastavaa poikkeus- ja häiriötilanteen aikana, koska työntekijät voivat olla hajallaan ja viestintäjärjestelmät voivat häiriön vuoksi olla poissa käytöstä. Tämän vuoksi jatkuvuusvalmiutta parannetaan rakentamalla varaviestijärjestelmä ja harjoittelemalla hätäviestintätoimenpiteitä säännöllisesti. (GRANITE)

Vakuuttaminen

Vakuuttaminen on yksi periaate, jolla riskiä siirretään. Vakuuttamisessa riski siirretään ulkopuoliselle taholle. Ulkopuoliselle taholle maksetaan siitä, että se korvaa kielteiset vaikutukset, jos riski toteutuu. Vakuutuksen hinta punnitaan suhteessa niihin kustannuksiin, jotka riskin toteutuminen aiheuttaisi toiminnalle. Vakuuttaminen on myös keino, jolla organisaatio voi varautua mahdollisiin häiriötilanteisiin ja siten edistää jatkuvuudenhallintaa.

Toiminnan keskeytymiselle on saatavilla erityyppisiä vakuutuksia. Vakuutuksilla korvataan niitä taloudellisia menetyksiä, joita yrityksen toiminnan keskeytymisestä aiheutuu. Tällaisia keskeytysvakuutuksia ovat esimerkiksi palovakuutus, rikkovakuutus, epidemiavakuutus, riippuvuusvakuutus ja vuokratuottokeskeytysvakuutus. Keskeytysvakuutukset auttavat yritystä

selviytymään kustannuksista, joita toiminnan keskeytyminen aiheuttaisi. Tällaisia kustannuksia ovat esimerkiksi menetetty tuotanto, palkat ja vuokrat. Vakuutuksen hinta määräytyy sen mukaan, kuinka suuri riski on ja kuinka kattava vakuutus on.

Henkilövakuutus tai henkilökeskeytysvakuutus suojaavat yrityksen toimintaa tärkeiden henkilöiden sairastumisen tai kuoleman varalta.

Digitaalisessa toimintaympäristössä tietoturvakatuus täydentää yrityksen omaisuuden ja toiminnan vakuutuksia. Näitä vakuutuksia tarjotaan eri kattavuuksilla ja nimillä, kuten kybervakuutus.

Täydennä osaamistasi

Seuraavaan on koottu dokumentteja, jotka koskevat jatkuvuudenhallinnan toteuttamista erilaisissa organisaatioissa. Voit perehtyä niihin omassa tahdissasi.

- a. Turvallisuuskomitea (2017): [Kokonaisturvallisuuden sanasto](#)
- b. VM 22/2017 Ohje riskienhallintaan: [LIITTEET 1-6](#)
- c. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä: [VAHTI 2/2016](#).
 - Ohjeen tavoitteena on tehostaa ja yhdenmukaistaa jatkuvuudenhallintaa mm. julkisessa hallinnossa.
- d. Valtionvarainministeriö (2012): [VAHTI 2/2012 ICT-varautumisen vaatimukset](#).
- e. Työterveyslaitos: [KUJA-malli](#), joka on laadittu julkisten organisaatioiden valmiussuunnittelun edistämiseksi.



Valitse alla olevasta listasta sinun mielestäsi yritysten yleisimmät haasteet jatkuvuudenhallinnassa.

- ◇ Ylimmän johdon tuen puute: Ilman tukea ja sitoutumista liiketoiminnan jatkuvuussuunnitelmat eivät välttämättä saa riittävästi resursseja, huomiota tai prioriteettia organisaatiossa.

- ◇ Riittämätön riskinarviointi: Kattavien riskiarviointien suorittamatta jättäminen voi johtaa huomiotta jääviin haavoittuvuuksiin ja mahdollisiin uhkiin, mikä johtaa tehottomaan liiketoiminnan jatkuvuussuunnitelmaan.
- ◇ Riippuvuuksien huomiotta jättäminen: Kriittisten liiketoimintatoimintojen, järjestelmien, toimittajien tai kumppaneiden välisten riippuvuuksien tunnistamisen ja korjaamisen epäonnistuminen voi johtaa jatkuvuussuunnitelman aukkoihin ja mahdollisiin epäonnistumiskohtiin.
- ◇ Riittämätön dokumentaatio: Liiketoiminnan jatkuvuussuunnitelma, joka on dokumentoitu huonosti tai joista puuttuu tarvittavat yksityiskohdat, voi olla haastavaa ymmärtää, toteuttaa ja päivittää tarvittaessa.
- ◇ Epätäydelliset palautusstrategiat: Palautusstrategioiden, kuten varmuuskopiointijärjestelmien, vaihtoehtoisten toimittajien tai etätyöominaisuuksien, riittämätön huomioiminen voi haitata organisaation kykyä jatkaa toimintaansa nopeasti.

Valitse alla olevasta listasta sinun mielestäsi yritysten yleisimmät haasteet jatkuvuudenhallinnassa, kun keskitytään tulevaisuuden suunnitteluun.

- ◇ Teknologisen kehityksen ja kehittyvien uhkien huomioimatta jättäminen: Liiketoiminnan jatkuvuussuunnitelmat, jotka eivät mukaudu teknologiseen kehitykseen tai eivät pysty vastaamaan uusiin uhkiin, kuten kyberturvallisuusriskeihin tai ilmastoon liittyviin tapahtumiin, voivat nopeasti vanhentua ja olla tehottomia.
- ◇ Riittämätön testaus ja ylläpito: Säännöllisten testausten, harjoitusten ja liiketoiminnan jatkuvuussuunnitelman ylläpidon laiminlyönti voi johtaa vanhentuneisiin menettelyihin, kouluttamattomaan henkilöstöön ja todentamattomiin palautusominaisuuksiin.
- ◇ Tarkistuksen ja päivityksen epäonnistuminen: Liiketoiminnan jatkuvuussuunnitelman säännöllisten tarkistusten ja päivitysten laiminlyönti voi johtaa vanhentuneisiin yhteystietoihin, vanhentuneisiin menettelyihin tai käsittelemättömiin muutoksiin liiketoimintaympäristössä, mikä tekee suunnitelmasta vähemmän hyödyllisen tarvittaessa.
- ◇ Riittämättömät viestintäsuunnitelmat: Selkeiden ja tehokkaiden viestintäsuunnitelmien puute häiriöiden aikana voi johtaa sekaannukseen, väärään tietoon ja viivästyneeseen reagointiin, mikä vaikuttaa organisaation kykyyn toipua tehokkaasti.
- ◇ Työntekijöiden tietoisuuden ja koulutuksen puute: Jos työntekijät eivät ole tietoisia toiminnan jatkuvuussuunnitelmasta tai heitä ei ole koulutettu riittävästi rooleihinsa ja vastuusiinsa häiriötilanteissa, suunnitelman tehokkuus voi vaarantua.

2.2 Häiriöiden kartoittaminen

Oppimistavoite: Tässä kappaleessa opit häiriön erilaisia määritelmiä ja esimerkkejä mahdollisista häiriöistä. Käytä tätä osaamista pohjana häiriöiden ja uhkien tunnistamiselle omassa toiminnassasi. Kappaleen lopussa pääset harjoittamaan oppimaasi monivalinta- ja valintatehtävissä häiriöiden tunnistamisesta ja ehkäisystä. Arvioitu ajankäyttö: 15 min.

Edellä esitettiin ISO 22301-standardiin pohjautuva määritelmä, jonka mukaan häiriö on **odotettu tai odottamaton tilanne**, joka aiheuttaa **suunnittelemtoman negatiivisen poikkeaman** tuotteiden ja palveluiden organisaation **tavoitteiden mukaisessa toimittamisessa**. Tarkastellaan seuraavassa laajemmin häiriön käsitettä ja häiriöiden kartoittamista.

Häiriö voidaan myös määritellä seuraavasti (JOHDA s. 219):

- **"tilanne tai tapahtuma, jonka vuoksi järjestelmä [...] ei toimi normaalisti"**
- **"toiminnan jonkin osatekijän haitallinen vaihtelu, jonka puitteissa toiminta voi silti pääosin jatkua".**

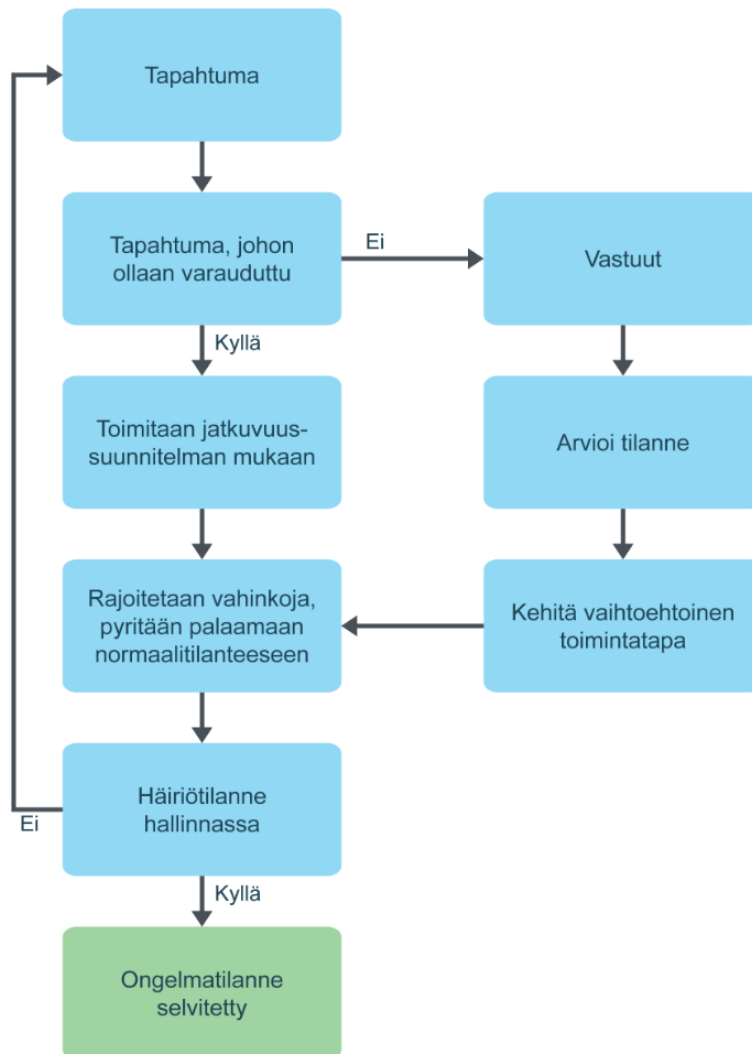
Häiriö voi siis ilmetä yksittäisenä tapahtumana tai se voi olla joko säännöllisesti tai epäsäännöllisesti toistuva tapahtuma.

Häiriötilanne on tapahtuma, josta seuraa häiriö, tuho, hätätilanne tai kriisi.



Häiriöt voidaan luokitella niiden vakavuuden perusteella. Riskienhallinnassa joudutaan tekemään asioiden priorisointia eli tärkeysjärjestykseen asettamista aivan kuten jatkuvuudenhallinnassakin. Jatkuvuudenhallinnassa organisaation eri toiminnot asetetaan siis tärkeysjärjestykseen, ja tärkeysjärjestyksen avulla voidaan määrittää, mitkä toiminnot on käynnistettävä ensimmäisenä häiriön sattuessa. Usein toiminnot ovat ketjuuntuneita, jolloin yhden toiminnon häiriö voi johtaa koko prosessin pysähtymiseen.

Seuraavassa kaaviossa on kuvattuna yleiskäyttöinen prosessikuvaus häiriöstä toipumiseen.



Prosessikuvaus häiriöstä toipumiseen (Iivari & Laaksonen 2009 s. 206).

Prosessin mukaan, aluksi selvitetään, onko tapahtuma sellainen, johon on etukäteen varauduttu. Mikäli on, edetään tapahtuman käsittelemiseksi jatkuvuussuunnitelman pohjalta, kunnes häiriö on selvitetty. Mikäli tapahtuma onkin sellainen, johon ei olla varauduttu, nojaututaan organisaatiossa määriteltuihin vastuisiin häiriöstä toipumisen edistämiseksi. Tarpeen kiireellisyyden arviointi on tärkeää, jotta kriittisimpiin asioihin reagoidaan ensimmäiseksi.

Häiriöt digiympäristössä

Digiympäristössä häiriö on VAHTI-sanaston (s. 19) mukaan "*odottamaton tai ei-toivottu tapahtuma, joka haittaa järjestelmän, järjestelmän käyttäjän tai niistä riippuvaisten toimintaa*".

Edelleen VAHTI-sanastossa tarkennetaan, että häiriöiksi kutsutaan tavallisesti tapahtumia, joista aiheutuva haitta on tilapäistä ja lyhytaikaista joko tapahtumaan luonteen vuoksi tai oikeiden vastatoimenpiteiden ansiosta. Digiympäristössä häiriön aiheuttaa esimerkiksi hyökkäys tai

odottamaton tapahtumaketju. Häiriöllä on usein jokin **mahdollistaja**, kuten järjestelmän heikkous, puute tai vika. (VAHTI s. 19)

Häiriö voi aluksi ilmetä joko digitaalisessa tai fyysisessä toimintaympäristössä, ja sen vaikutukset voivat laajentua ympäristöstä toiseen. Fyysisessä ympäristössä ilmeneviä vakavia liiketoimintaan kohdistuvia häiriötilanteita ovat esimerkiksi yrityksen tai sen yhteistyökumppanin toimitiloissa tapahtuva tulipalo, vesivahinko tai sähköjärjestelmän vaurio. Jos tällaiset häiriöt toteutuvat, ne voivat välittömästi katkaista myös yrityksen digitaalisen ympäristön toiminnan. Yrityksen digiympäristössä ilmeneviä tyypillisiä vakavia häiriötilanteita ovat tietovuoto ja laajamittainen käyttöhäiriö yrityksen tietoverkossa tai tietojärjestelmissä.

Vakavien häiriöiden uhkaa digiympäristössä lisäävät laajat toimittaja- ja alihankkijaverkostot, joissa useiden organisaatioiden tietojärjestelmät ovat yhteydessä toisiinsa.

Kansainvälinen kartoitus häiriöistä

Business Continuity Institute on kansainvälinen verkosto, joka koostuu liiketoiminnan jatkuvuuden asiantuntijoista. Verkostossa on yli 9000 jäsentä 120 maassa. Verkosto julkaisee vuosittaisia kartoituksia, joissa käsitellään yleisimpiä ja vakavimpia häiriöitä, joita organisaatiot voivat kohdata toiminnassaan.

Vuoden 2022 raportissa kuvataan merkittävimpiä häiriöitä (engl. major disruption) edellisen vuoden ajalta sekä esitetään arvioita mahdollisista merkittävistä häiriöistä, jotka voivat ilmetä seuraavien 12 kuukauden aikana.

Kartoituksen aineisto on kerätty pyytämällä vastaajia ilmoittamaan, kuinka usein tietty häiriötilanne tai tapahtuma esiintyy heidän organisaatiossaan ja miten suuri vaikutus sillä on. Jokaiselle tapahtumalle on laskettu **riski-indeksi**. Riski-indeksi saadaan kertomalla tapahtuman yleisyyttä kuvaava luku tapahtuman vaikutuksen arvioitua merkittävyttä ilmaisevalla luvulla.

Seuraava taulukko kuvaa vuoden 2021 tilannetta.

Tapahtuma/häiriö	Yleisyys	Vaikutus	Riski- indeksi	Tapahtuma englanniksi
1. Muu sairaus kuin ammattitauti (esim. pandemia)	9.7	2.5	24.5	1. Non-occupational disease (e.g. pandemic)
2. Häiriöt johtuen etätyöstä tai uudesta työpaikkaympäristöstä	11.4	2.1	24.3	2. (Issues arising from) remote working/new workplace environment
3. Matkustusrajoitukset	10.0	2.1	21.5	3. Travel restrictions
4. Työterveys (työperäinen sairaus, raportoitava ammattitauti, stressi/mielenterveysongelmat, lisääntyneet sairauspoissaolot)	9.4	1.9	17.9	4. Health incident (NOT transmissible disease such as COVID but occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)
5. Kyvykkään henkilöstön vaje ja avaintaitojen osaamisen puute	8.0	2.2	17.3	5. Lack of talent/key skills
6. Turvallisuushäiriö (tapaturma, kuolema, omaisuusvahinko, vaarallinen tapahtuma, viranomaisille raportoitava tapahtuma)	7.8	1.9	14.5	6. Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)
7. Häiriö toimitusketjussa	6.3	2.1	13.3	7. Supply chain disruption
8. Tietojärjestelmien ja tietoliikenteen katkokset	6.1	2.0	12.3	8. IT and telecom outage
9. Kyberhyökkäykset ja tietomurrot	6.0	2.0	11.7	9. Cyber attack & data breach
10. Ampumisvälikohtaus, yksittäinen hyökkääjä	4.8	2.3	11.1	10. Lone attacker/active shooter incident
11. Äärimmäiset sääilmiöt (esim. tulvat, myrskyt, pakkaset jne.)	5.4	2.0	10.9	11. Extreme weather events (e.g. floods, storms, freeze, etc.)
12. Muutokset sääntelyssä	5.2	2.1	10.9	12. Regulatory changes
13. Luonnonvarapula	5.2	2.0	10.3	13. Natural resources shortage
14. Korkeammat lainakustannukset	5.4	1.9	10.2	14. Higher cost of borrowing
15. Sähkönjakelun keskeytykset	5.0	1.9	9.7	15. Interruption to utility supply
16. Valuuttakurssien volatiileetti	4.8	2.0	9.6	16. Exchange rate volatility
17. Poliittinen väkivalta/siviili levottomuudet	4.9	1.9	9.4	17. Political violence/civil unrest
18. Energian hintasokki	4.5	2.0	9.2	18. Energy price shock
19. Poliittinen muutos	4.0	2.2	8.6	19. Political change
20. Uuden teknologian käyttöönotto (IoT, AI, Big data)	4.4	1.9	8.4	20. Introduction of new technology (IoT, AI, Big data)
21. Kriittinen infrastruktuurihäiriö	3.9	2.1	8.2	21. Critical infrastructure failure
22. Luonnonkatastrofit (maanjäristykset, tsunamit jne.)	4.3	1.9	7.9	22. Natural disasters (earthquakes, tsunamis, etc.)
23. Sääntelyviranomaisen toimenpiteet	3.7	2.0	7.2	23. Enforcement by regulator
24. Takaisin veto tuoteturvallisuuden vuoksi	3.2	1.8	5.6	24. Product safety recall

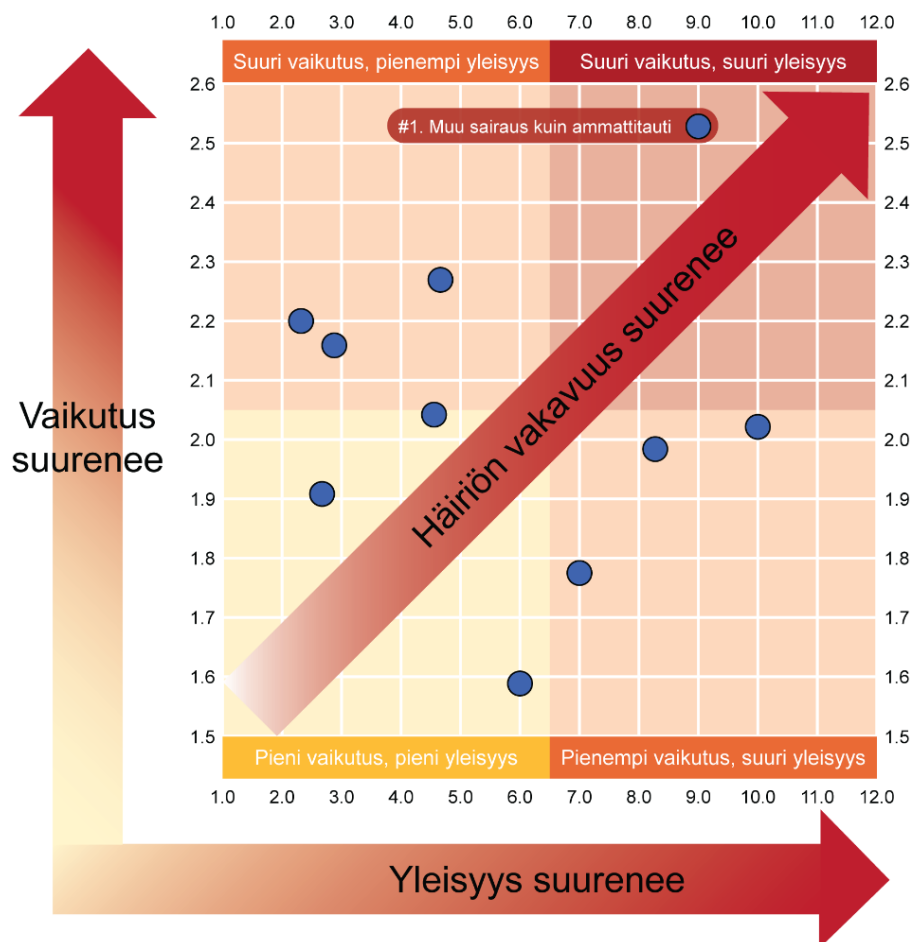
Taulukko on muokattu lähteestä Business Continuity Institute, Horizon Scan Report 2022.

Vuoden 2021 merkittävimmiksi häiriöiksi on nostettu Covid19-pandemia, uuden etätyö- ja hybridityöskentely-ympäristön haasteet sekä matkustusrajoitukset. On tärkeää huomata, että energianhinnan äkillinen nousu on taulukossa vasta sijalla 18.

On niin ikään huomattava, että tässä kartoituksessa lähes jokaisella esiin nostetulla häiriöllä on jokin yhteys digitaaliseen toimintaympäristöön, joko suoraan tai välillisesti.

Häiriökartoituksen visualisointi

Alla olevassa kuviossa ehdotetaan käyttökelpoista menetelmää, jolla häiriöitä voidaan kartoittaa kokonaisuutena. Häiriöt sijoitetaan kuvioon, jossa yhdellä akselilla on tapahtuman yleisyys ja toisella akselilla tapahtuman vaikutus. Tapahtuman yleisyyttä kuvaavat lukuarvot ja tapahtuman vaikutuksen arvioitua merkittävyyttä kuvaavat lukuarvot poimitaan edellä esitetystä taulukosta. Kaavion kenttä voidaan jakaa neljään sektoriin häiriöiden vakavuuden mukaan. Tällä menetelmällä organisaatio voi verrata omaa tulkintaansa uhkaavista häiriöistä Business Continuity Instituten raportin yhteisarvioon.



Yhteenveto arvioiduista riskeistä ja uhista vuonna 2021. Business Continuity Institute, Horizon Scan 2022.

Linkki raporttiin: [Business Continuity Institute, Horizon Scan 2022](#). Vuosittainen raportti julkaistaan aina keväällä. Tuorein raportti kannattaa käydä lukemassa, sillä siinä esitetään arvio merkittävimmistä häiriöistä seuraavien 12 kuukauden ajalle.

[Etelä-Pohjanmaan alueellinen riskiarvio](#) on julkaistu 5.5.2023. Siinä on esitetty skenaarioita muun muassa joukosta informaatioteknologiaan vaikuttavista alueellisista häiriöistä, kuten sähköntuotannossa, tietojärjestelmissä ja tietoliikenteessä.



Mikä seuraavista kuvauksista sopisi mielestäsi häiriökartoituksen nelikentässä kategoriaan "vakava, mutta ei yleinen"?

- ◇ Yrityksen sisäinen sähköpostipalvelin lakkaa toimimasta muutamaksi tunniksi, joka hidastaa viestintää organisaation sisällä.
- ◇ Työntekijä unohtaa salasansansa ja joutuu pyytämään uuden, mikä hidastaa hänen pääsyään työtehtäviin.
- ◇ Yrityksen koko verkkopalvelu kaatuu useiden tuntien ajaksi, mikä vaikuttaa tuhansiin asiakkaisiin.
- ◇ Asiakastietokantaan kohdistuu tietomurto, joka saattaa johtaa joidenkin asiakkaiden henkilökohtaisten tietojen vuotamiseen.

Valitse alla olevasta listasta ne keinot, joita olet itse käyttänyt estääksesi tai vähentääksesi häiriöiden todennäköisyyttä omassa digitaalisessa ympäristössäsi.

- ◇ Vaihdan salasansani säännöllisesti.
- ◇ Käytän kaksivaiheista tunnistusta.
- ◇ Käytän ja päivitän luotettavaa virustorjuntaohjelmistoa.
- ◇ Käytän vahvoja salasanoja, jotka sisältävät erikoismerkkejä, numeroita ja isoja sekä pieniä kirjaimia.
- ◇ Otan varmuuskopioita tärkeistä tiedostoista ja palautan tiedostojani säännöllisesti.
- ◇ En avaa epäilyttäviä sähköposteja, linkkejä tai tiedostoja.
- ◇ Päivitän käyttöjärjestelmäni ja sovellukseni säännöllisesti.
- ◇ Salaan verkkoliikenteeni VPN-yhteyden kautta.
- ◇ Vältän julkisen Wi-Fi-verkon käyttämistä, kun käsittelen arkaluontoista tietoa.
- ◇ Osaan tunnistaa kalasteluviestit.

2.3 ISO 22301 -standardi

Oppimistavoite: Tässä kappaleessa opit hyödyntämään ISO 22301 -standardin ohjeistusta siitä, miten jatkuvuudenhallintaa ja jatkuvuussuunnitelmaa toteutetaan. Standardissa on ohjeet jatkuvuudenhallinnan yhdenmukaiseen toteuttamiseen tavalla, jota noudatetaan kaikkialla maailmassa. ISO 22301:n vaatimuksiin on hyvä perehtyä, vaikka organisaatiosi ei suunnittelisi standardin sertifiointia. Kappaleen lopussa vastaat valintatehtäviin, jossa opastat toimimaan standardin mukaisesti. Testaa tunnistatko kaikki tarvittavat toimenpiteet! Arvioitu ajankäyttö: 20 min.

Standardi on määritelmä siitä, miten jokin asia tulisi tehdä. Standardiin sisältyy yleensä yhtenäinen toimintamalli, jonka noudattaminen auttaa eri toimijoita toimimaan yhdenmukaisesti ja tehokkaasti. ISO (International Organization for Standardization) on kansainvälinen standardisoimisjärjestö, jossa Suomea edustaa Suomen Standardisoimisliitto SFS.

ISO 22301 -standardin suomenkielinen versio on SFS-EN ISO 22301:2019 ja täydeltä nimeltään **"Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät."** Standardin vaatimuksia noudattamalla organisaatiot voivat

- varmistaa häiriötilanteiden varalta suojautuminen organisaation toiminnassa
- minimoida sen todennäköisyys, että toimintaa häiritseviä tapahtumia esiintyy
- varmistaa, että organisaatio on valmis varautumaan ja reagoimaan häiriötilanteisiin sekä palautumaan niistä.

ISO 22301 -standardin mukaan toteutettu toiminnan jatkuvuuden hallintajärjestelmä tukee organisaation riskienhallintaa.

Tässä kappaleessa käydään läpi standardin keskeisiä ohjeita siitä, miten jatkuvuuden hallintajärjestelmää toteutetaan organisaatiossa.

Hankkiminen ja mahdollinen sertifiointi

ISO 22301 -standardin määrittelevä dokumentti on saatavilla esim. [SFS:n verkkopalvelusta](#). Lisäksi on saatavilla erillinen ohjeistus nimeltä ISO 22313, joka tukee standardin käyttöönottoa.

Organisaatio voi sertifioida ISO 22301 -standardin ja näin osoittaa, että standardissa määritellyt vaatimukset täyttyvät organisaatiossa. Tämä lisää asiakkaiden ja yhteistyökumppaneiden luottamusta organisaation tuotteita ja toimintaa kohtaan. Sertifiointin jälkeen organisaatio käy läpi säännöllisiä seuranta-arviointeja 1–2 kertaa vuodessa. Joka kolmas vuosi suoritetaan uudelleensertifiointi.

Standardin ohjeistusta jatkuvuudenhallinnalle voidaan tuki hyödyntää organisaatiossa myös ilman sertifiointia.



Opi lisää:

- [Sertifiointista yleisellä tasolla](#)
- [Sertifiointiorganisaatioista Suomessa](#)

ISO 22301 -standardin vaatimukset

ISO 22301 -standardin vaatimukset ovat yleisiä: ne soveltuvat kaikenlaisille organisaatioille tai niiden osille.

Standardia hyödyntämällä yritysorganisaatio varmistaa, että sillä on käytössään suunniteltu ja tehokas **liiketoiminnan jatkuvuuden hallintajärjestelmä (BCM)**, jolla voidaan reagoida häiriötilanteisiin.

Kun jatkuvuussuunnittelua tehdään standardin mukaan, jatkuvuussuunnitteluntavoitteena on pyrkiä **integroimaan jatkuvuuden hallintajärjestelmä osaksi organisaation johtamista**, jotta se ei jäisi vain irralliseksi ohjeeksi.

ISO 22301 -standardin mukaan liiketoiminnan jatkuvuuden hallintajärjestelmän keskeiset elementit ovat seuraavat:

1. Liiketoiminnan vaikutusanalyysi (Business impact analysis, BIA)

- liiketoiminnan kannalta **kriittisten toimintojen** tunnistaminen ja
- analyysi siitä, miten kriittisten toimintojen häiriöt vaikuttavat liiketoimintaan

2. Riskien arviointi

Määritellään

- mitä riskejä kriittisiin toimintoihin kohdistuu
- kuinka merkittäviä ja todennäköisiä riskit ovat
- millä toimenpiteillä riskejä voidaan lieventää.

3. Strategia liiketoiminnan jatkuvuudelle

- Perustuu edeltävään vaikutusanalyysiin ja riskien arviointiin.
- Strategiassa määritellään, miten kriittisiä toimintoja suojataan, miten niiden häiriötilanteista toivutaan ja miten häiriöiden seuraukset käsitellään, sekä mitä resursseja tarvitaan häiriöstä toipumiseen.

4. Häiriöihin reagoinnin menettelyt ja käytännöt

- jatkuvuussuunnitelmien laatiminen sekä niiden harjoittelu ja testaus
- viestintää koskevien suunnitelmien laatiminen häiriötilanteiden varalta

Jatkuvuussuunnitelman puitteet

Standardin mukaan organisaation **tulee kehittää liiketoiminnan jatkuvuussuunnitelma**.

Jatkuvuussuunnitelman on **vastattava laajuudeltaan ja tyyppiltään niitä vaikutuksia**, jotka **voidaan sallia tai olla sallimatta** häiriön tapahtuessa.

Jatkuvuussuunnitelmassa määritellään siis, mitkä häiriön aiheuttamat kielteiset vaikutukset ovat hyväksyttäviä ja mitkä eivät. Ei-hyväksyttävien häiriöiden varalle varataan resursseja.

Jatkuvuussuunnitelman tulee olla dokumentoituna ja helposti saatavilla organisaatiossa. Lisäksi se tulisi tehdä saataville myös sidosryhmille, tarvittaessa niille räätälöidyssä muodossa. Jokaisen organisaation jäsenen tulee olla tietoinen omasta roolistaan jatkuvuuden ylläpitämisessä ja kunkin tunnistetun häiriön hallinnassa ennen häiriötä, sen aikana ja sen jälkeen.

Esimerkki jatkuvuussuunnitelman rakenteesta

Alla oleva esimerkki perustuu Dejan Košutićin esitykseen siitä, millainen olisi optimaalinen liiketoiminnan jatkuvuussuunnitelman rakenne erityisesti sellaisille pienille ja keskisuurille yrityksille, jotka noudattavat ISO 22301 -standardin vaatimuksia.



Kuvatut vaiheet pohjautuvat [Dejan Košutićin esitykseen](#).

Seuraavassa on esitetty Košutićin antama esimerkki jatkuvuussuunnitelman pääkohdista ja niiden sisällöstä.

1. Tarkoitus, laajuus ja käyttäjät: Määritellään, miksi suunnitelma on laadittu, mitkä sen tavoitteet ovat, mitä organisaation osia se kattaa ja kenen pitäisi lukea se.

2. Viiteasiakirjat: Jatkuvuussuunnitelma liittyy yleisemmin muun muassa organisaation liiketoiminnan jatkuvuuspolitiikkaan, liiketoiminnan vaikutusanalyysiin ja liiketoiminnan jatkuvuusstrategiaan. Näitä aiheita koskevat viiteasiakirjat on liitettävä jatkuvuussuunnitelmaan.

3. Oletukset: Määritellään ne edellytykset, joiden on oltava voimassa, jotta suunnitelman toimenpiteillä olisi suunniteltu vaikutus.

4. Roolit ja vastuut: Määritellään nimeltä tai toimenkuvan perusteella ne henkilöt, jotka vastaavat organisaatiossa häiriötilanteen hallinnasta ja joilla on valtuudet suorittaa tiettyjä toimintoja, jos häiriötilanne alkaa. Tällaisia toimintoja ovat esimerkiksi suunnitelmien aktivointi, kiireelliset hankinnat ja viestintä.

5. Keskeiset yhteystiedot: Kirjataan sellaisten henkilöiden yhteystiedot, jotka osallistuvat jatkuvuussuunnitelmaan.

6. Suunnitelman aktivointi ja deaktivointi: Määritellään, missä olosuhteissa suunnitelma voidaan aktivoida ja mikä on aktivoinnin tapa. Lisäksi määritellään, minkä edellytysten on täyttyttävä, jotta suunnitelma voidaan deaktivoida ja häiriön todeta päättyneen.

7. Viestintä: Määritellään, mitä viestintäkeinoja käytetään eri ryhmien välillä ja muiden sidosryhmien kanssa häiriön aikana. Lisäksi määritellään, kuka vastaa kommunikoinnista niiden osapuolten kanssa, joihin häiriötilanne vaikuttaa. Edelleen määritellään viranomaisten ja tiedotusvälineiden kanssa käytävän viestinnän säännöt.

8. Häiriöön reagointi: Määritellään, miten häiriön tapahtumaan reagoidaan välittömästi niin, että vahingot voidaan minimoida. Voidaan esimerkiksi määritellä, miten toimitaan välittömästi, kun palohälytin varoittaa tai kun saadaan kiristysviesti haaitaohjelmasta.

9. Fyysiset kokoontumispisteet ja siirtymät: Määritellään ensisijaiset fyysiset kokoontumispisteet häiriön alkamisen varalle. Määritellään myös vaihtoehtoiset kokoontumispisteet sen varalta, että ensisijaisia kokoontumispisteitä ei voida käyttää. Lisäksi kuvataan, miten ensisijaisista kokoontumispisteistä päästään vaihtoehtoihin kokoontumispisteisiin.

10. Toimintojen palautusjärjestys: Luetellaan kaikki palautettavat toiminnot ja ajat, jossa nämä toiminnot palautetaan (RTO).

11. Toiminnan elvytysuunnitelmat: Elvytysuunnitelmissa kuvataan kaikki ne toimet ja vastuut, joiden avulla työvoima, työtilat, infrastruktuuri, ohjelmistot ja prosessit palautetaan vaihteittain normaaliin toimintaan. Toiminnan elvytysuunnitelmissa kuvataan eri toimintojen keskinäiset riippuvuudet ja vuorovaikutus muiden toimintojen ja ulkopuolisten sidosryhmien kanssa.

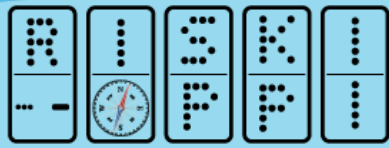
12. Vakavan häiriön palautussuunnitelma: Palautussuunnitelma on tyypillisesti digiympäristön häiriöiden varalta laadittu elvytysuunnitelma, jossa määritellään, miten tieto- ja viestintäteknologian infrastruktuuri palautetaan organisaation käyttöön.

13. Palauttamiseen vaaditut resurssit: Luetellaan resurssit eli kaikki toiminnan palauttamisen kannalta keskeiset työntekijät, kolmannen osapuolen palvelut, tilat, infrastruktuuri, tiedot ja laitteet. Eritellään, mitkä tahot ovat vastuussa tällaisten resurssien tarjoamisesta.

14. Toiminnan palauttaminen ja jatkaminen tilapäisistä toimenpiteistä: Määritellään, miten liiketoiminta palautetaan normaaliksi häiriötilanteen päätyttyä. Lisäksi määritellään, miten häiriön aikaiset tilapäiset toimenpiteet ajetaan alas.

Opi lisää

Tietojärjestelmien jatkuvuudenhallintaan voidaan soveltaa esimerkiksi ISO 27001 -standardia. Standardia noudattamalla organisaatio voi turvata toimintansa jatkuvuutta erilaisissa häiriötilanteissa, kuten tulipalossa, vesivahingossa, hakkeroinnissa, tietojen menetyksessä ja tietovuodoissa. Riskioppi-ympäristön kappaleessa 3.3. on yhteenveto ISO 27001 -standardin vaatimuksista.



TEHTÄVÄ!

Kuvittele seuraava tilanne:

Tuomas on aloitteleva digitaiteilija, joka avasi äskettäin oman verkkokauppansa esitelläkseen ainutlaatuisia taideteoksiaan taiteen harrastajille ympäri maailmaa. Hänen liiketoimintansa on kasvanut tasaisesti, ja hän on päättänyt varmistaa sen pitkäaikaisen menestyksen. Mukana on myös freelancer henkilökuntaa taideopiskelijoiden parista, jotka käyvät hänen työpajallaan epäsäännöllisesti. Tuomas ymmärtää liiketoiminnan jatkuvuuden merkityksen ja haluaa soveltaa ISO 22301 -periaatteita taiteellisen hankkeensa suojelemiseksi.



Vastaa alla, mitkä seuraavista toimista Tuomaksen täytyy tehdä, jotta ISO 22301 standardin liiketoiminnan analyysi ja riskien arviointi toteutuvat?

- ◇ Tuomaksen tulisi arvioida eri toimintojen häiriöiden, kuten verkkosivustojen kaatumisten, toimitusketjun viivästysten tai taidevarkauksien, mahdollisia vaikutuksia tuloihinsa, maineeseensa ja asiakastytyväisyyteensä.
- ◇ Tuomaksen tulisi tehdä kilpailuanalyysi markkinatrendien ja kilpailijastrategioiden tunnistamiseksi.
- ◇ Tuomaksen tulisi ottaa huomioon useat tekijät, kuten verkkokauppaansa kohdistuvat kyberuhat, luonnonkatastrofit, jotka voivat vahingoittaa hänen työpajaansa ja siellä olevia työvälineitä, sekä taideteosten vahingoittumisen mahdollisuus kuljetuksen aikana.
- ◇ Tuomaksen tulisi toteuttaa työhyvinvointiohjelma freelancereiden terveyden ja turvallisuuden edistämiseksi.
- ◇ Tuomaksen tulisi arvioida mahdollisten riskien merkitys ja todennäköisyys, sekä kehittää strategioita todennäköisyyden alentamiseksi.

Liiketoiminnan analyysi ja riskien arviointi eivät ole ainoita asioita, joita Tuomaksen tulisi ottaa huomioon.

Vastaa alla, mitkä seuraavista toimista Tuomaksen täytyy tehdä, jotta ISO 22301 standardin muut osa-alueet toteutuvat?

- ◇ Tuomaksen tulisi toteuttaa mesenaattilistaus verkkokauppaansa, jossa hän kiittää taiteensa ostajia.
- ◇ Tuomaksen tulisi hahmotella erityisiä toimenpiteitä kriittisten toimintojensa suojaamiseksi, kuten perusteellisten kyberturvallisuustoimenpiteiden toteuttaminen verkkokaupassaan, asianmukaisen vakuutusturvan hankkiminen taideteoksilleen ja varmuuskopiointijärjestelmien luominen digitaaliselle omaisuudelleen.
- ◇ Tuomaksen tulisi suorittaa säännöllisiä harjoituksia varmistaakseen, että hänen freelancerinsa on hyvin valmistautunut käsittelemään riski- ja uhkatilanteita.
- ◇ Tuomaksen tulisi järjestää kuukausittaisia taidetyöpajoja paikallisen yhteisön hyväksi.
- ◇ Tuomaksen tulisi luoda tehokkaat viestintäkanavat asiakkaiden, toimittajien ja paikallisten viranomaisten kanssa varmistaakseen koordinoitun reagoinnin häiriöiden aikana.

2.4 Jatkuvuussuunnittelun toteuttaminen: case Mirka Oy

Oppimistavoite: Tässä kappaleessa opit, miten jatkuvuussuunnitelma on toteutettu Mirka Oy:ssä. Mieti jatkuvuussuunnitelman toteuttamista omassa toiminnassasi lukemasi pohjalta. Kappaleen lopussa vastaat monivalintatehtäviin, jossa pääset arvioimaan oman yrityksesi tilannetta jatkuvuussuunnittelussa. Arvioitu ajankäyttö: 25 min.

Tämän kappaleen sisältö pohjautuu esitykseen, jonka Tea Tukia-Kangas Mirka Oy:stä piti Keskeytys 2019 -seminaarissa. [Esityksen diat on julkaistu LähiTapiolan verkkosivuilla.](#)

Yritys

Mirka Oy on suomalainen yritys, joka valmistaa ja markkinoi pintakäsittely- ja tarkkuushiontatarvikkeita. Yritys vie 97 prosenttia tuotannostaan ulkomaille. Yrityksellä on valmistustoimintaa neljällä paikkakunnalla Suomessa sekä Italiassa ja Belgiassa. Yrityksellä on 18 tytäryhtiötä ympäri maailmaa. Mirka Oy työllistää Suomessa noin 900 henkilöä ja maailmanlaajuisesti noin 600 henkilöä.

Jatkuvuussuunnittelu osana normaalia toimintaa

Mirka Oy:ssä jatkuvuussuunnittelu on osa normaalia liiketoimintaa. Pienemmässä mittakaavassa jatkuvuussuunnittelulla varaudutaan häiriöihin, jotka liittyvät esimerkiksi tiedon menetykseen,

työntekijöihin, asiakkaisiin tai toimittajiin. Jatkuvuussuunnittelulla varaudutaan myös suuriin katastrofeihin. Jatkuvuussuunnittelu auttaa yritystä alentamaan riskejä ja vakuuttamisen tarvetta.

Jatkuvuussuunnitelma on hyväksi havaittu työkalu, joka auttaa yrityksen johtoa ja henkilökuntaa toimimaan äkillisissä tilanteissa. Suunnitelmassa määritellään etukäteen, miten eri tilanteissa toimitaan. Tämä mahdollistaa nopean reagoinnin ja vahinkojen minimoimisen.

Jatkuvuudenhallinnan tavoitteet

Mirka Oy:n jatkuvuudenhallinnalle asettamat tavoitteet ovat seuraavat:

- Keskitytään tuotannon toiminnan jatkumiseen ensin Suomessa ja sitten Euroopan laitoksissa.
- Jatkuvuudenhallinta tehdään itse, jolloin organisaatio oppii samalla.
- Kaikki jatkuvuudenhallintaan liittyvä informaatio kootaan yhteen paikkaan olemassa oleville alustoille yrityksen intranettiin.
- Jatkuvuudenhallintaa koskevan tiedon levittäminen organisaatiossa ja henkilöstön osallistuminen jatkuvuudenhallintaan on tärkeää.
- Pyritään siihen, että jatkuvuudenhallinta on osa jokapäiväistä toimintaa.

Mirka Oy:n tavoitteena on ollut luoda organisaatiolle ensin jatkuvuussuunnitelman ”versio 1.0” ja parantaa tätä ensimmäistä versiota sitä mukaa, kun organisaation osaaminen kasvaa.

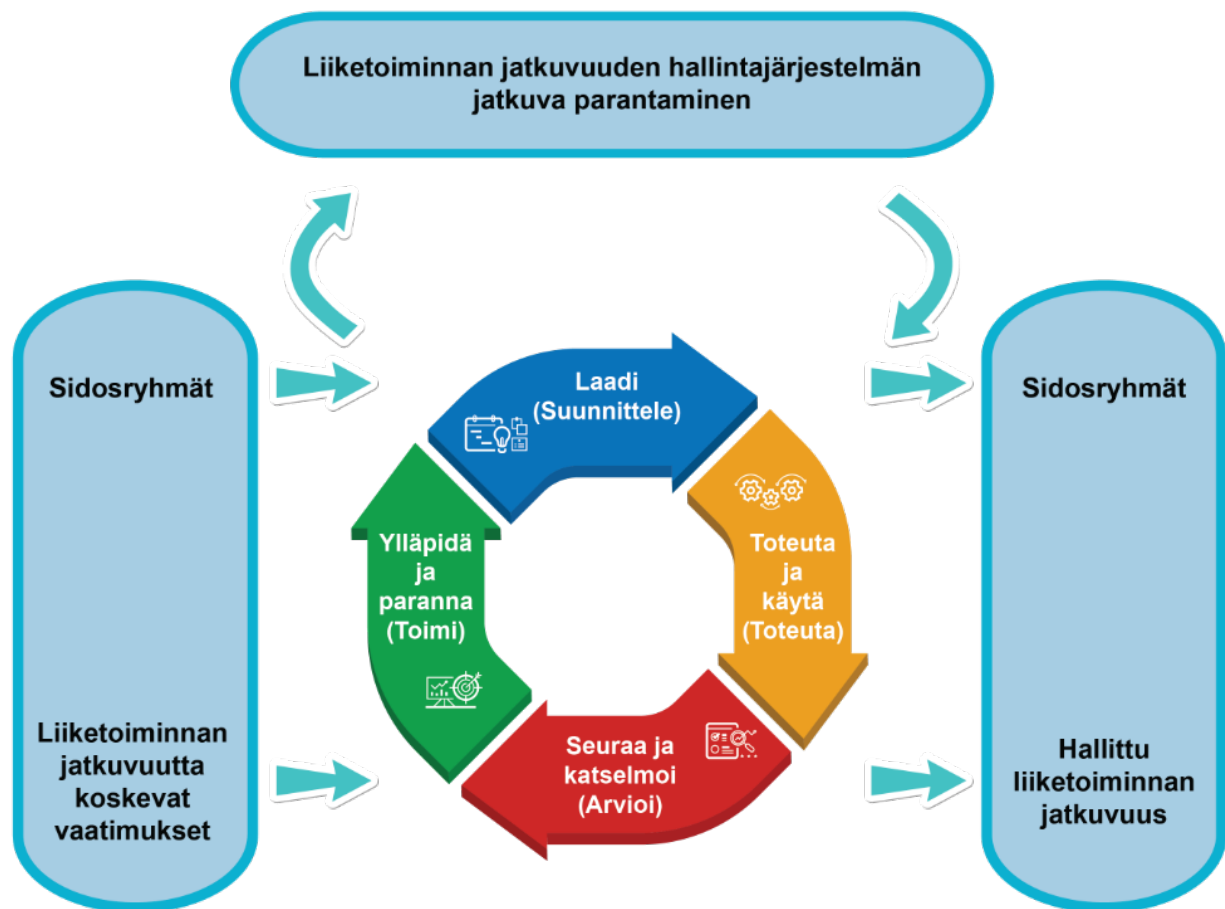
Visiona on rakentaa tuotannon ja toiminnan turvallisuutta vaiheittain toisiaan seuraavien tasojen pohjalta:

- Riskienhallintamenettely on sovittu ja dokumentoitu.
- Jatkuvuudenhallinnan nyky- ja tavoitetilä on tunnistettu ja siihen liittyvät vastuuhenkilöt on määritelty.
- Jatkuvuuden kehittämisen hankkeet ovat vireillä.
- Häiriöiden hallintamenettelyt on määritelty kriittisten kumppaneiden kanssa solmituissa sopimuksissa.
- Jatkuvuusharjoituksia suoritetaan.
- Kriittisten kumppaneiden toimintakyky on varmistettu vaatimalla alihankkijoita ja kumppaneita laatimaan omat jatkuvuussuunnitelmat.
- Jatkuvuudenhallinnan menettelyjä auditoidaan.

Hallintajärjestelmän jatkuva parantaminen

Liiketoiminnan jatkuvuuden hallintajärjestelmän tarkoituksena on auttaa yritystä suojautumaan häiriötilanteilta ja pienentämään häiriöiden todennäköisyyttä. Lisäksi hallintajärjestelmällä parannetaan organisaation kykyä varautua ja reagoida häiriöihin sekä mahdollistetaan se, että organisaatio voi palautua häiriöistä nopeasti ja jatkaa toimintaa normaalisti häiriöiden jälkeen.

Hallintajärjestelmää on parannettava ja tarkennettava säännöllisesti, sillä olosuhteet muuttuvat jatkuvasti. Tähän tarkoitukseen voidaan käyttää **PDCA- eli plan-do-check-act -mallin** mukaista prosessia, joka on esitelty alla olevassa kuvassa.



Hyvä tietää: Plan-Do-Check-Act -mallin prosessia sovelletaan muun muassa ISO 22301:2019 -standardissa.

PDCA-mallissa liiketoiminnan jatkuvuuden hallintajärjestelmää kehitetään ottamalla syötettä sidosryhmiltä ja jatkuvuuden hallinnan vaatimuksista. Tämä sidosryhmiltä ja jatkuvuuden hallinnan vaatimuksista saatu syöte käsitellään mallin mukaisesti syklisesti eli toistuvasti. Näin prosessia parannetaan jokaisella käsittelykierroksella.

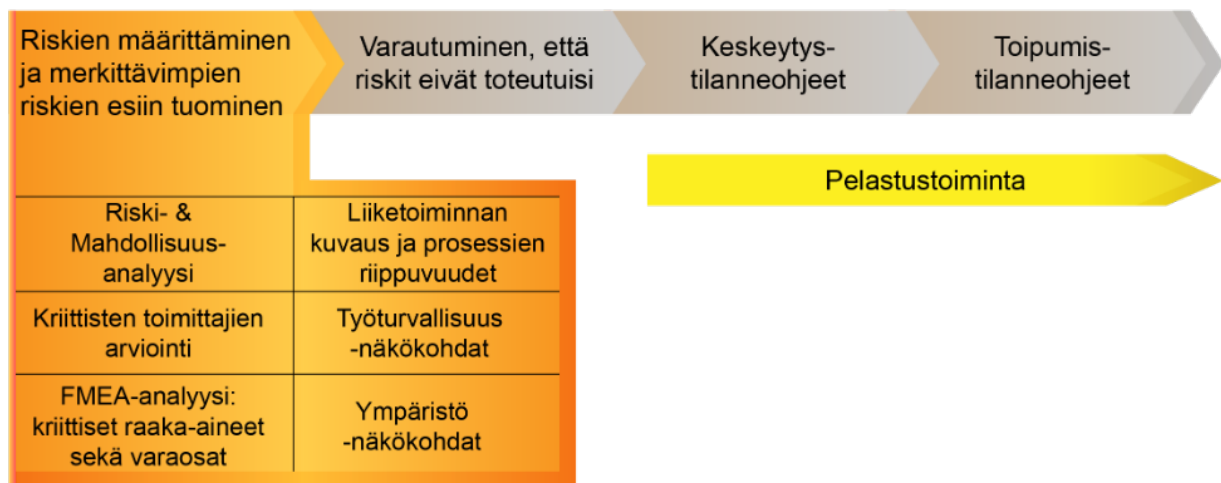
Mallin neljässä vaiheessa tehtävät toimenpiteet ovat seuraavat:

Suunnittele (Plan): Luodaan toiminnan jatkuvuuden politiikkaa, tavoitteita, valvontaa, prosesseja ja menettelyjä, jotka ovat olennaisia liiketoiminnan jatkuvuuden parantamisessa. Tavoitteena on saavuttaa tuloksia, jotka vastaavat organisaation yleisiä periaatteita ja tavoitteita.

- Mirka Oy:n casessa Suunnittele-vaihe käsittää liikkeellelähdön ja etenemisen jatkuvuussuunnitelmassa. Vaihe koostuu edelleen neljästä vaiheesta. Nämä vaiheet on esitetty alla olevassa kuvassa.
- Suunnittelun lähtökohtana on riskien määrittäminen. Riskejä määritetään kuuden erilaisen toimenpiteen avulla. Nämä toimenpiteet ovat:

- 1) riski- ja mahdollisuusanalyysi
- 2) liiketoiminnan kuvaus ja prosessien riippuvuudet
- 3) kriittisten toimittajien arviointi
- 4) FMEA-analyysi eli vika- ja vaikutusanalyysi
- 5) työturvallisuusnäkökohtien arviointi
- 6) ympäristönäkökohtien arviointi.

Määritellään keskeytystilanne- ja toipumistilanneohjeet jatkuvuuden hallintajärjestelmän osana. Näissä ohjeissa määritellään esimerkiksi **pelastustoiminta**.



Liiketoiminnan jatkuvuuden hallintajärjestelmän Suunnittelu-vaiheen eteneminen Mirka Oy:n tapauksessa. Erilaisilla analyysillä varmistetaan, että riskit määritellään ja tuodaan esiin monesta näkökulmasta.

Toteuta (Do): Toteutetaan liiketoiminnan jatkuvuuspolitiikkaa, valvontaa, prosesseja ja menettelyjä.

Arvioi (Check): Seurataan suorituskäytäntöä ja arvioidaan sitä suhteessa liiketoiminnan jatkuvuuspolitiikkaan ja tavoitteisiin. Raportoidaan tulokset johdolle arviointia varten. Johto määrittää korjaavia ja parantavia toimia sekä antaa valtuuksia niiden toteuttamiseen.

Toimi (Act): Toteutetaan korjaavia toimenpiteitä johdolta saadun arvioinnin tulosten perusteella ja ylläpidetään ja parannetaan näin liiketoiminnan jatkuvuuden hallintajärjestelmää. Lisäksi uudelleenarvioidaan säännöllisesti hallintajärjestelmän laajuutta ja liiketoiminnan jatkuvuuspolitiikkaa ja tavoitteita.

PDCA-mallin mukaisten toimien ja prosessin kautta tuotetaan hallittua liiketoiminnan jatkuvuutta, joka täyttää jatkuvuudenhallinnalle asetetut vaatimukset. Lisäksi prosessi tuottaa syötettä yrityksen sidosryhmille.

Toiminta-analyysin pohja

Toiminta-analyysissä pilkotaan kukin toiminto osaprosesseihin. Sitten arvioidaan eri osaprosesseissa esiintyvän mahdollisen häiriön kriittisyys prosessin ja toimitusketjun kannalta.

Toiminta-analyysi on osana esimerkiksi LähiTapiolan julkaisemaa [jatkuvuussuunnitelman mallipohjaa, jonka voit ladata käyttöösi täältä](#).



Toiminnon prosessit on priorisoitu toipumisaikavaatimuksen *) mukaisesti viiteen luokkaan.

Prioriteetti	Liiketoimintaprosessi	Vastuuhenkilö	Keskeiset resurssit ja riippuvuudet**)
1 Toipumisaikavaatimus < X tuntia			
2 Toipumisaikavaatimus < X tuntia			
3 Toipumisaikavaatimus < X vrk			
4 Toipumisaikavaatimus < X vko			
5 Ei määriteltyä toipumisaikaa			

LähiTapiolan julkaisema pohja jatkuvuussuunnitelman dokumentille. Materiaalin tekijänoikeudet kuuluvat LähiTapiola-ryhmälle

Jatkuvuussuunnitelma-asiakirja

Jatkuvuussuunnitelma-asiakirja sisältää kuvauksen toimipaikan jatkuvuussuunnittelusta. Asiakirjassa määritellään myös kutakin jatkuvuussuunnittelun osa-aluetta koskevat tiedonlähteet. Näin kaikki asiaankuuluvat tiedot ovat helposti saatavilla ja löydettävissä.

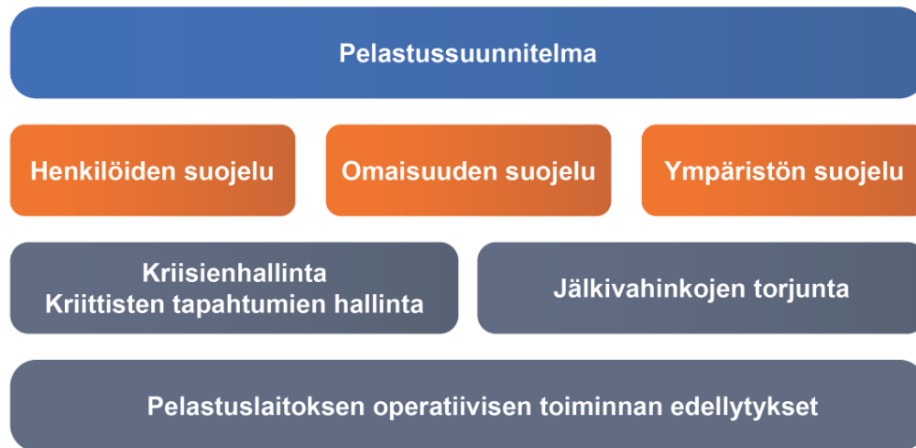
Yleisellä tasolla jatkuvuussuunnitelman toteutuksen vaiheet ovat seuraavat:

1. Jaetaan jatkuvuussuunnitteluun liittyvät vastuut ja määritellään, miten jatkuvuussuunnittelu organisoidaan.
2. Kuvataan toiminta sekä siihen liittyvät kriittiset prosessit ja resurssit;
3. Määritellään merkittävimmät riskit ja niiden vaikutukset toimintaan.
4. Suunnitellaan jatkuvuusriskien hallintaa: kuinka pienennetään häiriöherkkyyttä, mitä varajärjestelyjä on ja kuinka resursseja käytetään.
5. Suunnitellaan keskeytys- ja toipumistilanteita laatimalla toimintaohjeet häiriö- ja toipumistilanteiden varalle, jakamalla vastuut ja laatimalla erityistilanneohjeet ja toipumissuunnitelmat.
6. Testataan suunnitelmaa.
7. Koulutetaan henkilöstöä suunnitelman sisällöstä.
8. Pidetään suunnitelmaa ajan tasalla.

Jatkuvuussuunnitelma-asiakirjaa päivitetään vuosittain tuoreen riskienarvioinnin tekemisen jälkeen.

Pelastustoiminta

Mirka Oy:n casessa pelastussuunnitelman perustana ovat ne edellytykset, joihin pelastuslaitoksen operatiivinen toiminta perustuu. Näistä edellytyksistä käsin rakennetaan suunnitelmat **kriisienhallintaa ja jälkivahinkojen torjuntaa varten**. Kriisienhallintaan sisältyy myös kriittisten tapahtumien hallinta. Kriisienhallintasuunnitelmat kattavat yrityksen henkilöstön suojelun ja osan omaisuuden suojelusta. Jälkivahinkojen torjuntasuunnitelmat kattavat osan omaisuuden suojelusta ja ympäristön suojelun.



Pelastussuunnitelman elementit Mirka Oy:n casessa.

Dokumenttikirjastot

Toiminnan jatkuvuutta koskeva dokumenttikirjasto on yrityksen intranetissä. Dokumentit ovat näkyvissä koko henkilöstölle, mutta jatkuvuushallintaa ja varajärjestelyjä käsittelevät asiakirjat näkyvät vain määritellyille toimihenkilöille.



Dokumenttikirjastoja jatkuvuussuunnittelun toteuttamisessa Mirkan Oy:n casessa.

Tutustu koko esitykseen Mirkan casesta

["Jatkuvuussuunnitelman laatiminen käytännön tasolla"](#) (Tea Tukia-Kangas, Mirka Oy, 2019)



Missä vaiheessa arvioisit teidän yrityksenne tai organisaationne olevan jatkuvuussuunnittelussa?

- ◇ Me emme ole vielä keskustellut tai aloittanut liiketoiminnan jatkuvuuden suunnittelua.
- ◇ Olemme liiketoiminnan jatkuvuuden suunnittelun alkuvaiheessa. Alustavia keskusteluja on käyty ja organisaatiossa on tietoisuutta sen tärkeydestä.
- ◇ Me olemme laatineet liiketoiminnan jatkuvuussuunnitelman ja tunnistaneet kriittiset prosessit ja resurssit, mutta toteutus ja testaus ovat vielä kesken.
- ◇ Yrityksellämme on kattava liiketoiminnan jatkuvuussuunnitelma, jota tarkistetaan ja päivitetään säännöllisesti, testatuilla menettelyillä ja selkeillä rooleilla ja vastuilla, joilla varmistetaan jatkuvuus häiriöiden aikana.
- ◇ En osaa sanoa / Ei relevantti minulle

Minkä seuraavista koet olevan suurin haaste teidän yrityksenne tai organisaationne jatkuvuussuunnittelussa?

- ◇ Ilman johtomme tukea on vaikea kohdentaa resursseja ja saada tarvittavaa sitoutumista vankan liiketoiminnan jatkuvuussuunnitelman kehittämiseen ja toteuttamiseen.
- ◇ Työntekijöidemme vähäinen tietoisuus ja sitoutuminen haittaavat liiketoiminnan jatkuvuussuunnitelmamme tehokkuutta todellisen kriisin aikana.
- ◇ Yrityksemme resurssirajoitusten vuoksi on haastavaa kohdistaa riittävät taloudelliset, teknologiset ja henkilöresurssit kattavan liiketoiminnan jatkuvuussuunnitelman kehittämiseen ja ylläpitämiseen.
- ◇ Muuttuva liiketoimintaympäristö on haaste yrityksellemme, koska meidän on mukautettava jatkuvuussuunnitelmaamme teknologioiden, prosessien, säännösten ja markkinaolosuhteiden muutoksiin.
- ◇ Viestintäkatkokset yrityksessämme, mukaan lukien epäselvät viestintäkanavat, riittämätön tiedon levittäminen tai epäjohtonmukaisuudet viestinnässä, voivat johtaa sekaannukseen ja viivästyksiin reagoititoimissamme kriisin aikana.
- ◇ En osaa sanoa / Ei relevantti minulle

2.5 Elinkaariajattelu täydentää riskienhallintaa

Oppimistavoite: Tässä kappaleessa opit hyödyntämään elinkaariajattelua riskienhallinnan tukena. Opit myös, miten digipalvelun elinkaarianalyysi tehdään ISO 14040 -standardin mukaisesti. Kappaleen lopussa vastaat monivalintatehtäviin elinkaarianalyysin vaiheista. Pistesaldosi kasvaa huikeasti, jos vastaat molempiin oikein! Arvioitu ajankäyttö: 25 min.

Kestävällä kehityksellä tarkoitetaan, että **ihminen, ympäristö ja talous otetaan tasavertaisesti huomioon** päätöksenteossa ja toiminnassa. Talouden kasvuun ei tule pyrkiä keinoilla, joilla on kohtuuttomasti kielteisiä vaikutuksia ihmiseen ja ympäristöön. **Kestävän kehityksen periaate** on yksi toiminnan jatkuvuuden tae, sillä kohtuuton resurssien käyttö päättää toiminnan nopeasti.

Ympäristötietoisuuden kasvaessa yritykset ja niiden asiakkaat kiinnittävät jatkuvasti enemmän huomiota tuotteiden ja palvelujen ympäristövaikutuksiin.

Digitalisaatio ja digitaalinen transformaatio voidaan nähdä kestävän kehityksen kannalta myönteisenä kehityskulkuna. Tämä johtuu siitä, että digitalisaatiolla tavoitellaan fyysisten tuotteiden korvaamista digitaalisilla ratkaisuilla, kuten digipalveluilla. Ajatellaan, että digitaalisilla palveluilla vähennetään fyysisen tuotannon hiilijalanjälkeä, koska digipalvelut ovat aineettomia. Kuitenkin **myös digitaalisten palveluiden tuottamisella on hiilijalanjälki läpi niiden elinkaaren**. Kokonaisuutena ICT-ala kuluttaa paljon energiaa ja materiaaleja, mutta sillä voidaan mahdollisesti myös ratkaista ilmasto- ja ympäristöhaasteita. (Ojala et al. 2020, s. 22–23)

Hiilijalanjälki ja hiilikädenjälki

Hiilijalanjälki on mittari, jolla kuvataan tuotteen tai palvelun koko elinkaaren aikana syntyvää ilmastokuormaa, kuten kasvihuonekaasupäästöjä. Digitaalisen palvelun tuottamisesta syntyvät kasvihuonekaasupäästöt lasketaan palvelun energiankulutuksen perusteella.

- ISO 14067 -standardissa määritellään menetelmät, joita käytetään hiilijalanjäljen laskemiseen ja raportointiin. Hiilijalanjäljen laskennan vaiheet ovat vastaavat kuin elinkaarianalyysin standardeissa ISO 14040 ja 14044.
- Kaikkien energiatuotannon muotojen rakentamiseen ja lopulta purkamiseen tarvitaan materiaaleja ja energiaa. Päästöjen suuruus riippuu materiaalien ja energian määristä ja tuotantomuodoista. Päästöt lasketaan tuotettua energiayksikköä kohti.



Hiilikädenjälki puolestaan kuvaa tuotteen, palvelun tai yrityksen toiminnan positiivisia ympäristövaikutuksia. Nämä positiiviset vaikutukset **pienentävät toisen toimijan**, kuten asiakkaan, **hiilijalanjälkeä verrattuna siihen, paljonko vastaavan tuotteen/palvelun käyttäminen keskimäärin kuluttaisi** (engl. baseline). (Pajula et al. 2021)

Hiilikädenjälki-käsitteellä viitataan laajemminkin kaikkiin toimiin, joilla pienennetään tuotteen tai palvelun hiilijalanjälkeä. Hiilikädenjälkeä voidaan kasvattaa esimerkiksi parantamalla tuotteiden kierrätettävyyttä, pidentämällä niiden elinikää, lisäämällä uusiutuvien materiaalien käyttöä tuotannossa sekä suunnittelemalla tuotteita, jotka toimivat **hiilinieluna**. Hiilinielut ovat mekanismeja, jotka sitovat tuotettuja hiilidioksidipäästöjä. (Pajula et al. 2021)

Hiilikädenjälki voidaan asettaa tavoitteeksi tuote- ja tuotantokehityksessä, nostaa tuotteen ominaisuudeksi sen markkinoinnissa sekä tukemaan asiakkaiden ja sidosryhmien päätöksentekoa. (Pajula et al. 2021)

- Suomalaiset tutkijat ovat julkaisseet ohjeistuksen hiilikädenjäljen laskentaan artikkelissaan [Approach for assessing environmental handprints](#) (s. 15).

Tuotteen elinkaari

ISO 14040 -standardin määritelmän mukaan ”*elinkaari on tuotejärjestelmän peräkkäiset tai vuorovaikutteiset vaiheet raaka-aineiden hankinnasta tai tuottamisesta luonnonvaroista loppusijoitukseen*”.

Fyysisen tuotteen elinkaaren vaiheita ovat tyypillisesti raaka-aineiden hankinta, tuotteen valmistus, tuotteen kuljetus asiakkaalle sekä tuotteen käyttö ja lopulta käytöstä poisto, kuten puretun tuotteen materiaalien kierrättäminen.

Myös digipalveluista voidaan tunnistaa vastaavat tuotteen elinkaaren vaiheet.

Elinkaaren jokaisen vaiheen ympäristövaikutukset voidaan selvittää analyysillä, kunhan käytettävissä on riittävästi dataa.

Elinkaariajattelu

Elinkaariajattelulla tarkoitetaan, että riskejä tai ympäristö- tai terveysvaikutuksia arvioitaessa ei rajoituta tuotteen mahdollisiin välittömiin ympäristö- tai terveysvaikutuksiin, vaan huomioon otetaan tuotteen koko tuotantoketjun ympäristökuorma.

Elinkaariajattelun avulla voidaan arvioida, kuinka merkittäviä koko ketjun ympäristö- tai terveysriskit ovat, kun riskejä verrataan vaihtoehtoihin kokonaisratkaisuihin.

Elinkaariajattelu ei siis rajoitu pelkästään tuotekehitykseen ja valmistukseen. Se on pätevä väline myös omaan käyttöön sopivan tuotteen tai palvelun valinnassa sekä tuotteiden ja palvelujen vertailussa.

Elinkaarianalyysi

Elinkaarianalyysi (engl. Life Cycle Analysis, LCA) on menetelmä, jolla voidaan selvittää toiminnan, tuotteen tai palvelun aiheuttamia ympäristövaikutuksia ja kuluttamia resursseja koko sen elinkaaren aikana. Analyysissä otetaan huomioon koko toimintaketju sekä siihen sisältyvät välilliset ja välittömät vaikutukset. Jotta analyysi pystytään tekemään täsmällisesti, dataa tulee olla käytettävissä elinkaariketjun kaikista vaiheista.

Elinkaarianalyysien toteuttamista yhtenäistää ISO-standardi 14040. Standardissa määritellään **elinkaarianalyysin päävaiheet** seuraavasti: **tavoitteen ja soveltamisalan määrittely, inventaarioanalyysi, vaikutusten arviointi ja tulosten tulkinta**. ISO 14044 -standardissa puolestaan määritellään elinkaariarvioinnin vaatimuksia.

Elinkaarianalyysi aloitetaan **tavoitteen määrittelyllä**. Sen yhteydessä määritellään elinkaarianalyysin käyttötarkoitus, analyysin tekemisen syyt, aiottu kohdeyleisö ja se, käytetäänkö tuloksia julkisesti esitettävissä vertailuissa.

Ensimmäisessä vaiheessa tehdään myös **soveltamisalan määrittely**. Soveltamisalan määrittelyssä määritellään työn toiminnallinen yksikkö, työn rajoitukset, oletukset ja ne vaatimukset, jotka asetetaan analyysissä käytettävälle tiedolle. **Toiminnallinen yksikkö** tarkoittaa ISO 14044 -standardin mukaista referenssiyksikköä. Referenssiyksikkö kuvaa tarkasteltavan tuotejärjestelmän määrällistä suorituskkyä.

Lisäksi tehdään **työn rajojen määrittely**. Sillä ilmaistaan, mitä yksikköprosesseja analyysissä käytetään. **Yksikköprosessit** ovat inventaarioanalyysin **pienimpiä huomioitavia kohteita**, jotka vaikuttavat elinkaaren syötteeseen ja tulokseen.

Elinkaarianalyysissä työn rajoitusten pitää olla yhdenmukaiset analyysin tavoitteiden kanssa. Soveltamisalan määrittelyn yhteydessä kerrotaan, mikäli joitain prosesseja tai syötteitä ei oteta elinkaareissa huomioon. Jos jokin tieto rajataan elinkaarianalyysin ulkopuolelle, se pitää perustella.

Elinkaarianalyysin toinen vaihe on **inventaarioanalyysi**. Inventaarioanalyysissä kerätään ja analysoidaan tietoa raaka-aineista, joita käytetään elinkaaren aikana, ja lopputuloksena syntyvistä tuotteista ja päästöistä. Analyysiä varten kerätään tietoa kaikista järjestelmään kuuluvista yksikköprosesseista. Näiden tietojen kelpoisuus myös tarkistetaan, ettei tieto ole vääristynyttä.

Lisäksi inventaarioanalyysissä kuvataan kerättävän tai tietokannoista haettavan tiedon allokointi ja laskentamenetelmät. **Allokointi tarkoittaa elinkaaren materiaalivirtojen ja tuotosten kohdentamista**. Allokointi on välttämätöntä myös digitaalisen palvelun elinkaarianalyysissä, koska digitaalinen palvelu sisältää päällekkäistä infrastruktuuria. Esimerkiksi samoja palvelinlaitteita käytetään useiden digipalveluiden toteuttamiseen. Allokoinnin yhteydessä yksikköprosessit voidaan jakaa alaprosesseihin ja niihin liittyviä syöte- ja tuotostietoja voidaan kerätä.

Elinkaarianalyysin kolmas vaihe on **vaikutusarviointi**. Vaikutusarvioinnissa pohditaan, kuinka merkittäviä inventaarioanalyysissä todetut ympäristövaikutukset ovat. Vaikutusarvioinnissa saadut tulokset sijoitetaan vaikutusluokkiin ja lasketaan vaikutusluokkaindikaattorien tulokset. Vaikutusluokkaindikaattorien tulosten laskennassa inventaarioanalyysissä saadut tulokset muutetaan yhteiseen yksikköön. Laskennan jälkeen tiedot kootaan sellaisiin ryhmiin, joissa tulokset on tarkoituksenmukaisinta esitellä. Vaikutusarvioinnissa tutkitaan **soveltamisalassamääriteltäjä ympäristövaikutuksia**.

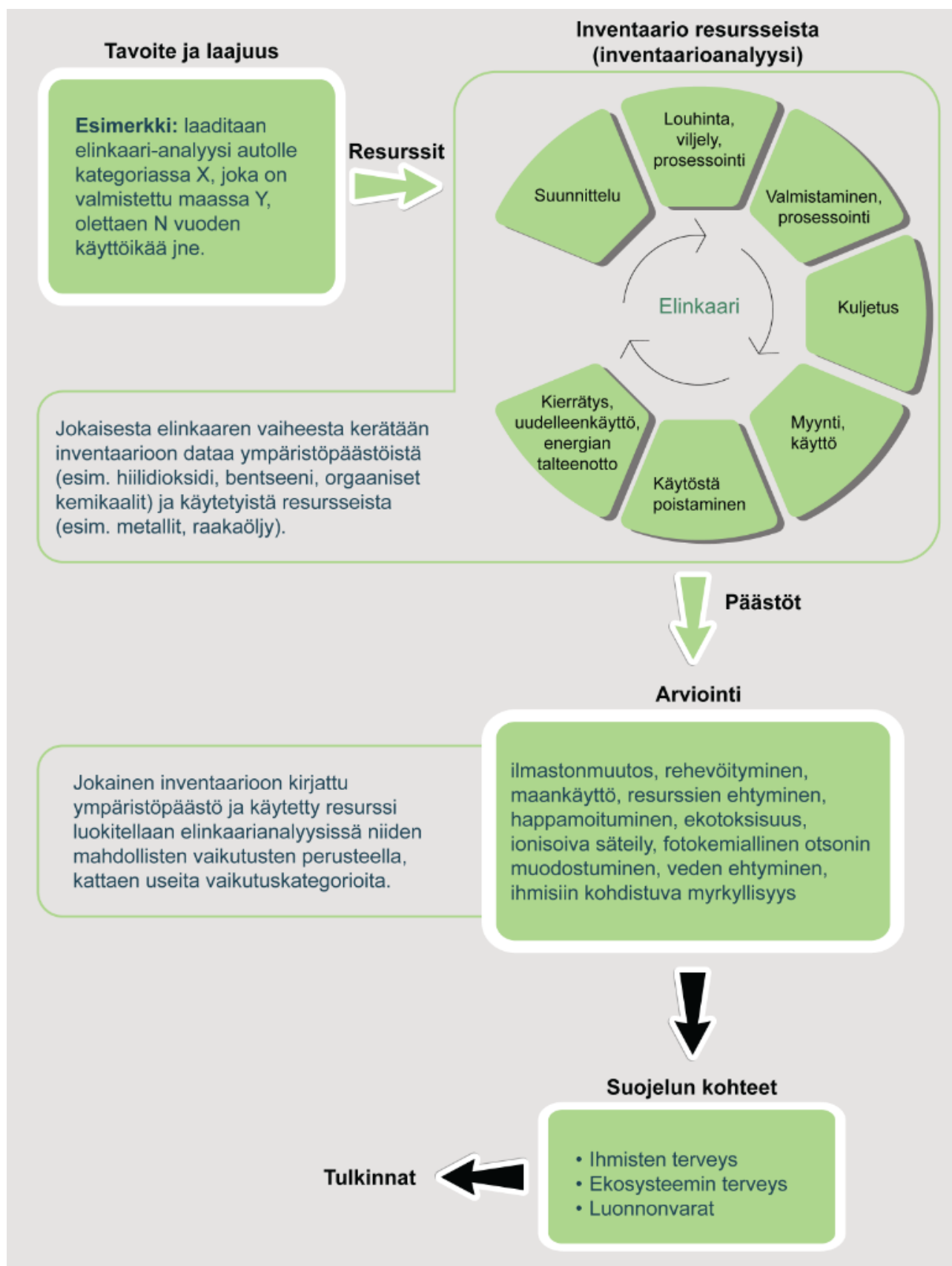
Elinkaarianalyysin neljäs ja viimeinen vaihe on **tulosten tulkinta**. Sen yhteydessä tarkastellaan inventaarioanalyysin ja vaikutusarvioinnin tuloksia sitä, miten nämä tulokset vaikuttavat toisiinsa.

Elinkaarelle voidaan tehdä myös **herkkyysanalyysi**. Herkkyysanalyysin avulla arvioidaan, miten menetelmien ja lähtötietojen valinta vaikuttaa elinkaarianalyysin tuloksiin.

Elinkaarianalyysin ja inventaarioanalyysin **tulosten luotettavuutta** arvioidaan **elinkaarianalyysin arvioinnilla**. Arvioinnissa tarkastetaan käytetyn tiedon täydellisyys ja johdonmukaisuus. Johdonmukaisuuden tarkistuksen yhteydessä tutkitaan, ovatko menetelmä ja lähtötieto yhdenmukaisia tavoitteiden ja soveltamisalan kanssa.

Raportoinnissa esitetään, miten käytetyt tiedot on kerätty ja käsitelty. Lisäksi todetaan elinkaarianalyysin tulokset ja niistä tehdyt johtopäätökset.

ISO 14040 -standardin mukaan elinkaarianalyysi koostaa tuotejärjestelmän panokset, tuotokset sekä mahdolliset ympäristövaikutukset ja arvioi niitä koko tuotejärjestelmän elinkaaren ajalta. EU:ssa on käytössä ohjeistus *International reference Life Cycle Data system handbook* joka koostuu [useasta dokumentista](#).



Elinkaarianalyysin vaiheet prosessina (Sala et al. 2016 s. 7). [Lataa kuvan täysikokoinen versio.](#)

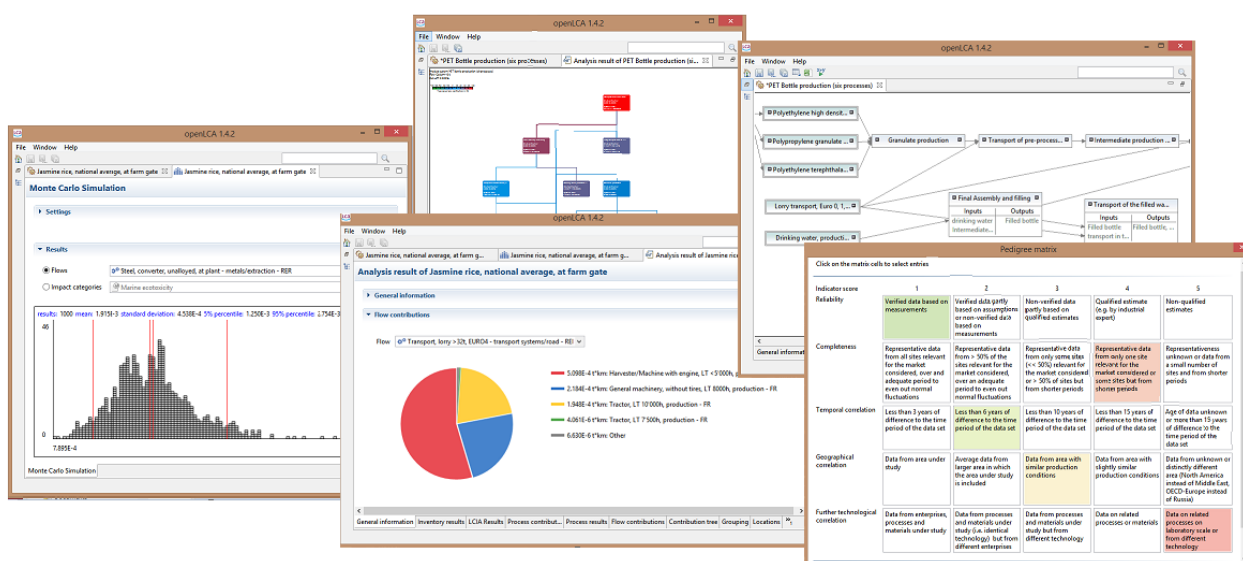
Elinkaarianalyysin toteuttaminen

Elinkaarianalyysia voidaan lähestyä joko haitanjaollisen arvioinnin tai seurausvaikutuksellisen arvioinnin kautta.

Haitanjaollisella elinkaariarvioinnilla (engl. attributional LCA) tarkastellaan elinkaaren perusvirtoja ja mahdollisia ympäristövaikutuksia muuttumattomassa tilassa. Arvioinnissa huomioidaan ne ominaisuudet, jotka vaikuttavat suoraan tutkittavaan elinkaareen. (SYKE 2010 s. 32–33.)

Seurausvaikutusten arvioinnilla (engl. consequential LCA) tutkitaan ”mitä jos” -skenaarioita eli pyritään mallintamaan, miten erityyppiset päätökset vaikuttavat tuotteen tai palvelun ympäristövaikutuksiin. Seurausvaikutusten arvioinnissa huomioidaan prosessit, jotka voivat muuttua tietyn päätöksen jälkeen tuotteen tai palvelun suunnittelussa, toteutuksessa tai sen kysynnän muutoksissa. (SYKE 2010 s. 32–33.)

Elinkaarianalyysi on helpointa laatia ohjelmistolla. Tällainen ohjelmisto on esimerkiksi [OpenLCA](#). Ohjelmisto mallintaa tuotteen tai palvelun elinkaarta elinkaaren eri vaiheita kuvaavan datan pohjalta. Se myös laskee ja mallintaa tuotteen tai palvelun elinkaaren ympäristövaikutuksia. Tällaiseen elinkaaren rakentamiseen ohjelmistot käyttävät dataa ohjelmiston omista ja ulkopuolisista tietokannoista.



OpenLCA -ohjelmiston eri näkymiä elinkaarianalyysin toteuttamiseen. Mahdollisuuksiesi mukaan, lataa tämä ilmainen ohjelmisto ja tutustu sen ominaisuuksiin. [Kuvan lähde](#).

Digipalvelun ympäristövaikutusten arviointi

Digitaalisilla palveluilla on huomattavia ympäristövaikutuksia. Vuonna 2020 julkaistun tutkimuksen mukaan **digipalvelut aiheuttivat 4 % kaikista ihmisten tuottamista kasvihuonekaasupäästöistä** (Bordage 2020).

Digipalvelun ympäristövaikutuksia voidaan tarkastella ainakin kolmesta näkökulmasta. Alla perehdytään lyhyesti näihin kolmeen näkökulmaan.

Ensinnäkin digipalveluiden infrastruktuurin mahdollistavien laitteiden (kuten palvelimet, reitittimet, valokuitukaapeli, jne.) valmistaminen kuluttaa raaka-aineita ja energiaa sekä aiheuttaa päästöjä. Komponentit valmistettaviin laitteisiin haalitaan ympäri maailmaa, minkä jälkeen valmiit digilaitteet rakennetaan ja kuljetetaan käyttäjilleen.

Toiseksi digipalveluiden toteuttaminen kuluttaa paljon energiaa. Sähkön tuotanto ja kulutus ovatkin merkittävä päästöjen aiheuttaja. Datakeskukset tuottavat paljon lämpöä, minkä takia niitä joudutaan jäähdyttämään. Sähköä kuluu myös, kun digilaitteita pidetään päällä ja ohjelmistoja ajetaan. Tähän sisältyy myös digipalveluiden ylläpitäminen. Mitä enemmän laskentaa digipalvelun tuottaminen edellyttää tietokoneelta tai palvelimelta, sitä enemmän se kuluttaa energiaa ja aikaansaa lämpöä. Palvelun asiakkaan puolella esimerkiksi suurempi näyttölaite kuluttaa enemmän sähköä kuin pienempikokoinen näyttö.

Kolmanneksi tulee huomioida, että digitalisaatio on globaali ilmiö, joten sen ympäristövaikutuksia ei voida tarkastella pelkästään toimiala- tai maakohtaisesti. Digitaalisen palvelun tuottamat päästöt ylittävät monesti maiden rajat. Tällainen tilanne on esimerkiksi silloin, kun Suomessa käytetään massiiviseen dataprosessointiin pilvipalvelua, joka aktivoi toisessa maassa datakeskuksen, jonka energia puolestaan tuotetaan fossiilisilla polttoaineilla. Myös globaalin tietoliikenneverkon ylläpitäminen kuluttaa paljon energiaa. (Toivonen 2021)

Digipalvelun elinkaarianalyysi

Kun analysoidaan digitaalista palvelua, elinkaarianalyysissä noudatetaan samoja vaiheita kuin fyysisen tuotteen elinkaarianalyysiä tehtäessä. Seuraavassa käydään lyhyesti läpi muutama digipalvelun elinkaarianalyysin kannalta keskeinen käsite.

- Digipalvelun **toiminnallinen yksikkö** elinkaarianalyysissä voi olla esimerkiksi siirretyn tai tallennetun datan määrä, käytössä olevien laitteiden (kuten palvelimien tai prosessoreiden) kappalemäärä, vuosittainen käyttö tai energiankulutus. (Pohjonen 2022)
- Digipalvelun **inventaarioanalyysissä** huomioidaan digilaitteiden ja digi-infran tuotantoprosessit. Tuotantoprosesseihin lasketaan mukaan myös komponenttien raaka-aineiden tuotanto. Lisäksi analyysissä otetaan huomioon käytettävä palvelualusta (esim. pilvipalvelu) ja digitaalinen kulutuskäyttäytyminen (Bordage 2019 s. 38).
- Digipalvelun **allokointiin** käy ohjeeksi esimerkiksi GHG-protokolla. Sen mukaan paras tapa allokoida ICT-tuotteita on kohdentaa tarkastelu jaetun komponentin, kuten datan, käytön mukaan. Verkkoyhteyden käyttöä voidaan allokoida siirretyn datan perusteella esimerkiksi sekunnissa siirrettyjen megatavujen (Mt/s) ja siirron suunnan perusteella. Ohjelmiston käyttöä voidaan allokoida sen perusteella, paljonko ohjelmisto vie käyttömuistia tai levytilaa. Datakeskuksen käyttöä allokoidaan tiedon käsittelyyn kuluneen ajan tai käytettyjen palvelinlaitteiden lukumäärän perusteella. (GeSI 2017, s.4-30)
- Digipalvelun **elinkaaren loppuosa** voi olla hankala määritellä, sillä monesti ei tiedetä tai suunnitella, mitä digitaaliselle palvelulle tapahtuu sen käytön jälkeen: poistetaanko

esimerkiksi vanha verkkosivusto vai jääkö se kuormittamaan ympäristöä olemalla käyttövalmiina tietoverkossa. (Pohjonen 2022)

GeSI-järjestö (2017) on esittänyt viisikohtaisen protokollan, jolla lasketaan digipalvelun hiilijalanjälki sen energiakulutuksen kautta:

1. Suoritetaan energiankulutuksen mittausta tai arviointi.
2. Mitataan digipalvelun käyttöprofiili.
3. Lasketaan käytetty energia.
4. Määritellään yleinen energian kulutus sen perusteella, mitä vaihtuvia energiaa kuluttavia toimintoja palvelun tuottamiseen sisältyy, mm. laitteiden jäähdyttäminen.
Energiankulutuksen päästöt selvitetään alueellisten päästökertoimien avulla tai laskemalla energiankulutus elinkaarianalyysiohjelmalla.
5. Digipalvelun energiankulutus muunnetaan kasvihuonekaasupäästöiksi. (GeSI 2017)

GHG-protokollan yhteydessä annetaan myös yleisiä ohjeita digipalveluiden soveltamisalan määrittelyyn, elinkaarianalyysissä tarvittavan datan keräämiseen, huomioitaviin epävarmuustekijöihin ja rajojen asettamiseen. (Pohjonen 2022)

Elinkaariajattelu riskienhallinnan tukena

Elinkaariajattelu tukee riskienhallintaa, sillä sen avulla voidaan tunnistaa riskejä. Tällaisia havaittavia riskejä voivat olla esimerkiksi se, että tuotantoketjun jokin toimittaja on täysin riippuvainen yhden raaka-aineen saatavuudesta tai sen liiketoiminta on haavoittuvainen tietyn energiamuodon hintavaihteluille.

Elinkaariajattelu voi myös paljastaa sellaisia prosessien ja organisaation sisäisiä ristiriitoja, jotka voivat osoittautua uhkiksi toiminnalle kokonaisuutena. Jollakin organisaation alueella voidaan olla hyvin tarkkoja ympäristöasiassa, jolla ei ole kokonaisuuden kannalta olennaista merkitystä verrattuna toisella organisaation alueella tehtäviin päätöksiin tai toimenpiteisiin.

Ekosuunnittelu

Suunnittelu on tuotteen tai palvelun elinkaaren ensimmäinen vaihe. **Ekologisella suunnittelulla (ekodesign)** pyritään **pienentämään** tuotteen tai palvelun **ympäristövaikutuksia jo suunnitteluvaiheessa**.

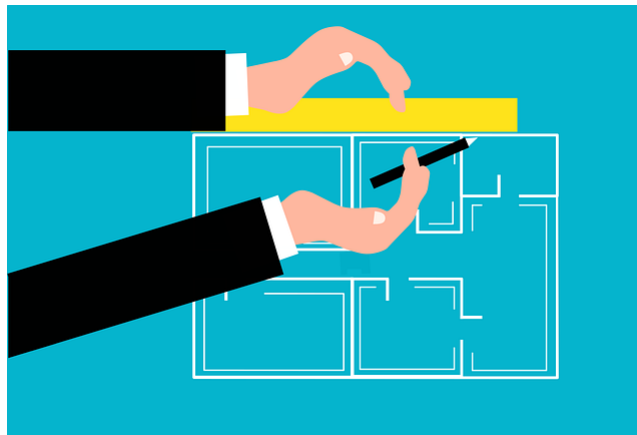
Ekodesignin periaatteita hyödyntävässä tuotekehityksessä pyritään vaikuttamaan merkittävään osaan tuotteen elinkaaren aikaisista negatiivisista ympäristövaikutuksista joko vähentämällä, välttämällä tai poistamalla niitä. Tuotetta suunnitellaan paitsi asiakkaan tarpeet mielessä, myös tavoitellen tuotteen tuottamisen ja käytön kielteisten ympäristövaikutusten pienentämistä.

Suomessa on voimassa *laki tuotteiden ekologiselle suunnittelulle ja energiamerkinnälle asetettavista vaatimuksista* (19.12.2008/1005).

Ekodesignin periaatteita voi hyödyntää usealla tavalla digipalveluiden suunnittelussa. Digitaalisten palveluiden tuottaminen kuluttaa energiaa, joten digipalveluiden ekodesignissa kiinnitetään huomiota energiankulutukseen vähentämiseen palvelun koko elinkaaren aikana. Huomiota kiinnitetään mm. siihen, millä tuotantomuodoilla palvelinlaitteiden tarvitsema energia tuotetaan, milloin ja miten digipalvelun tuottavaa ohjelmistoa suoritetaan, kuinka usein dataa siirretään ja miten palvelinlaitteiden lämpö hyödynnetään. Digipalvelun käyttöliittymä voidaan suunnitella sellaiseksi, että sitä voidaan käyttää hyvin myös pienempinäytöisellä laitteella, joka kuluttaa vähemmän sähköä.



Kuvittele, että olet arkkitehti, joka suunnittelee uutta toimistorakennusta asiakkaalle, jolle rakennuksen kestävyys on prioriteetti.



Vastaa alla, missä elinkaariarvioinnin vaiheessa lasketaan rakennusmateriaalien ympäristövaikutukset?

- ◇ Tavoitteen ja soveltamisalan määrittely
- ◇ Vaikutusten arviointi
- ◇ Inventaarioanalyysi
- ◇ Tulosten tulkinta

Kuvittele, että työskentelet suosituilla suoratoistopalustalla, joka tarjoaa elokuvia miljoonille käyttäjille ympäri maailmaa. Osana kestävän kehityksen aloitteitasi, suoritat elinkaarianalyysin suoratoistopalvelulle.



Vastaa alla, missä analyysin vaiheessa jakaisit datakeskusten, verkkoinfrastruktuurin ja ohjelmistojen käytön ympäristövaikutukset kriteerien, kuten tiedonsiirron, käsittelyajan ja palvelimen käytön, perusteella?

- ◇ Toiminnallinen yksikkö
- ◇ Vaikutusarviointi
- ◇ Allokointi
- ◇ Digipalvelun elinkaaren loppuosa

Lähteet



Lähdeluettelo on koottu [tälle sivulle](#).